



Log Reference

FortiSIEM 7.3.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



01/09/2025

FortiSIEM 7.3.0 Log Reference

TABLE OF CONTENTS

Change Log	123
Important Logs By Use case	124
Use Case: Collector clock skew detected	124
EventType: PH_COLLECTOR_CLOCK_SKEW	125
Use Case: Collector failing to forward events to External System	125
EventType: PH_AGENTMGR_KAFKA_PRODUCER_ERROR	125
EventType: PH_EVENT_FWD_SOCKET_CONNECT_FAILED	126
EventType: PH_EVENT_FWD_SOCKET_WRITE_FAILED	126
Use Case: Collector failing to send events to Worker on time	126
EventType: PH_COLLECTOR_EVENT_STORE_DELAYED	127
Use Case: Collector failing to send events to Workers	127
EventType: PH_EVENT_PKG_FILE_UPLOAD_FAILED	127
EventType: PH_EVENT_PKG_HTTP_FAILED	127
EventType: PH_EVENT_PKG_HTTP_INIT_FAILED	128
EventType: PH_EVT_PACKAGER_FILE_UPLOAD_FAILURE	128
Use Case: Collector/Worker to Supervisor communication issue	129
EventType: PH_COLLECTOR_DOWN	129
EventType: PH_WORKER_DOWN	129
Use Case: Devices not sending logs	129
EventType: PH_DEV_MON_LOG_DEVICE_DELAY_HIGH	129
EventType: PH_DEV_MON_LOG_DEVICE_DELAY_LOW	130
Use Case: EPS License Exceeded	130
EventType: PH_PARSER_GLOBAL_LICENSE_EXCEED	130
Use Case: EPS Reporting	131
EventType: PH_SYSTEM_EPS_GLOBAL	131
EventType: PH_SYSTEM_EPS_NODE	131
EventType: PH_SYSTEM_EPS_ORG	133
Use Case: Event Archiving Error (Elasticsearch to EventDB/NFS)	133
EventType: PH_ES_COLD_STORAGE_ARCHIVING_FAILED	133
EventType: PH_ES_HOT_STORAGE_ARCHIVING_FAILED	134
EventType: PH_ES_WARM_STORAGE_ARCHIVING_FAILED	134
Use Case: Event Archiving Error (EventDB to EventDB/NFS)	134
EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_FAILED	134
EventType: PH_SYSTEM_DISK_ARCHIVING_FAILED	134
Use Case: FortiSIEM Process is Down	134
EventType: PH_APPSERVER_FRAMEWORK_SECURITY_INIT_SYSTEM_ERROR	135
EventType: PH_MODULE_ABORT	135
EventType: PH_MODULE_ABORT_FOUND	135
EventType: PH_MODULE_EXITING	136
EventType: PH_MODULE_INIT_FAILURE	136
Use Case: FortiSIEM process to Supervisor communication issue	136
EventType: PH_DATAMANAGER_HTTP_UPLOAD_ERROR	136
EventType: PH_EVT_PACKAGER_HTTP_RESPONSE_ERROR	137
EventType: PH_IDENTITYMASTER_HTTP_UPLOAD_ERROR	137

EventType: PH_MONITOR_UNABLE_CONTACT_APPSVR	137
EventType: PH_PARSER_HTTP_RESPONSE_ERROR	138
EventType: PH_PARSER_HTTP_UPLOAD_FAILURE	138
Use Case: GUI Change Audit	138
EventType: PH_AUDIT_CASE_CLOSED	139
EventType: PH_AUDIT_CASE_CREATED	139
EventType: PH_AUDIT_CASE_UPDATED	140
EventType: PH_AUDIT_CMDB_DISK_PRUNE_FAILED	140
EventType: PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS	140
EventType: PH_AUDIT_DASHBOARD_SHARED	141
EventType: PH_AUDIT_DEVICE_ADDED	141
EventType: PH_AUDIT_DEVICE_DELETED	142
EventType: PH_AUDIT_DEVICE_DISCOVERY_ITEM_CHANGED	142
EventType: PH_AUDIT_DEVICE_MERGED_BY_IP_WITH_DIFF_NAME	143
EventType: PH_AUDIT_DEVICE_STATUS_CHANGED	143
EventType: PH_AUDIT_GROUP_CREATED	144
EventType: PH_AUDIT_GROUP_DELETED	144
EventType: PH_AUDIT_INCIDENT_SYS_CLEAR	145
EventType: PH_AUDIT_INCIDENT_USER_CLEAR	145
EventType: PH_AUDIT_MALWARE_DATA_DELETED	145
EventType: PH_AUDIT_MALWARE_DATA_UPDATED	146
EventType: PH_AUDIT_OBJECT_CREATED	146
EventType: PH_AUDIT_OBJECT_DELETED	147
EventType: PH_AUDIT_OBJECT_UPDATED	147
EventType: PH_AUDIT_PASSWORD_CHANGED	148
EventType: PH_AUDIT_REPORT_SCHEDULED	148
EventType: PH_AUDIT_RULE_ACTIVATED	148
EventType: PH_AUDIT_RULE_DEACTIVATED	149
EventType: PH_AUDIT_USER_ADDED	149
EventType: PH_AUDIT_USER_DEFAULT_ROLE_CHANGED	149
EventType: PH_AUDIT_USER_DELETED	150
EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_CHANGED	150
EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_ENABLED	151
EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_REMOVED	151
Use Case: GUI User Login	152
EventType: PH_AUDIT_ACCOUNT_LOCKED	152
EventType: PH_AUDIT_USER_LOGIN_FAILURE	152
EventType: PH_AUDIT_USER_LOGIN_SUCCESS	153
EventType: PH_AUDIT_USER_LOGOFF	153
Use Case: Incident External Integration issue	154
EventType: PH_APPSERVER_IN_INTEGRATION_ERROR	154
EventType: PH_APPSERVER_OUT_INTEGRATION_ERROR	154
Use Case: Incident email notification issue	154
EventType: PH_APPSERVER_NOTIFIER_ERROR	154
EventType: PH_INCIDENT_ACTION_STATUS	154
Use Case: Linux Agent operational errors	155
EventType: PH_FAILED_TO_EXEC	155
EventType: PH_LINUX_AGENT_BIND_PORT_FAILED	155
EventType: PH_LINUX_AGENT_CONFIG_ATTR_NOT_FOUND	156

EventType: PH_LINUX_AGENT_CREATE_SOCKET_FAILED	156
EventType: PH_LINUX_AGENT_HOST_IP_GOT_FAILED	156
EventType: PH_LINUX_AGENT_OPEN_FILE_FAILED	156
EventType: PH_LINUX_AGENT_OPEN_PORT_FAILED	157
EventType: PH_LINUX_AGENT_RECV_ERROR	157
EventType: PH_LINUX_AGENT_VERIFIER_ERROR	157
Use Case: Malware IOC handling Errors	158
EventType: PH_APPSERVER_EXT_THREAT_INTEL_UPDATE_ERROR	158
EventType: PH_APPSERVER_FORTIGUARD_IOC_INTEGRATION_ERROR	158
EventType: PH_APPSERVER_IOC_TASK_CREATE_FAILED_ERROR	158
Use Case: Query Errors	159
EventType: PH_APPSERVER_QUERY_EXPORT_ERROR	159
EventType: PH_APPSERVER_QUERY_RESULT_RETRIEVE_ERROR	159
EventType: PH_APPSERVER_QUERY_RUN_ERROR	159
EventType: PH_APPSERVER_QUERY_STOP_ERROR	159
EventType: PH_APPSERVER_REPORT_BUNDLE_PRINT_ERROR	160
Use Case: Query Performance	160
EventType: PH_AUDIT_QUERY_COMPLETED	160
Use Case: Rule Performance	160
EventType: PH_RULEMOD_PROFILE	161
Use Case: Rule trigger issues	161
EventType: PH_DROP_EVENT_FROM_SHARED_BUFFER	161
EventType: PH_DROP_INCIDENT	162
EventType: PH_REPORT_PACK_FAILED	162
EventType: PH_RULEMOD_SUMMARY_UPLOAD_FAILED	163
EventType: PH_UTIL_NOTIFICATION_UPLOAD_FAILURE	163
Use Case: Scheduled Report issue	163
EventType: PH_REPORT_ACTION_STATUS	163
Use Case: Test Connectivity/Discovery Errors	164
EventType: PH_DISCOV_DISCOV_REQ_GET_FAILED	164
EventType: PH_DISCOV_RESULT_SEND_FAILED	164
EventType: PH_DISCOV_TEST_CONN_GET_REQ_FAILED	164
EventType: PH_DISCOV_TEST_CONN_RESULT_SEND_ERROR	164
Use Case: Windows/Linux Agent operational errors	165
EventType: PH_AUDIT_AGENT_DISABLED	165
EventType: PH_AUDIT_AGENT_NOTRESPONDING	165
EventType: PH_AUDIT_AGENT_UNINSTALLED	166
Use Case: Worker failing to store events in ClickHouse	166
EventType: PH_CLICKHOUSE_INSERTION_DROP_EVENTS	167
EventType: PH_DATAMANAGER_CLICKHOUSE_HTTP_UPLOAD_ERROR	167
Use Case: Worker failing to store events in Elasticsearch	167
EventType: PH_DATAMANAGER_EVTLOADER_ERROR	167
EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FAIL	168
Use Case: Worker failing to store events in EventDB	168
EventType: PH_DATAMANAGER_SUMMARYWRITER_ERROR	168
EventType: PH_UNABLE_ACCESS_DIR	169
EventType: PH_UNABLE_CREATE_DIR	169
EventType: PH_UNABLE_OPEN_DIR	169

Use Case: Worker falling behind in storing configuration files to SVN-lite	170
EventType: PH_EVT_HANDLER_SVN_QUEUE_WARNING	170
Use Case: Worker falling behind in storing events to Event Database	170
EventType: PH_EVT_HANDLER_EVT_QUEUE_LARGE	170
EventType: PH_EVT_HANDLER_EVT_QUEUE_WARNING	171
AppServer Logs	172
EventType: PH_APPSERVER_ADMIN_AGENT_GET_UPDATE_FAILED_ERROR	178
EventType: PH_APPSERVER_ADMIN_AGENT_UNKOWN_TASK_ID_ERROR	178
EventType: PH_APPSERVER_ADMIN_CUST_GENERATE_KEY_ERROR	178
EventType: PH_APPSERVER_ADMIN_GET_RESOURCE_FAILED	179
EventType: PH_APPSERVER_ADMIN_LOCATE_KEY_FAILED	179
EventType: PH_APPSERVER_ADMIN_RESET_FIELD_FAILED_ERROR	179
EventType: PH_APPSERVER_AUDIT_REPORT_EXPORT_ERROR	179
EventType: PH_APPSERVER_BEACON_LIB_ERROR	179
EventType: PH_APPSERVER_BEACON_REGISTER_ERROR	180
EventType: PH_APPSERVER_BEACON_SERVER_ERROR	180
EventType: PH_APPSERVER_BEACON_WEB_SERVER_ERROR	180
EventType: PH_APPSERVER_BEAN_REF_CHECK_WARN	180
EventType: PH_APPSERVER_BEAN_SYNC_PROPERTIES_ERROR	180
EventType: PH_APPSERVER_BEAN_TO_VALUE_ERROR	180
EventType: PH_APPSERVER_BEAN_TO_XML_ERROR	181
EventType: PH_APPSERVER_BEAN_VALUE_TO_BEAN_ERROR	181
EventType: PH_APPSERVER_CMDB_REPORT_DATA_ERROR	181
EventType: PH_APPSERVER_CMDB_REPORT_EXPORT_ERROR	181
EventType: PH_APPSERVER_CMDB_REPORT_IMPORT_ERROR	181
EventType: PH_APPSERVER_CMDB_REPORT_QUERY_ERROR	182
EventType: PH_APPSERVER_CMDB_REPORT_TYPE_ERROR	182
EventType: PH_APPSERVER_COLLECTOR_INFO_ERROR	182
EventType: PH_APPSERVER_COLLECTOR_LICENSE_ERROR	182
EventType: PH_APPSERVER_COLLECTOR_STATUS_ERROR	182
EventType: PH_APPSERVER_COMMONPWD_EXPORT_ERROR	182
EventType: PH_APPSERVER_DASHBOARD_DATA_ERROR	183
EventType: PH_APPSERVER_DASHBOARD_HTML_BUILD_XML_ERROR	183
EventType: PH_APPSERVER_DASHBOARD_WIDGET_ERROR	183
EventType: PH_APPSERVER_DATA_IMPORT_ERROR	183
EventType: PH_APPSERVER_DATA_ROBUST_INFO_ERROR	183
EventType: PH_APPSERVER_DB_CONNECTION_CLOSE_ERROR	184
EventType: PH_APPSERVER_DB_DATA_ERROR	184
EventType: PH_APPSERVER_DB_DELETE_ERROR	184
EventType: PH_APPSERVER_DB_QUERY_ERROR	184
EventType: PH_APPSERVER_DB_UPDATE_ERROR	184
EventType: PH_APPSERVER_DISCOVERY_CREDENTIAL_DECRYPT_	
PASSWORD_WARN	184
EventType: PH_APPSERVER_DISCOVERY_RESULT_ENCRYPT_XML_	
ELEMENT_ERROR	185
EventType: PH_APPSERVER_DISCOVERY_RESULT_ERROR	185
EventType: PH_APPSERVER_DISCOVERY_RESULT_UNKOWN_TASK_ID_	
ERROR	185
EventType: PH_APPSERVER_EAMIL_GENERATE_EVENT_ERROR	185

EventType: PH_APPSERVER_ELASTIC_UPDATE_ERROR	185
EventType: PH_APPSERVER_EMAIL_PREPARE_DATA_ERROR	186
EventType: PH_APPSERVER_EVENTDB_EXPORT_ERROR	186
EventType: PH_APPSERVER_EVENT_ATTRIBUTE_BUILD_XML_ERROR	186
EventType: PH_APPSERVER_EXPORT_ERROR	186
EventType: PH_APPSERVER_EXT_THREAT_INTEL_DOWNLOAD_ERROR	186
EventType: PH_APPSERVER_EXT_THREAT_INTEL_PARSE_ERROR	186
EventType: PH_APPSERVER_EXT_THREAT_INTEL_UPDATE_ERROR	187
EventType: PH_APPSERVER_FILE_NOT_FOUND	187
EventType: PH_APPSERVER_FILE_READ_ERROR	187
EventType: PH_APPSERVER_FILE_SYSTEM_ERROR	187
EventType: PH_APPSERVER_FILE_WRITE_ERROR	187
EventType: PH_APPSERVER_FLEX_INTERCEPTOR_NO_LOGIN_EXCEPTION_ERROR	188
EventType: PH_APPSERVER_FORTIGUARD_IOC_INTEGRATION_ERROR	188
EventType: PH_APPSERVER_FRAMEWORK_REGISTER_ERROR	188
EventType: PH_APPSERVER_FRAMEWORK_RUN_THREAD_ERROR	188
EventType: PH_APPSERVER_FRAMEWORK_SECURITY_CHECK_LICENSE_WARN	188
EventType: PH_APPSERVER_FRAMEWORK_SECURITY_GET_ENTITY_MANAGER_ERROR	189
EventType: PH_APPSERVER_FRAMEWORK_SECURITY_GET_RS_EXPIRATION_ERROR	189
EventType: PH_APPSERVER_FRAMEWORK_SECURITY_INIT_SYSTEM_ERROR	189
EventType: PH_APPSERVER_FRAMEWORK_SERVICE_MISSED_WARN	189
EventType: PH_APPSERVER_FRAMEWORK_SHUTDOWN_SERVICE_STARTER_WARN	189
EventType: PH_APPSERVER_GENERIC_ERROR	190
EventType: PH_APPSERVER_GENERIC_INFO	190
EventType: PH_APPSERVER_GENERIC_WARN	190
EventType: PH_APPSERVER_GET_MAX_CONFIG_ITEM_COUNT_ERROR	190
EventType: PH_APPSERVER_GROUP_DATA_ERROR	190
EventType: PH_APPSERVER_IDENTITYLOCATION_EXPORT_ERROR	190
EventType: PH_APPSERVER_INCIDENT_NOTIFY_ERROR	191
EventType: PH_APPSERVER_INCIDENT_UPDATE_ERROR	191
EventType: PH_APPSERVER_INTEGRATION_ERROR	191
EventType: PH_APPSERVER_INTEGRATION_UPDATE_POLICY_ERROR	191
EventType: PH_APPSERVER_INTEGRATION_UPDATE_POLICY_WARN	191
EventType: PH_APPSERVER_INTEGRATION_WARN	192
EventType: PH_APPSERVER_IN_INTEGRATION_ERROR	192
EventType: PH_APPSERVER_IOC_LICENSE_CHECK_FAILED_WARN	192
EventType: PH_APPSERVER_IOC_TASK_CREATE_FAILED_ERROR	192
EventType: PH_APPSERVER_JOB_DISTRIBUTE_ERROR	192
EventType: PH_APPSERVER_LICENSE_EXPIRY_ERROR	192
EventType: PH_APPSERVER_LICENSE_VALIDATION_ERROR	193
EventType: PH_APPSERVER_LOGIN_ERROR	193
EventType: PH_APPSERVER_LOG_INTEGRITY_ERROR	193
EventType: PH_APPSERVER_MONITOR_AUDIT_PERF_ERROR	193

EventType: PH_APPSERVER_MONITOR_HEALTH_CONFIG_SET_ERROR	193
EventType: PH_APPSERVER_NETSEGMENT_EXPORT_ERROR	194
EventType: PH_APPSERVER_NOTIFICATION_EMAIL_GET_RESOURCE_FAILED	194
EventType: PH_APPSERVER_NOTIFICATION_ERROR	194
EventType: PH_APPSERVER_NOTIFICATION_JMS_CONNECTION_ERROR	194
EventType: PH_APPSERVER_NOTIFICATION_UPDATE_ERROR	194
EventType: PH_APPSERVER_NOTIFIER_ERROR	194
EventType: PH_APPSERVER_NO_WATCHLIST_SELECTED_WARN	195
EventType: PH_APPSERVER_OPENPROXY_EXPORT_ERROR	195
EventType: PH_APPSERVER_OUT_INTEGRATION_ERROR	195
EventType: PH_APPSERVER_PARSER_IMPORT_ERROR	195
EventType: PH_APPSERVER_PARSER_UPDATE_ERROR	195
EventType: PH_APPSERVER_PARSING_CONSTRAINT_ERROR	196
EventType: PH_APPSERVER_PDF_BUILDER_ERROR	196
EventType: PH_APPSERVER_PERFMON_TASK_ERROR	196
EventType: PH_APPSERVER_QUERY_CHECK_POLICY_ACTION_WARN	196
EventType: PH_APPSERVER_QUERY_EXPORT_ERROR	196
EventType: PH_APPSERVER_QUERY_RESULT_PARSER_ERROR	196
EventType: PH_APPSERVER_QUERY_RESULT_RETRIEVE_ERROR	197
EventType: PH_APPSERVER_QUERY_RUN_ERROR	197
EventType: PH_APPSERVER_QUERY_STOP_ERROR	197
EventType: PH_APPSERVER_QUERY_STRING_ESCAPE_ERROR	197
EventType: PH_APPSERVER_RBAC_ERROR	197
EventType: PH_APPSERVER_RBAC_NO_PERMISSION_WARN	198
EventType: PH_APPSERVER_REALTIME_QUERY_ERROR	198
EventType: PH_APPSERVER_REMEDY_ERROR	198
EventType: PH_APPSERVER_REPORT_BUNDLE_PRINT_ERROR	198
EventType: PH_APPSERVER_REPORT_COMPILE_ERROR	198
EventType: PH_APPSERVER_REPORT_DEVICE_COMPONENT_SN_ERROR	198
EventType: PH_APPSERVER_REPORT_DEVICE_DETAIL_ERROR	199
EventType: PH_APPSERVER_REPORT_DEVICE_SN_ERROR	199
EventType: PH_APPSERVER_REPORT_DEVICE_SUMMARY_ERROR	199
EventType: PH_APPSERVER_REPORT_EXPORT_ERROR	199
EventType: PH_APPSERVER_REPORT_FAILED_BLOCK_SUMMARY_ERROR	199
EventType: PH_APPSERVER_REPORT_FIRE_TRIGGER_EVENT_ERROR	200
EventType: PH_APPSERVER_REPORT_GET_PH_CONFIG_ERROR	200
EventType: PH_APPSERVER_REPORT_IDENTITY_AND_LOCATION_ERROR	200
EventType: PH_APPSERVER_REPORT_LOG_FILE_SUMMARY_ERROR	200
EventType: PH_APPSERVER_REPORT_TEMPLATE_GENERATE_PDF_ERROR	200
EventType: PH_APPSERVER_REPORT_TEMPLATE_INIT_IMAGE_ERROR	200
EventType: PH_APPSERVER_REPORT_TEMPLATE_INIT_PARM_ERROR	201
EventType: PH_APPSERVER_REPORT_TEMPLATE_PDF_SUMMARY_ERROR	201
EventType: PH_APPSERVER_REPORT_TICKET_SUMMARY_ERROR	201
EventType: PH_APPSERVER_REPORT_UPDATE_ERROR	201
EventType: PH_APPSERVER_REPORT_USER_SUMMARY_ERROR	201
EventType: PH_APPSERVER_REST_ERROR	202
EventType: PH_APPSERVER_REST_H5_ERROR	202
EventType: PH_APPSERVER_RISKSCORE_CALCULATE_ERROR	202

EventType: PH_APPSERVER_RULE_ACTIVE_ERROR	202
EventType: PH_APPSERVER_RULE_CLONE_ERROR	202
EventType: PH_APPSERVER_RULE_DEBUG_INVALID_EVENT_DB_ID_ERROR	202
EventType: PH_APPSERVER_RULE_DEBUG_WORKERS_SETTING_ERROR	203
EventType: PH_APPSERVER_RULE_TEST_ERROR	203
EventType: PH_APPSERVER_RULE_UPDATE_ERROR	203
EventType: PH_APPSERVER_SCHEDULE_ERROR	203
EventType: PH_APPSERVER_SCHEDULE_UPDATE_ERROR	203
EventType: PH_APPSERVER_SECURITY_ERROR	204
EventType: PH_APPSERVER_SERVLET_ERROR	204
EventType: PH_APPSERVER_SERVLET_NO_ACCESS_TO_URI_WARN	204
EventType: PH_APPSERVER_SOCKET_COMM_ERROR	204
EventType: PH_APPSERVER_SVN_ERROR	204
EventType: PH_APPSERVER_SYNC_UPDATE_CONFIG_ERROR	204
EventType: PH_APPSERVER_SYSCONFIG_GET_ERROR	205
EventType: PH_APPSERVER_SYSTEM_WINAGENT_REGISTER_WARN	205
EventType: PH_APPSERVER_SYS_APPLICATION_ERROR	205
EventType: PH_APPSERVER_SYS_DATA_UPDATE_ERROR	205
EventType: PH_APPSERVER_TASK_CREATE_ERROR	205
EventType: PH_APPSERVER_TASK_FLEX_RESULT_BUILD_XML_ERROR	206
EventType: PH_APPSERVER_TASK_GET_ERROR	206
EventType: PH_APPSERVER_TASK_UPDATE_ERROR	206
EventType: PH_APPSERVER_TICKET_EXPORT_ERROR	206
EventType: PH_APPSERVER_UPDATER_FIND_EXIST_USER_BY_NOTHING_ERROR	206
EventType: PH_APPSERVER_USERAGENT_EXPORT_ERROR	206
EventType: PH_APPSERVER_VULNERABILITY_IGNORE_WARN	207
EventType: PH_APPSERVER_WATCHLIST_ADD_TO_DISTIRBUTED_QUEUE	207
EventType: PH_APPSERVER_WATCHLIST_EXPORT_ERROR	207
EventType: PH_APPSERVER_WATCHLIST_IMPORT_ERROR	207
EventType: PH_APPSERVER_WATCHLIST_IMPORT_WARN	207
EventType: PH_APPSERVER_WATCHLIST_UPDATE_ERROR	208
EventType: PH_APPSERVER_WEBSERVICE_UPDATE_TASK_ERROR	208
EventType: PH_APPSERVER_WORKER_PROVISION_FAILED	208
EventType: PH_APPSERVER_WS_COMM_ERROR	208
EventType: PH_APPSERVER_XML_PARSE_ERROR	208
EventType: PH_AUDIT_ACCOUNT_LOCKED	208
EventType: PH_AUDIT_AGENT_DISABLED	209
EventType: PH_AUDIT_AGENT_INSTALLED	209
EventType: PH_AUDIT_AGENT_NOTRESPONDING	210
EventType: PH_AUDIT_AGENT_RUNNING	210
EventType: PH_AUDIT_AGENT_STARTED	211
EventType: PH_AUDIT_AGENT_STOPPED	211
EventType: PH_AUDIT_AGENT_UNINSTALLED	212
EventType: PH_AUDIT_CASE_ASSIGNED	212
EventType: PH_AUDIT_CASE_CLOSED	213
EventType: PH_AUDIT_CASE_CREATED	213
EventType: PH_AUDIT_CASE_EVIDENCE_ADDED	214
EventType: PH_AUDIT_CASE_EVIDENCE_DELETED	214

EventType: PH_AUDIT_CASE_INCIDENT_ADDED	215
EventType: PH_AUDIT_CASE_MERGED	215
EventType: PH_AUDIT_CASE_NOTE_ADDED	216
EventType: PH_AUDIT_CASE_NOTE_DELETED	216
EventType: PH_AUDIT_CASE_NOTE_MODIFIED	216
EventType: PH_AUDIT_CASE_PRIORITY_CHANGED	217
EventType: PH_AUDIT_CASE_REASSIGNED	217
EventType: PH_AUDIT_CASE_STAGE_CHANGED	218
EventType: PH_AUDIT_CASE_STAT	218
EventType: PH_AUDIT_CASE_STATUS_CHANGED	219
EventType: PH_AUDIT_CASE_SUMMARY_CHANGED	219
EventType: PH_AUDIT_CASE_UPDATED	220
EventType: PH_AUDIT_CI_QUOTE_EXCEEDED	220
EventType: PH_AUDIT_CMDB_DISK_PRUNE_FAILED	220
EventType: PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS	221
EventType: PH_AUDIT_DASHBOARD_SHARED	221
EventType: PH_AUDIT_DATA_PURGE	221
EventType: PH_AUDIT_DB_LEADER_CHANGE	221
EventType: PH_AUDIT_DEFAULT_PWD_MATCH	222
EventType: PH_AUDIT_DEVICE_ADDED	222
EventType: PH_AUDIT_DEVICE_DELETED	223
EventType: PH_AUDIT_DEVICE_DISCOVERY_ITEM_CHANGED	223
EventType: PH_AUDIT_DEVICE_MAINTENANCE_ENDED	224
EventType: PH_AUDIT_DEVICE_MAINTENANCE_STARTED	224
EventType: PH_AUDIT_DEVICE_MERGED_BY_IP_WITH_DIFF_NAME	225
EventType: PH_AUDIT_DEVICE_STATUS_CHANGED	225
EventType: PH_AUDIT_DEVICE_UNMANAGED	226
EventType: PH_AUDIT_DEV_MON_JOB_NOT_STARTED	227
EventType: PH_AUDIT_DEV_MON_JOB_STATUS_CHANGE	227
EventType: PH_AUDIT_DISCOVERY	227
EventType: PH_AUDIT_EXPORT_REPORT_END	227
EventType: PH_AUDIT_GENAI_USER_QUERY	228
EventType: PH_AUDIT_GENERIC	228
EventType: PH_AUDIT_GROUP_CREATED	228
EventType: PH_AUDIT_GROUP_DELETED	228
EventType: PH_AUDIT_INACTIVE_USER_LOGIN	229
EventType: PH_AUDIT_INCIDENT_SYS_CLEAR	229
EventType: PH_AUDIT_INCIDENT_USER_CLEAR	229
EventType: PH_AUDIT_INTEGRATION_POLICY_EXECUTED	230
EventType: PH_AUDIT_MALWARE_DATA_DELETED	230
EventType: PH_AUDIT_MALWARE_DATA_UPDATED	231
EventType: PH_AUDIT_ML_GENERIC_ERROR	231
EventType: PH_AUDIT_ML_GENERIC_INFO	231
EventType: PH_AUDIT_ML_INFERENCE_COMPLETED	231
EventType: PH_AUDIT_ML_INFERENCE_RESULT	232
EventType: PH_AUDIT_ML_INFERENCE_STARTED	232
EventType: PH_AUDIT_ML_TRAINING_COMPLETED	232
EventType: PH_AUDIT_ML_TRAINING_STARTED	232
EventType: PH_AUDIT_NOTIF_POLICY_EXECUTED	232

EventType: PH_AUDIT_OBJECT_CREATED	233
EventType: PH_AUDIT_OBJECT_DELETED	233
EventType: PH_AUDIT_OBJECT_UPDATED	233
EventType: PH_AUDIT_ONDEMAND_REMEDIATION_EXECUTED	234
EventType: PH_AUDIT_PASSWORD_CHANGED	234
EventType: PH_AUDIT_QUERY_COMPLETED	235
EventType: PH_AUDIT_QUERY_SCHEDULED	235
EventType: PH_AUDIT_QUERY_START	236
EventType: PH_AUDIT_QUERY_STOP	236
EventType: PH_AUDIT_REPL_LEADER_CHANGE	236
EventType: PH_AUDIT_REPORT_SCHEDULED	237
EventType: PH_AUDIT_REPORT_SCHEDULE_APPROVE	237
EventType: PH_AUDIT_REPORT_SCHEDULE_REQUEST	238
EventType: PH_AUDIT_REPORT_SERVER_LICENSE_EXPIRED	238
EventType: PH_AUDIT_REPORT_SERVER_LICENSE_REMOVED	238
EventType: PH_AUDIT_REPORT_SERVER_LICENSE_TO_EXPIRE	239
EventType: PH_AUDIT_RISK_DECREASE_LOW	239
EventType: PH_AUDIT_RISK_DECREASE_MED	239
EventType: PH_AUDIT_RISK_INCREASE_HIGH	239
EventType: PH_AUDIT_RISK_INCREASE_MED	239
EventType: PH_AUDIT_RULE_ACTIVATED	239
EventType: PH_AUDIT_RULE_ACTIVATION_APPROVE	240
EventType: PH_AUDIT_RULE_ACTIVATION_REQUEST	240
EventType: PH_AUDIT_RULE_DEACTIVATED	241
EventType: PH_AUDIT_RULE_DEACTIVATION_APPROVE	241
EventType: PH_AUDIT_RULE_DEACTIVATION_REQUEST	242
EventType: PH_AUDIT_SVC_LOGIN_FAILURE	242
EventType: PH_AUDIT_SVC_LOGIN_SUCCESS	242
EventType: PH_AUDIT_SVC_LOGOFF	242
EventType: PH_AUDIT_SVC_SESSION_TIMEOUT	243
EventType: PH_AUDIT_TUNNEL_CLOSE	243
EventType: PH_AUDIT_TUNNEL_OPEN	243
EventType: PH_AUDIT_USER_ADDED	244
EventType: PH_AUDIT_USER_CHANGE_ORG_SCOPE	244
EventType: PH_AUDIT_USER_DEFAULT_ROLE_CHANGED	245
EventType: PH_AUDIT_USER_DELETED	245
EventType: PH_AUDIT_USER_LOGIN_FAILURE	246
EventType: PH_AUDIT_USER_LOGIN_SUCCESS	246
EventType: PH_AUDIT_USER_LOGOFF	247
EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_CHANGED	247
EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_ENABLED	247
EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_REMOVED	248
EventType: PH_AUDIT_USER_SESSION_TIMEOUT	248
EventType: PH_AUDIT_WS_COMM	248
Data Manager Logs	250
EventType: PH_CLICKHOUSE_CHECKIN_QUERY_THREADS_FAILED	256
EventType: PH_CLICKHOUSE_CHECKOUT_QUERY_THREADS_FAILED	257
EventType: PH_CLICKHOUSE_DISK_UTILS_PER_STORAGE_TIER	257
EventType: PH_CLICKHOUSE_DROP_PARTITION_FAILED	257

EventType: PH_CLICKHOUSE_DROP_PARTITION_STARTED	258
EventType: PH_CLICKHOUSE_DROP_PARTITION_SUCCEEDED	258
EventType: PH_CLICKHOUSE_GET_ONLINE_NODE_FAILED	259
EventType: PH_CLICKHOUSE_GET_PARTITIONS_FAILED	259
EventType: PH_CLICKHOUSE_GET_SHARDS_FAILED	259
EventType: PH_CLICKHOUSE_GET_STORAGE_STATS_FAILED	260
EventType: PH_CLICKHOUSE_GET_STORAGE_TIER_FAILED	260
EventType: PH_CLICKHOUSE_INSERTION_DROP_EVENTS	260
EventType: PH_CLICKHOUSE_INSERTION_EPS	261
EventType: PH_CLICKHOUSE_JSON_ENCODER_EPS	261
EventType: PH_CLICKHOUSE_JSON_ENCODER_EPS_PER_THREAD	261
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_ACTIVE_CONSOLIDATION	262
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CALCULATE_REQUEST_	
PARSE_FAILED	262
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CALCULATE_REQUEST_	
STARTED	262
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CANDIDATE_PARTITIONS	262
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CONSOLIDATION_DATE	262
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CONSOLIDATION_STATUS_	
CHANGE	263
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_	
DONE	263
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_	
STARTED	263
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_	
STOPPED	264
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_	
TIMER	264
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DB_QUERY_FAILED	264
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_EMPTY_PARTITION_	
CHECKSUM	264
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_EXEC_FAILED	265
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_MIN_MAX_QUERY_FAILED	265
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_OPTIMIZE_COMMAND_	
FAILED	265
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_	
CONSOLIDATION_DONE	266
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_	
CONSOLIDATION_STARTED	266
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_UPDATED_	
AFTER_CHECKSUM	267
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_MISMATCH	267
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_MISMATCH_	
REPLICAS	268
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_PARTITION_INFO_	
EMPTY	268
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_REQUEST_PARSE_	
FAILED	269
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_EMPTY	269

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_ERROR	269
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_PARSE_FAILED	269
EventType: PH_CLICKHOUSE_MOVE_PARTITION_FAILED	270
EventType: PH_CLICKHOUSE_MOVE_PARTITION_STARTED	270
EventType: PH_CLICKHOUSE_MOVE_PARTITION_SUCCEEDED	270
EventType: PH_CLICKHOUSE_NOT_REACHABLE	271
EventType: PH_CLICKHOUSE_QUERY_REDIS_CONN_FAILURE	271
EventType: PH_CLICKHOUSE_QUERY_REDIS_GET_FAILURE	271
EventType: PH_CLICKHOUSE_QUERY_UNCOMPRESS_FAILURE	272
EventType: PH_CLICKHOUSE_QUERY_ZLIB_INIT_FAILURE	272
EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_QUERY_CHECKIN	272
EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_QUERY_CHECKOUT	272
EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_THREADS_CHECKIN	273
EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_THREADS_CHECKOUT	273
EventType: PH_CLICKHOUSE_ROUND_ROBIN_INSERTION	274
EventType: PH_CLICKHOUSE_ROUND_ROBIN_QUERY	274
EventType: PH_CLICKHOUSE_STORAGE_FREE_SPACE_CRITICAL	274
EventType: PH_CLICKHOUSE_STORAGE_FREE_SPACE_LOW	275
EventType: PH_CLICKHOUSE_STORAGE_UTILS_PER_ORG_PER_DAY	275
EventType: PH_CLICKHOUSE_WRITE_FAILED	275
EventType: PH_CLUSTER_COLLECT_ALL_IP_FAILED	276
EventType: PH_CLUSTER_COLLECT_CONFIG_DATA_FAILED	276
EventType: PH_CLUSTER_CONFIG_SSH_KEY_FAILED	276
EventType: PH_CLUSTER_GET_FW_IP_FAILED	276
EventType: PH_CLUSTER_GET_TASK_FAILED	276
EventType: PH_CLUSTER_NOT_SUPPORT_TASK	277
EventType: PH_CLUSTER_NOT_VALID_FELLOWER	277
EventType: PH_CLUSTER_RELOAD_CONFIG_FAILED	277
EventType: PH_CLUSTER_RM_DB_FAILED	277
EventType: PH_CLUSTER_RUN_COMMAND_FAILED	277
EventType: PH_CLUSTER_SCIRPT_FAILED	278
EventType: PH_CLUSTER_SEND_TASK_FAILED	278
EventType: PH_CLUSTER_SSH_KEY_IS_WRONG	278
EventType: PH_CLUSTER_TASK_DATA_EMPTY	278
EventType: PH_CLUSTER_TASK_INFO_IS_WRONG	279
EventType: PH_CLUSTER_TASK_NOT_CONTAIN_LIC	279
EventType: PH_CLUSTER_UPDATE_CONFIG_ERROR	279
EventType: PH_DATAINTEGRITY_PASSPHRASE_LOAD_ERROR	279
EventType: PH_DATAINTEGRITY_SIGNER_ERROR	280
EventType: PH_DATAINTEGRITY_UTILS_ERROR	280
EventType: PH_DATAINTEGRITY_VERIFIER_ERROR	280
EventType: PH_DATAMANAGER_CLICKHOUSE_HTTP_UPLOAD_ERROR	281
EventType: PH_DATAMANAGER_CLUSTER_ENCODE_ERROR	281
EventType: PH_DATAMANAGER_CLUSTER_INIT_ERROR	281
EventType: PH_DATAMANAGER_CLUSTER_WAIT_ERROR	282
EventType: PH_DATAMANAGER_CLUSTER_WRITER_ERROR	282
EventType: PH_DATAMANAGER_DASHBOARD_RESPONSE_ERROR	282
EventType: PH_DATAMANAGER_ELASTICWRITER_ERROR	283

EventType: PH_DATAMANAGER_EVTATTR_ERROR	283
EventType: PH_DATAMANAGER_EVTCACHE_DUPLICATE_ERROR	283
EventType: PH_DATAMANAGER_EVTCACHE_GET_ERROR	283
EventType: PH_DATAMANAGER_EVTCACHE_PARSE_ERROR	284
EventType: PH_DATAMANAGER_EVTDBNOTIFIER_ERROR	284
EventType: PH_DATAMANAGER_EVTIDX_CORRUPT_ERROR	284
EventType: PH_DATAMANAGER_EVTIDX_MERGE_ERROR	285
EventType: PH_DATAMANAGER_EVTIDX_QUERY_ERROR	285
EventType: PH_DATAMANAGER_EVTIDX_READ_BLOCK_ERROR	285
EventType: PH_DATAMANAGER_EVTIDX_READ_KEY_ERROR	286
EventType: PH_DATAMANAGER_EVTIDX_READ_POST_ERROR	286
EventType: PH_DATAMANAGER_EVTIDX_WRITE_ERROR	286
EventType: PH_DATAMANAGER_EVTIDX_WRITE_KEY_ERROR	287
EventType: PH_DATAMANAGER_EVTIDX_WRITE_POST_ERROR	287
EventType: PH_DATAMANAGER_EVTLOADER_ERROR	287
EventType: PH_DATAMANAGER_EVTWRITER_ERROR	288
EventType: PH_DATAMANAGER_EXPORT_ERROR	288
EventType: PH_DATAMANAGER_FILE_READ_FAILURE	288
EventType: PH_DATAMANAGER_FILE_RENAME_FAILURE	289
EventType: PH_DATAMANAGER_FILE_SIGN_ERROR	289
EventType: PH_DATAMANAGER_FILE_WRITE_FAILURE	289
EventType: PH_DATAMANAGER_GET_SIGN_ERROR	290
EventType: PH_DATAMANAGER_GLOBAL_CACHE_MISSING	290
EventType: PH_DATAMANAGER_HDFSWRITER_ERROR	290
EventType: PH_DATAMANAGER_HTTP_UPLOAD_ERROR	290
EventType: PH_DATAMANAGER_INIT_ERROR	291
EventType: PH_DATAMANAGER_INTEGRITY_CHECK_ERROR	291
EventType: PH_DATAMANAGER_INTEGRITY_RESPONSE_ERROR	291
EventType: PH_DATAMANAGER_INVALID_LOG_FILE	292
EventType: PH_DATAMANAGER_IP_TYPE_INVALID	292
EventType: PH_DATAMANAGER_KAFKAWRITER_CONFIG_ERROR	292
EventType: PH_DATAMANAGER_KAFKAWRITER_ERROR	293
EventType: PH_DATAMANAGER_LOG_BUFFER_PAUSED_LOW_SPACE	293
EventType: PH_DATAMANAGER_LOG_BUFFER_PAUSED_STATFS_FAILURE	293
EventType: PH_DATAMANAGER_LOG_BUFFER_RESUMED	293
EventType: PH_DATAMANAGER_PUT_SIGN_ERROR	293
EventType: PH_DATAMANAGER_QUERY_EXPR_ERROR	294
EventType: PH_DATAMANAGER_QUERY_RESPONSE_ERROR	294
EventType: PH_DATAMANAGER_REDIS_KEY_NOT_EXIST	294
EventType: PH_DATAMANAGER_SUMMARYWRITER_ERROR	295
EventType: PH_DATAMGR_BAD_EVTBLKIDX_FILE	295
EventType: PH_DATAMGR_BAD_SEGMENT	295
EventType: PH_DATAMGR_INDEX_MERGE_FAILED	295
EventType: PH_DATAMGR_INDEX_MERGE_FAILED_INDEX	295
EventType: PH_DATAMGR_INDEX_MERGE_FAILED_INDEX_GROUP	296
EventType: PH_DATAMGR_SEGMENT_MERGE_ERROR	296
EventType: PH_DATAMGR_SEGMENT_MERGE_FAILED	296
EventType: PH_DATAMGR_UNABLE_FLUSH_INDEX	296
EventType: PH_DATAMGR_UNABLE_OPEN_EVTBLK_FILE	296

EventType: PH_DATAPURGER_ARCHIVE_TASK_ERROR	297
EventType: PH_DATAPURGER_CMD_FAILURE	297
EventType: PH_DATAPURGER_DR_ES_RESTORE_FAILED	297
EventType: PH_DATAPURGER_DR_ES_ROLE_UNKNOWN	298
EventType: PH_DATAPURGER_DR_ES_SNAPSHOTS_GET_FAILED	298
EventType: PH_DATAPURGER_DR_ES_SNAPSHOT_DELETION_FAILED	298
EventType: PH_DATAPURGER_DR_ES_SNAPSHOT_FAILED	298
EventType: PH_DATAPURGER_DUCHECKER_ERROR	299
EventType: PH_DATAPURGER_ENFORCE_ERROR	299
EventType: PH_DATAPURGER_EVAL_ERROR	299
EventType: PH_DATAPURGER_HTTP_UPLOAD_ERROR	300
EventType: PH_DATAPURGER_INIT_ERROR	300
EventType: PH_DATAPURGER_OPEN_FILE_ERROR	300
EventType: PH_DATAPURGER_PARSE_XML_ERROR	301
EventType: PH_DATAPURGER_POLICY_ERROR	301
EventType: PH_DATAPURGER_RESPONSE_ERROR	301
EventType: PH_DATAPURGER_STORAGE_POLICY_CLICKHOUSE_NODES_EMPTY	301
EventType: PH_DATA_CLUSTER_ALL_COORDINATOR_DOWN	302
EventType: PH_DATA_CLUSTER_BUSY	302
EventType: PH_DATA_CLUSTER_CLICKHOUSE_CONFIG_NO_PORT	302
EventType: PH_DATA_CLUSTER_COORDINATOR_DOWN	303
EventType: PH_DATA_CLUSTER_COORDINATOR_UP	303
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_HTTPPORT	303
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_IP	303
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_JAVAPORT	304
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NAME	304
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NUMREPLICAS	304
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NUMSHARD	304
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NULL	304
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_WRONG_FORMAT	305
EventType: PH_DATA_CLUSTER_ELASTIC_EVENTID_NOT_FOUND	305
EventType: PH_DATA_CLUSTER_ELASTIC_HTTP_CLIENT_FAIL	305
EventType: PH_DATA_CLUSTER_ELASTIC_HTTP_CMD_FAIL	305
EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_FAIL	306
EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_RESEND_FAIL	306
EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FAIL	306
EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FIRST_FAIL	307
EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_UPLOAD_FAIL	307
EventType: PH_DATA_CLUSTER_ELASTIC_WRONG_JSON_FORMAT	307
EventType: PH_DATA_CLUSTER_GET_HOSTNAME_FAIL	308
EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_PORT	308
EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_SERVER	308
EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_YARN_PORT	308
EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_YARN_SERVER	308
EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NULL	308
EventType: PH_DATA_CLUSTER_HDFS_HTTP_CMD_FAIL	309
EventType: PH_DATA_CLUSTER_HDFS_LISTSTATUS_FAIL	309
EventType: PH_DATA_CLUSTER_HDFS_SEND_FAIL	309

EventType: PH_DATA_CLUSTER_HDFS_UPLOAD_FAIL	310
EventType: PH_DATA_CLUSTER_JSON_GET_ATTRIBUTE_NAME_FAIL	310
EventType: PH_ES_ARCHIVE_STORAGE_CHECK_ERROR	310
EventType: PH_ES_ARCHIVE_STORAGE_LOW	310
EventType: PH_ES_ARCHIVE_STORAGE_PURGING_FAILED	311
EventType: PH_ES_ARCHIVE_STORAGE_PURGING_FINISHED	311
EventType: PH_ES_ARCHIVE_STORAGE_PURGING_STARTED	311
EventType: PH_ES_ARCHIVE_STORAGE_PURGING_SUCCESS	312
EventType: PH_ES_ARCHIVE_STORAGE_USAGE	312
EventType: PH_ES_CCR_DELAY	312
EventType: PH_ES_COLD_STORAGE_ARCHIVING_FAILED	313
EventType: PH_ES_COLD_STORAGE_ARCHIVING_FINISHED	313
EventType: PH_ES_COLD_STORAGE_ARCHIVING_STARTED	313
EventType: PH_ES_COLD_STORAGE_ARCHIVING_SUCCESS	313
EventType: PH_ES_COLD_STORAGE_CHECK_ERROR	314
EventType: PH_ES_COLD_STORAGE_LOW	314
EventType: PH_ES_COLD_STORAGE_PURGING_FAILED	314
EventType: PH_ES_COLD_STORAGE_PURGING_FINISHED	315
EventType: PH_ES_COLD_STORAGE_PURGING_STARTED	315
EventType: PH_ES_COLD_STORAGE_PURGING_SUCCESS	315
EventType: PH_ES_COLD_STORAGE_USAGE	316
EventType: PH_ES_HOTCOLD_STORAGE_MOVING_FAILED	316
EventType: PH_ES_HOTCOLD_STORAGE_MOVING_FINISHED	316
EventType: PH_ES_HOTCOLD_STORAGE_MOVING_STARTED	316
EventType: PH_ES_HOTCOLD_STORAGE_MOVING_SUCCESS	317
EventType: PH_ES_HOT_STORAGE_ARCHIVING_FAILED	317
EventType: PH_ES_HOT_STORAGE_ARCHIVING_FINISHED	317
EventType: PH_ES_HOT_STORAGE_ARCHIVING_STARTED	318
EventType: PH_ES_HOT_STORAGE_ARCHIVING_SUCCESS	318
EventType: PH_ES_HOT_STORAGE_CHECK_ERROR	318
EventType: PH_ES_HOT_STORAGE_LOW	319
EventType: PH_ES_HOT_STORAGE_MOVING_FAILED	319
EventType: PH_ES_HOT_STORAGE_MOVING_FINISHED	319
EventType: PH_ES_HOT_STORAGE_MOVING_STARTED	320
EventType: PH_ES_HOT_STORAGE_MOVING_SUCCESS	320
EventType: PH_ES_HOT_STORAGE_PURGING_FAILED	320
EventType: PH_ES_HOT_STORAGE_PURGING_FINISHED	320
EventType: PH_ES_HOT_STORAGE_PURGING_STARTED	321
EventType: PH_ES_HOT_STORAGE_PURGING_SUCCESS	321
EventType: PH_ES_HOT_STORAGE_USAGE	322
EventType: PH_ES_INDEX_SEGMENT_MERGE_FAILED	322
EventType: PH_ES_REST_FAILED	322
EventType: PH_ES_SM_ADD_INDEX_FAILED	322
EventType: PH_ES_SM_HOURLCHECK_FAILED	323
EventType: PH_ES_SM_INIT_FAILED	323
EventType: PH_ES_SM_INIT_INDEX_FAILED	323
EventType: PH_ES_SNAPSHOT_FAILED	323
EventType: PH_ES_TO_NFS_ARCHIVE_FAILED_ADD_INDEX	323
EventType: PH_ES_WARM_STORAGE_ARCHIVING_FAILED	323

EventType: PH_ES_WARM_STORAGE_ARCHIVING_FINISHED	324
EventType: PH_ES_WARM_STORAGE_ARCHIVING_STARTED	324
EventType: PH_ES_WARM_STORAGE_ARCHIVING_SUCCESS	324
EventType: PH_ES_WARM_STORAGE_CHECK_ERROR	325
EventType: PH_ES_WARM_STORAGE_LOW	325
EventType: PH_ES_WARM_STORAGE_MOVING_FAILED	325
EventType: PH_ES_WARM_STORAGE_MOVING_FINISHED	326
EventType: PH_ES_WARM_STORAGE_MOVING_STARTED	326
EventType: PH_ES_WARM_STORAGE_MOVING_SUCCESS	326
EventType: PH_ES_WARM_STORAGE_PURGING_FAILED	327
EventType: PH_ES_WARM_STORAGE_PURGING_FINISHED	327
EventType: PH_ES_WARM_STORAGE_PURGING_STARTED	327
EventType: PH_ES_WARM_STORAGE_PURGING_SUCCESS	327
EventType: PH_ES_WARM_STORAGE_USAGE	328
EventType: PH_HDFS_ARCHIVE_STORAGE_LOW	328
EventType: PH_HDFS_ARCHIVE_STORAGE_USAGE	328
EventType: PH_HDFS_PURGING_FAILED	329
EventType: PH_HDFS_PURGING_FINISHED	329
EventType: PH_HDFS_PURGING_STARTED	329
EventType: PH_HDFS_PURGING_SUCCESS	330
EventType: PH_SYSTEM_ARCHIVE_LOW	330
EventType: PH_SYSTEM_ARCHIVE_PURGED_LOW_SPACE	330
EventType: PH_SYSTEM_ARCHIVE_PURGED_POLICY	331
EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_FAILED	331
EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_FINISHED	331
EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_STARTED	331
EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_SUCCESS	331
EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_FAILED	331
EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_FINISHED	332
EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_STARTED	332
EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_SUCCESS	332
EventType: PH_SYSTEM_ARCHIVE_RETENTION_POLICY_VIOLATED	332
EventType: PH_SYSTEM_ARCHIVE_USAGE	333
EventType: PH_SYSTEM_DATAMGR_ARCHIVE_SKIP	333
EventType: PH_SYSTEM_DISK_ARCHIVING_FAILED	333
EventType: PH_SYSTEM_DISK_ARCHIVING_FINISHED	333
EventType: PH_SYSTEM_DISK_ARCHIVING_STARTED	334
EventType: PH_SYSTEM_DISK_ARCHIVING_SUCCESS	334
EventType: PH_SYSTEM_DISK_PURGED	334
EventType: PH_SYSTEM_DISK_PURGING_FAILED	334
EventType: PH_SYSTEM_DISK_PURGING_FINISHED	334
EventType: PH_SYSTEM_DISK_PURGING_STARTED	335
EventType: PH_SYSTEM_DISK_PURGING_SUCCESS	335
EventType: PH_SYSTEM_DISK_USAGE	335
EventType: PH_SYSTEM_DISK_USAGE_WARNING	335
EventType: PH_SYSTEM_ONLINE_RETENTION_POLICY_VIOLATED	336
EventType: PH_SYSTEM_RETENTION_POLICY_EXEC_TIME	336
EventType: PH_SYSTEM_RETENTION_POLICY_FAILED	336
EventType: PH_SYSTEM_RETENTION_POLICY_FINISHED	337

EventType: PH_SYSTEM_RETENTION_POLICY_STARTED	337
EventType: PH_SYSTEM_RETENTION_POLICY_STATS	337
EventType: PH_SYSTEM_RETENTION_POLICY_SUCCESS	337
Discovery Logs	338
EventType: PH_DEVICE_NOT_ADDED	344
EventType: PH_DISCOVERY_COMPLETE	344
EventType: PH_DISCOVERY_RESULT_SENT	344
EventType: PH_DISCOV_ACCESS_IP_PARSE_ERROR	344
EventType: PH_DISCOV_ADS_ACCOUNT_TO_EXPIRE	345
EventType: PH_DISCOV_ADS_ACCT_DISABLED	345
EventType: PH_DISCOV_ADS_DORMANT_ACCT	345
EventType: PH_DISCOV_ADS_PASSWORD_NEVER_EXPIRES	346
EventType: PH_DISCOV_ADS_PASSWORD_NOT_REQD	346
EventType: PH_DISCOV_ADS_PASSWORD_STALE	347
EventType: PH_DISCOV_ADS_PASSWORD_TO_EXPIRE	347
EventType: PH_DISCOV_ARUBA_WLAN_HOST_LOCATION	348
EventType: PH_DISCOV_AWS_DEVICE_DELETED	349
EventType: PH_DISCOV_AWS_DEVICE_UNKNOWN	349
EventType: PH_DISCOV_AWS_DISCOV_FAILED	349
EventType: PH_DISCOV_AZURE_DISCOV_FAILED	350
EventType: PH_DISCOV_BASIC_FAILED	350
EventType: PH_DISCOV_BASIC_SKIPPED	350
EventType: PH_DISCOV_BASIC_SNMP_DETAIL	351
EventType: PH_DISCOV_BASIC_SNMP_ERROR	351
EventType: PH_DISCOV_BASIC_SNMP_FAILED	351
EventType: PH_DISCOV_BASIC_SNMP_STARTED	352
EventType: PH_DISCOV_BASIC_SNMP_SUCCESS	352
EventType: PH_DISCOV_BASIC_SSH_DETAIL	353
EventType: PH_DISCOV_BASIC_SSH_ERROR	353
EventType: PH_DISCOV_BASIC_SSH_FAILED	353
EventType: PH_DISCOV_BASIC_SSH_STARTED	354
EventType: PH_DISCOV_BASIC_SSH_SUCCESS	354
EventType: PH_DISCOV_BASIC_STARTED	354
EventType: PH_DISCOV_BGP_OSPF_FAILED	355
EventType: PH_DISCOV_BROCADE_SERVER_IRON_HW_INFO_WARNING	355
EventType: PH_DISCOV_CANCEL_UNKNOWN_REQ	355
EventType: PH_DISCOV_CERT_FILE_DOWNLOAD_FAILURE	355
EventType: PH_DISCOV_CHECKPOINT_TEST_CONN_FAILED	356
EventType: PH_DISCOV_CISCO_ASA_GET_CONTEXT_FAILED	356
EventType: PH_DISCOV_CISCO_ASA_IPSEC_VPN_FAILED	356
EventType: PH_DISCOV_CISCO_ASA_RAS_VPN_FAILED	357
EventType: PH_DISCOV_CISCO_ASA_RUN_CONFIG_FAILED	357
EventType: PH_DISCOV_CISCO_ASA_SET_CONTEXT_FAILED	357
EventType: PH_DISCOV_CISCO_ASA_STARTUP_CONFIG_FAILED	358
EventType: PH_DISCOV_CISCO_CALL_MANAGER_WARNING	358
EventType: PH_DISCOV_CISCO_CATOS_INTF_FAILED	359
EventType: PH_DISCOV_CISCO_CDP_ERROR	359
EventType: PH_DISCOV_CISCO_IOS_L2_WARNING	359
EventType: PH_DISCOV_CISCO_IOS_TRUNK_PORT_ERROR	360

EventType: PH_DISCOV_CISCO_JUNOS_L2_WARNING	360
EventType: PH_DISCOV_CISCO_NXOS_HW_STATUS_WARNING	360
EventType: PH_DISCOV_CISCO_NXOS_INTF_SHORT_NAME_NOT_FOUND	361
EventType: PH_DISCOV_CISCO_NXOS_L2_WARNING	361
EventType: PH_DISCOV_CISCO_WLAN_HOST_LOCATION	361
EventType: PH_DISCOV_CLOCK_ROLLS_BACK	362
EventType: PH_DISCOV_CONTACT_APP_SERVER	362
EventType: PH_DISCOV_CREDEN_INSERT_ERROR	363
EventType: PH_DISCOV_CUSTOM_MAP_LOAD_FAILED	363
EventType: PH_DISCOV_DATA_DOMAIN_HW_STATUS_WARNING	363
EventType: PH_DISCOV_DELL_BLADE_CHASSIS_WARNING	364
EventType: PH_DISCOV_DELL_COMPELLENT_STORAGE_WARNING	364
EventType: PH_DISCOV_DISCOV_REQ_GET_FAILED	364
EventType: PH_DISCOV_DISCOV_RESULT_SENDER_THREADS_SPAWN_FAILED	364
EventType: PH_DISCOV_DISCOV_THREADS_SPAWN_FAILED	365
EventType: PH_DISCOV_EC2_INSTANCE_PARSE_FAILED	365
EventType: PH_DISCOV EMC_CLARION_ERROR	365
EventType: PH_DISCOV EMC_VNX_DISCOV_FAILED	365
EventType: PH_DISCOV EMC_VNX_PING_FAILED	366
EventType: PH_DISCOV_EQLOGIC_CONN_FAILED	366
EventType: PH_DISCOV_EQLOGIC_HW_INFO_FAILED	367
EventType: PH_DISCOV_ESX_HOST_PING_ONLY_DISCOV_ERROR	367
EventType: PH_DISCOV_FAILED_INVALID_REQUEST	367
EventType: PH_DISCOV_FAILED_INVALID_REQUEST_XML	368
EventType: PH_DISCOV_FAILED_XML_ERROR	368
EventType: PH_DISCOV_FAIL_CMDB_DEV	368
EventType: PH_DISCOV_FILE_BASED_DISCOV_DIR_NOT_CONFIGURED	368
EventType: PH_DISCOV_FILE_BASED_DISCOV_FAILED	369
EventType: PH_DISCOV_FORTINET_CPU_INFO_WARNING	369
EventType: PH_DISCOV_FORTINET_LINK_STAT_WARNING	369
EventType: PH_DISCOV_FORTINET_SYS_UPDATE_VERSION_WARNING	370
EventType: PH_DISCOV_GENERIC_ERROR	370
EventType: PH_DISCOV_GEN_WLAN_HOST_LOCATION	370
EventType: PH_DISCOV_GET_SNMP_ENGINE_ID_FAILED	371
EventType: PH_DISCOV_HOST_CONVERT_PROCESS_UPTIME_ERROR	371
EventType: PH_DISCOV_HOST_ERROR	372
EventType: PH_DISCOV_HOST_INSTALL_SW_WARNING	372
EventType: PH_DISCOV_HOST_LOCATE_PROCESS_ERROR	372
EventType: PH_DISCOV_HOST_LOCATION	373
EventType: PH_DISCOV_HOST_NET_INTF	373
EventType: PH_DISCOV_HOST_STARTED	373
EventType: PH_DISCOV_HOST_SUCCESS	374
EventType: PH_DISCOV_HOST_SUCCESS_DETAIL	374
EventType: PH_DISCOV_HOST_WARNING	375
EventType: PH_DISCOV_HP3COM_HW_WARNING	375
EventType: PH_DISCOV_HP_BLADE_HW_STATUS_WARNING	375
EventType: PH_DISCOV_INIT_MODULE_FAILED	376
EventType: PH_DISCOV_INTERFACE_VIA_SNMP_FAILED	376

EventType: PH_DISCOV_IP_TYPE_INVALID	376
EventType: PH_DISCOV_ISILON_HW_STATUS_WARNING	376
EventType: PH_DISCOV_JMX_TEST_CONN_FAILED	377
EventType: PH_DISCOV_JUNIPER_SSG_HW_INFO_WARNING	377
EventType: PH_DISCOV_L2_FAILED	378
EventType: PH_DISCOV_L2_STARTED	378
EventType: PH_DISCOV_L2_SUCCESS	378
EventType: PH_DISCOV_LDAP_ERROR	379
EventType: PH_DISCOV_LDAP_OU_ERROR	379
EventType: PH_DISCOV_LINUX_DSKTABLE_NOT_CONFIG	379
EventType: PH_DISCOV_LOGIN_ERROR	380
EventType: PH_DISCOV_NEXT_HOP_VIA_SNMP_FAILED	380
EventType: PH_DISCOV_NIMBLE_VOLUME_WARNING	381
EventType: PH_DISCOV_NOZOMI_DISCOV_FAILED	381
EventType: PH_DISCOV_PARAM_PARSE_FAILED	381
EventType: PH_DISCOV_PARSER_MSG_EXCEEDS_THRESHOLD	382
EventType: PH_DISCOV_PARSER_MSG_THREAD_SPAWN_FAILED	382
EventType: PH_DISCOV_PERF_TEMPLATE_LOAD_FAILED	382
EventType: PH_DISCOV_PING_ONLY_LIST_NOT_MATCH	382
EventType: PH_DISCOV_READ_COMPRESS_THRESHOLD_FAILED	382
EventType: PH_DISCOV_RECVD_VALID_REQUEST	383
EventType: PH_DISCOV_RESULT_SEND_FAILED	383
EventType: PH_DISCOV_RESULT_SEND_WARNING	383
EventType: PH_DISCOV_RESULT_XML_WRITE_FAILURE	383
EventType: PH_DISCOV_RUNNING_SERVICE	384
EventType: PH_DISCOV_RUN_JAVA_PROBE_ERROR	384
EventType: PH_DISCOV_RUN_SW_FILTER_LOAD_FAILED	385
EventType: PH_DISCOV_RUN_SW_FILTER_PARSE_FAILED	385
EventType: PH_DISCOV_RUN_VM_TEST_CONN_ERROR	385
EventType: PH_DISCOV_SKIPPED	385
EventType: PH_DISCOV_SKIP_DEV	385
EventType: PH_DISCOV_SNMP_ERROR	386
EventType: PH_DISCOV_SSH_ERROR	386
EventType: PH_DISCOV_START	387
EventType: PH_DISCOV_TELNET_ERROR	387
EventType: PH_DISCOV_TEST_CONN_GET_REQ_FAILED	387
EventType: PH_DISCOV_TEST_CONN_MSRPC_ERROR	387
EventType: PH_DISCOV_TEST_CONN_NO_UCSAPI_CRED	388
EventType: PH_DISCOV_TEST_CONN_RESULT_SENDER_THREADS_SPAWN_FAILED	388
EventType: PH_DISCOV_TEST_CONN_RESULT_SEND_ERROR	388
EventType: PH_DISCOV_TEST_CONN_RESULT_SEND_WARNING	388
EventType: PH_DISCOV_TEST_CONN_THREADS_SPAWN_FAILED	389
EventType: PH_DISCOV_TEST_CONN_VMSDK_ERROR	389
EventType: PH_DISCOV_TRIPP_UPS_HW_STATUS_WARNING	389
EventType: PH_DISCOV_TRUNK_PORTS_ERROR	390
EventType: PH_DISCOV_UNHANDLED_ACCESS_PROTO	390
EventType: PH_DISCOV_UPLOAD_DATA_FAILED	390
EventType: PH_DISCOV_VMWARE_DUP_DEV_ID	390

EventType: PH_DISCOV_VMWARE_ERROR	390
EventType: PH_DISCOV_VOIP_PHONE_ID	391
EventType: PH_DISCOV_WMI_PULL_ERROR	391
EventType: PH_LIB_TOPO_APACHE_PING_FAILED	391
EventType: PH_LIB_TOPO_APP_GROUP_FILTER_PARSE_ERROR	392
EventType: PH_LIB_TOPO_APP_GROUP_FILTER_PUSH_ERROR	392
EventType: PH_LIB_TOPO_AWS_NEW_INSTANCE_NOT_RUN	392
EventType: PH_LIB_TOPO_AWS_OBTAIN_INSTANCE_FAILURE	392
EventType: PH_LIB_TOPO_CHECK_APP_LIST_WARNING	392
EventType: PH_LIB_TOPO_CISCO_IOS_CBQOS_ERROR	393
EventType: PH_LIB_TOPO_CISCO_MERAKI_GET_CHILD_DEVICE_WARNING	393
EventType: PH_LIB_TOPO_CISCO_MERAKI_GET_INTFS_WARNING	394
EventType: PH_LIB_TOPO_CISCO_MERAKI_GET_INTF_WARNING	394
EventType: PH_LIB_TOPO_CISCO_MERAKI_MAC_2_HOST_LOOKUP_FAILED	394
EventType: PH_LIB_TOPO_CISCO_MERAKI_MAC_2_INTF_LOOKUP_FAILED	395
EventType: PH_LIB_TOPO_CISCO_UCS_LOGIN_FAILED	395
EventType: PH_LIB_TOPO_CISCO_UCS_REQUEST_ERROR	395
EventType: PH_LIB_TOPO_CPU_TOO_HIGH	396
EventType: PH_LIB_TOPO_CUST_CONFIG_JOB_DOWNLOAD_SCRIPT_	
FAILED	396
EventType: PH_LIB_TOPO_CUST_FIM_JOB_CHECK_PATH_ERROR	396
EventType: PH_LIB_TOPO_CUST_FIM_JOB_DEVICE_UNAVAILABLE	397
EventType: PH_LIB_TOPO_CUST_FIM_JOB_FILE_TOO_LARGE	397
EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_DATA_FAILED	398
EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_FILE_INFO_FAILED	398
EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_MD5_FAILED	398
EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_REMOTE_FILE_ERROR	399
EventType: PH_LIB_TOPO_CUST_FIM_JOB_INCORRECT_CRED	399
EventType: PH_LIB_TOPO_CUST_FIM_JOB_RUN_SCP_FAILED	400
EventType: PH_LIB_TOPO_CUST_FIM_JOB_TOO_MANY_FILES	400
EventType: PH_LIB_TOPO_CUST_LOGIN_JOB_CREATE_EVENT_FAILED	400
EventType: PH_LIB_TOPO_CUST_LOGIN_JOB_GET_DATA_FAILED	401
EventType: PH_LIB_TOPO_CUST_SNMP_JOB_CREATE_EVENT_FAILED	401
EventType: PH_LIB_TOPO_CUST_SNMP_JOB_GET_DATA_FAILED	401
EventType: PH_LIB_TOPO_CUST_WMI_JOB_CREATE_EVENT_FAILED	402
EventType: PH_LIB_TOPO_CUST_WMI_JOB_GET_DATA_FAILED	402
EventType: PH_LIB_TOPO_ETHERMIB_STAT_LOOKUP_ERROR	403
EventType: PH_LIB_TOPO_EVENT_DROP_RULE_ENCODE_VALUE_GROUP_	
ERROR	403
EventType: PH_LIB_TOPO_EVENT_DROP_RULE_PARSE_ERROR	403
EventType: PH_LIB_TOPO_EXCLUDED_DISK_PARSE_ERROR	404
EventType: PH_LIB_TOPO_FCT_DEV_MAPPING_ENTRY_INVALID	404
EventType: PH_LIB_TOPO_FGT_FABRIC_DISCOV_FAIL	404
EventType: PH_LIB_TOPO_FGT_GET_CONFIG_BACKUP_FAILED	404
EventType: PH_LIB_TOPO_FGT_GET_USER_DEV_STORE_FAIL	405
EventType: PH_LIB_TOPO_FGT_GET_USER_DEV_UNKNOWN	405
EventType: PH_LIB_TOPO_FGT_INSTALLED_SW_FAIL	405
EventType: PH_LIB_TOPO_FGT_SEC_POSTURE_RPT_API_FAIL	405
EventType: PH_LIB_TOPO_FILE_READ_ERROR	405

EventType: PH_LIB_TOPO_FOUNDRY_HW_STATUS_ERROR	406
EventType: PH_LIB_TOPO_GEN_UPS_STATUS_GET_ERROR	406
EventType: PH_LIB_TOPO_GET_NETAPP_NFS_FAILED	406
EventType: PH_LIB_TOPO_H3C_CPU_UTIL_ERROR	407
EventType: PH_LIB_TOPO_HP3COM_CPU_UTIL_ERROR	407
EventType: PH_LIB_TOPO_HP3COM_MEM_UTIL_ERROR	408
EventType: PH_LIB_TOPO_HPUX_PROC_CPU_MEM_TOO_HIGH	408
EventType: PH_LIB_TOPO_HYPERV_METRICS_GET_ERROR	408
EventType: PH_LIB_TOPO_IMPORTANT_INTF_PARSE_ERROR	409
EventType: PH_LIB_TOPO_INTF_UTIL_ERROR	409
EventType: PH_LIB_TOPO_JSON_PARSE_FAILED	409
EventType: PH_LIB_TOPO_JUNIPER_INTF_SPEED_GET_ERROR	410
EventType: PH_LIB_TOPO_LIEBERT_HVAC_STATUS_GET_ERROR	410
EventType: PH_LIB_TOPO_LOGIN_PING_FAILED	410
EventType: PH_LIB_TOPO_MAINTENANCE_DURATION_INCORRECT	411
EventType: PH_LIB_TOPO_MEM_TOO_HIGH	411
EventType: PH_LIB_TOPO_NETAPP_AGGREGATE_STAT_ERROR	411
EventType: PH_LIB_TOPO_NETAPP_ANALYZE_VERSION_ERROR	412
EventType: PH_LIB_TOPO_NETAPP_DISK_STAT_ERROR	412
EventType: PH_LIB_TOPO_NETAPP_GET_NFS_METRIC_ERROR	413
EventType: PH_LIB_TOPO_NETAPP_GET_VERSION_ERROR	413
EventType: PH_LIB_TOPO_NETAPP_LUN_STAT_ERROR	413
EventType: PH_LIB_TOPO_NETAPP_PROTO_STAT_ERROR	414
EventType: PH_LIB_TOPO_NETAPP_VOLUME_STAT_ERROR	414
EventType: PH_LIB_TOPO_NOT_SUPPORT_REST_API	414
EventType: PH_LIB_TOPO_OPEN_FILE_FAILED	415
EventType: PH_LIB_TOPO_PARSE_INTF_MAP_FAILURE	415
EventType: PH_LIB_TOPO_PERF_JOB_EXEC_FAILED	415
EventType: PH_LIB_TOPO_PERF_JOB_INIT_FAILED	416
EventType: PH_LIB_TOPO_PERF_JOB_REMOVE_FAILED	416
EventType: PH_LIB_TOPO_PERF_TEMPLATE_LOAD_ERROR	416
EventType: PH_LIB_TOPO_PERF_TEMPLATE_PARSE_FAILURE	417
EventType: PH_LIB_TOPO_PERF_TEMPLATE_PARSE_WARNING	417
EventType: PH_LIB_TOPO_PORT_FILTER_PARSE_ERROR	417
EventType: PH_LIB_TOPO_PORT_FILTER_PUSH_ERROR	417
EventType: PH_LIB_TOPO_PROC_CPU_MEM_TOO_HIGH	418
EventType: PH_LIB_TOPO_REST_API_FAILED	418
EventType: PH_LIB_TOPO_RUN_SW_FILTER_PARSE_ERROR	418
EventType: PH_LIB_TOPO_RUN_SW_FILTER_PUSH_ERROR	418
EventType: PH_LIB_TOPO_SNMPWALK_ERROR	419
EventType: PH_LIB_TOPO_STM_JOB_EXEC_FAILED	419
EventType: PH_LIB_TOPO_STM_JOB_INIT_FAILED	419
EventType: PH_LIB_TOPO_TEST_CONN_HTTP_AGENT_FAILED	420
EventType: PH_LIB_TOPO_TEST_CONN_JDBC_AGENT_FAILED	420
EventType: PH_LIB_TOPO_TEST_CONN_JMX_AGENT_FAILED	420
EventType: PH_LIB_TOPO_TRUNK_PORT_MAP_PARSE_ERROR	421
EventType: PH_LIB_TOPO_VALIDATE_ACCESS_FAILED	421
EventType: PH_LIB_TOPO_WIN_GET_EXCH_DATABASE_INSTANCE_WARNING	421

EventType: PH_LIB_TOPO_WIN_GET_EXCH_DATABASE_WARNING	422
EventType: PH_LIB_TOPO_WIN_GET_EXCH_MAIL_SUBMISSION_WARNING ..	422
EventType: PH_LIB_TOPO_WIN_GET_EXCH_PUB_MAILBOX_WARNING	423
EventType: PH_LIB_TOPO_WIN_GET_EXCH_REG_MAILBOX_WARNING	423
EventType: PH_LIB_TOPO_WIN_GET_EXCH_REPLICATION_WARNING	423
EventType: PH_LIB_TOPO_WIN_GET_EXCH_RPC_WARNING	424
EventType: PH_LIB_TOPO_WIN_GET_EXCH_SMTP_WARNING	424
EventType: PH_LIB_TOPO_WIN_GET_EXCH_STORE_INTF_WARNING	424
EventType: PH_LIB_TOPO_WIN_GET_EXCH_TRANSPORT_QUEUE_WARNING	425
EventType: PH_LIB_TOPO_WMI_GET_CPU_COUNT_ERROR	425
EventType: PH_LIB_TOPO_WMI_GET_CPU_WARNING	426
EventType: PH_LIB_TOPO_WMI_GET_PAGE_ACTIVITY_ERROR	426
EventType: PH_LIB_TOPO_WMI_GET_REAL_MEM_ERROR	426
EventType: PH_LIB_TOPO_WMI_GET_RUN_SW_PERF_ERROR	427
EventType: PH_MAX_DEVICES_EXCEEDED	427
EventType: PH_MAX_DEVICES_LIMIT_REACHED	427
EventType: PH_TEST_CONN_COMPLETE	427
EventType: PH_TEST_CONN_CONTACT_APP_SERVER	428
EventType: PH_TEST_CONN_FAILED	428
EventType: PH_TEST_CONN_FAILED_INVALID_REQUEST	428
EventType: PH_TEST_CONN_FAILED_INVALID_REQUEST_XML	428
EventType: PH_TEST_CONN_RECVD_VALID_REQUEST	429
EventType: PH_TEST_CONN_RESULT_SENT	429
EventType: PH_TEST_CONN_STARTED	429
Event Collection and Forwarding Logs	430
EventType: PH_AGENTMGR_ACI_ATTR_NOT_FOUND	441
EventType: PH_AGENTMGR_ACI_CURL_HANDLE_GET_FAILED	441
EventType: PH_AGENTMGR_ACI_FILE_WRITE_ERROR	441
EventType: PH_AGENTMGR_ACI_JSON_PARSE_FAILED	441
EventType: PH_AGENTMGR_ACI_SERVER_EMPTY	442
EventType: PH_AGENTMGR_ACI_TOKEN_GET_FAILED	442
EventType: PH_AGENTMGR_ALERTLOGIC_CURL_HANDLE_GET_FAILED	442
EventType: PH_AGENTMGR_ALERTLOGIC_FILE_LOAD_ERROR	442
EventType: PH_AGENTMGR_ALERTLOGIC_FILE_READ_ERROR	443
EventType: PH_AGENTMGR_ALERTLOGIC_FILE_WRITE_ERROR	443
EventType: PH_AGENTMGR_ALERTLOGIC_INVALID_DATA	443
EventType: PH_AGENTMGR_ALERTLOGIC_INVALID_PATH	443
EventType: PH_AGENTMGR_ALERTLOGIC_QUERY_INTERVAL_TOO_LONG	444
EventType: PH_AGENTMGR_ALERTLOGIC_SERVER_EMPTY	444
EventType: PH_AGENTMGR_AMPCLOUD_CURL_CONNECT_FAILED	444
EventType: PH_AGENTMGR_AMPCLOUD_CURL_HANDLE_GET_FAILED	444
EventType: PH_AGENTMGR_AMPCLOUD_FILE_LOAD_ERROR	445
EventType: PH_AGENTMGR_AMPCLOUD_FILE_READ_ERROR	445
EventType: PH_AGENTMGR_AMPCLOUD_INVALID_DATA	445
EventType: PH_AGENTMGR_AMPCLOUD_JSON_PARSE_FAILED	445
EventType: PH_AGENTMGR_AMPCLOUD_NO_DEFINE_SEVERITY	446
EventType: PH_AGENTMGR_AMPCLOUD_SERVER_EMPTY	446
EventType: PH_AGENTMGR_API_PERMISSION_MISSING	446
EventType: PH_AGENTMGR_AWSCLOUDWATCH_GETLOGS	446

EventType: PH_AGENTMGR_AWSFLOWLOG_EVENT_PULL_FAILED	447
EventType: PH_AGENTMGR_AWSFLOWLOG_FILE_WRITE_ERROR	447
EventType: PH_AGENTMGR_AWSFLOWLOG_LOG_FORMAT_WRONG	447
EventType: PH_AGENTMGR_AWSKINESIS_CONSUMER_START_FAILED	448
EventType: PH_AGENTMGR_AWS_CACHE_FILE_ERROR	448
EventType: PH_AGENTMGR_AWS_DELETE_OJECTKEY_FAILED	448
EventType: PH_AGENTMGR_AWS_DOWNLOAD_OJECT_FAILED	448
EventType: PH_AGENTMGR_AWS_EVT_DOWNLOAD_FAILED	449
EventType: PH_AGENTMGR_AWS_EVT_SEND_FAILED	449
EventType: PH_AGENTMGR_AWS_GET_OJECTKEY_FAILED	449
EventType: PH_AGENTMGR_AWS_GZ_FILE_OPEN_ERROR	450
EventType: PH_AGENTMGR_AWS_JSON_PARSE_FAILED	450
EventType: PH_AGENTMGR_AWS_SQSURL_FORMAT_ERROR	450
EventType: PH_AGENTMGR_BOX_API_CALL_FAILED	450
EventType: PH_AGENTMGR_BOX_ATTR_NOT_FOUND	450
EventType: PH_AGENTMGR_BOX_EVENT_PULL_FAILED	451
EventType: PH_AGENTMGR_BOX_FILE_ID_EMPTY	451
EventType: PH_AGENTMGR_BOX_FILE_LIMIT_EXCEED	451
EventType: PH_AGENTMGR_BOX_FILE_NOT_MONITORED_ERROR	451
EventType: PH_AGENTMGR_BOX_FILE_PATH_PARSE_FAILED	452
EventType: PH_AGENTMGR_BOX_FILE_TYPE_WRONG	452
EventType: PH_AGENTMGR_BOX_FOLDER_TYPE_WRONG	452
EventType: PH_AGENTMGR_BOX_HTTP_NO_RESPONSE	452
EventType: PH_AGENTMGR_BOX_JSON_PARSE_FAILED	453
EventType: PH_AGENTMGR_BOX_RESPONSE_NO_SPECIAL_ATTRIBUTE	453
EventType: PH_AGENTMGR_BOX_TIME_CONVERT_FAILED	453
EventType: PH_AGENTMGR_BOX_XML_PARSE_FAILED	453
EventType: PH_AGENTMGR_CISCOAMP_CONSUMER_START_FAILED	454
EventType: PH_AGENTMGR_CLOUDPASSAGE_API_CALL_FAILED	454
EventType: PH_AGENTMGR_CLOUDPASSAGE_FILE_WRITE_ERROR	454
EventType: PH_AGENTMGR_CLOUDPASSAGE_GET_EVENT_FAILED	454
EventType: PH_AGENTMGR_CLOUDPASSAGE_JSON_EMPTY	455
EventType: PH_AGENTMGR_CLOUDPASSAGE_JSON_PARSE_FAILED	455
EventType: PH_AGENTMGR_CLOUDPASSAGE_TOKEN_EMPTY	455
EventType: PH_AGENTMGR_CLOUDTRAIL_FILE_READ_FAILED	455
EventType: PH_AGENTMGR_CONFIG_ERROR	456
EventType: PH_AGENTMGR_CONFIG_VERSION_SEND_FAILED	456
EventType: PH_AGENTMGR_CONFIG_WARNING	456
EventType: PH_AGENTMGR_CREDENTIAL_GET_FAILED	457
EventType: PH_AGENTMGR_CROWDSTRIKE_GET_DATAFEED_URL_FAILED	457
EventType: PH_AGENTMGR_CUST_RESULT_UPLOAD_FAILED	457
EventType: PH_AGENTMGR_DIR_CREATE_FAILED	457
EventType: PH_AGENTMGR_EVENT_PULL_FAILED	458
EventType: PH_AGENTMGR_FALCONDATAREP_SCRIPT_FAILED	458
EventType: PH_AGENTMGR_FILE_PARSE_ERROR	458
EventType: PH_AGENTMGR_FILE_WRITE_ERROR	459
EventType: PH_AGENTMGR_FIREAMP_CERT_DOWNLOAD_FAILED	459
EventType: PH_AGENTMGR_FIREAMP_DATA_FORMAT_SET_FAILED	459
EventType: PH_AGENTMGR_FIREAMP_EVENT_PULL_FAILED	460

EventType: PH_AGENTMGR_FIREAMP_EVT_TYPE_LOAD_FAILED	460
EventType: PH_AGENTMGR_FIREAMP_FILE_LOAD_ERROR	460
EventType: PH_AGENTMGR_FIREAMP_FILE_OPEN_ERROR	461
EventType: PH_AGENTMGR_FIREAMP_INVALID_DATA	461
EventType: PH_AGENTMGR_FIREAMP_NEW_AGENT_FAILED	461
EventType: PH_AGENTMGR_FIREAMP_NO_ATTR	461
EventType: PH_AGENTMGR_FIREAMP_NO_PROTOCOL	461
EventType: PH_AGENTMGR_FORTICASB_GET_SERVICE_ALERT_ERROR	462
EventType: PH_AGENTMGR_FORTICASB_GET_SERVICE_ERROR	462
EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_FAILED	462
EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_NEXT_PAGE	463
EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_NO_RESULTS	463
EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_RESULTS	463
EventType: PH_AGENTMGR_FORTINDR_GET_BUCKET_KEY	463
EventType: PH_AGENTMGR_FORTINDR_GET_BUCKET_OBJ	464
EventType: PH_AGENTMGR_GET_SCAN_RESULTS_FAILED	464
EventType: PH_AGENTMGR_GITHUB_API_CALL_FAILED	465
EventType: PH_AGENTMGR_GITHUB_CREDENTIAL_GET_FAILED	465
EventType: PH_AGENTMGR_GITHUB_EVENT_PULL_FAILED	465
EventType: PH_AGENTMGR_GITHUB_FILE_OPEN_ERROR	466
EventType: PH_AGENTMGR_GITHUB_JSON_PARSE_FAILED	466
EventType: PH_AGENTMGR_GITHUB_TIME_CONVERT_FAILED	466
EventType: PH_AGENTMGR_GIT_CLONE_REPO_FAILED	466
EventType: PH_AGENTMGR_GIT_HANDLE_ERR_FILE_FAILED	467
EventType: PH_AGENTMGR_GIT_PULL_EVT_FAILED	467
EventType: PH_AGENTMGR_GIT_SAVE_COMMITID_FAILED	467
EventType: PH_AGENTMGR_GZ_FILE_OPEN_ERROR	467
EventType: PH_AGENTMGR_INIT_AGENT	468
EventType: PH_AGENTMGR_INIT_CACHE_FILE_FAILED	468
EventType: PH_AGENTMGR_INIT_NO_CRED	468
EventType: PH_AGENTMGR_INVALID_MGR	468
EventType: PH_AGENTMGR_IPS_AUTH_FAILED	469
EventType: PH_AGENTMGR_IPS_EVENT_PULL_FAILED	469
EventType: PH_AGENTMGR_IPS_FILE_OPEN_ERROR	469
EventType: PH_AGENTMGR_IPS_OBTAIN_SUBSCRIPTION_FAILED	469
EventType: PH_AGENTMGR_IPS_SET_SSL_FAILED	470
EventType: PH_AGENTMGR_JAVA_AGENT_PIPE_WRITE_FAILED	470
EventType: PH_AGENTMGR_JAVA_AGENT_START_FAILED	470
EventType: PH_AGENTMGR_JAVA_AGENT_TYPE_UNKNOWN	470
EventType: PH_AGENTMGR_JAVA_AGENT_USER_MISSING	471
EventType: PH_AGENTMGR_JAVA_AGENT_ZOMBIE	471
EventType: PH_AGENTMGR_JAVA_CMD_SEND_FAILED	471
EventType: PH_AGENTMGR_JAVA_FORK_FAILED	471
EventType: PH_AGENTMGR_JAVA_INCOMPLETE_DEV_INFO	472
EventType: PH_AGENTMGR_JAVA_NO_DEV_TYPE_FOR_JDBC	472
EventType: PH_AGENTMGR_JAVA_NO_STATUS_FILE	472
EventType: PH_AGENTMGR_JAVA_PIPE_FAILED	472
EventType: PH_AGENTMGR_JAVA_PROCESS_STATE_GET_FAILED	473
EventType: PH_AGENTMGR_JAVA_SIGKILL_SEND_FAILED	473

EventType: PH_AGENTMGR_JAVA_UNSUPPORT_DEV_TYPE_FOR_JDBC	473
EventType: PH_AGENTMGR_JAVA_USER_PWD_GET_FAILED	474
EventType: PH_AGENTMGR_JSON_PARSE_FAILED	474
EventType: PH_AGENTMGR_KAFKA_CONSUME_LOG_FAILED	474
EventType: PH_AGENTMGR_KAFKA_CREATE_CONSUMER	474
EventType: PH_AGENTMGR_KAFKA_CREATE_CONSUMER_FAILED	475
EventType: PH_AGENTMGR_KAFKA_CREATE_PRODUCER_FAILED	475
EventType: PH_AGENTMGR_KAFKA_CREATE_TOPIC_FAILED	475
EventType: PH_AGENTMGR_KAFKA_ERROR	476
EventType: PH_AGENTMGR_KAFKA_METADATA_FAILED	476
EventType: PH_AGENTMGR_KAFKA_PRODUCER_ERROR	477
EventType: PH_AGENTMGR_KAFKA_PULL_JOB_FAILED	477
EventType: PH_AGENTMGR_KAFKA_REBALANCE	477
EventType: PH_AGENTMGR_KAFKA_RELEASE_CONSUMER	477
EventType: PH_AGENTMGR_KAFKA_START_FAILED	478
EventType: PH_AGENTMGR_KAFKA_SUBSCRIBE_FAILED	478
EventType: PH_AGENTMGR_KAFKA_UPDATE_CONFIG_FAILED	478
EventType: PH_AGENTMGR_KAFKA_UPDATE_ERROR	479
EventType: PH_AGENTMGR_KILL_PROCESS	479
EventType: PH_AGENTMGR_MSAZURE_CONFIG_ARM_FAILED	479
EventType: PH_AGENTMGR_MSAZURE_DOWNLOAD_FAILED	480
EventType: PH_AGENTMGR_MSAZURE_JSON_EMPTY	480
EventType: PH_AGENTMGR_MSAZURE_JSON_FILE_NAME_EMPTY	480
EventType: PH_AGENTMGR_MSAZURE_JSON_FILE_PARSE_FAILED	480
EventType: PH_AGENTMGR_MSAZURE_JSON_PARSE_FAILED	480
EventType: PH_AGENTMGR_MSAZURE_LOGIN_FAILED	481
EventType: PH_AGENTMGR_MSG_QUEUE_ACCESS_FAILED	481
EventType: PH_AGENTMGR_MSG_RECV_FAILED	481
EventType: PH_AGENTMGR_OCI_SET_INSTANCE_NAME_FAILED	481
EventType: PH_AGENTMGR_OFFICE365_API_CALL_FAILED	482
EventType: PH_AGENTMGR_OFFICE365_EVENT_PULL_FAILED	482
EventType: PH_AGENTMGR_OFFICE365_FILE_WRITE_ERROR	482
EventType: PH_AGENTMGR_OFFICE365_GET_SUBSCRIBE_FAILED	483
EventType: PH_AGENTMGR_OFFICE365_JSON_PARSE_FAILED	483
EventType: PH_AGENTMGR_OFFICE365_START_SUBSCRIBE_FAILED	483
EventType: PH_AGENTMGR_OFFICE365_SUBSCRIBE_EMPTY	483
EventType: PH_AGENTMGR_OFFICE365_SUBSCRIBE_FAILED	484
EventType: PH_AGENTMGR_OFFICE365_TOKEN_EMPTY	484
EventType: PH_AGENTMGR_OKTA_EVT_DOWNLOAD_FAILED	484
EventType: PH_AGENTMGR_OKTA_FILE_WRONG	484
EventType: PH_AGENTMGR_OKTA_NO_USER_INFO	485
EventType: PH_AGENTMGR_OKTA_RESULT_UPLOAD_FAILED	485
EventType: PH_AGENTMGR_OKTA_RESULT_UPLOAD_WARNING	485
EventType: PH_AGENTMGR_PARSER_UNABLE_CONNECT	485
EventType: PH_AGENTMGR_PERF_OBJ_PARSE_FAILURE	486
EventType: PH_AGENTMGR_PROCESS_INIT_FAILED	486
EventType: PH_AGENTMGR_PULLING_JOB_OUTDATE	486
EventType: PH_AGENTMGR_REMOVE_FILE_FAILED	486
EventType: PH_AGENTMGR_REST_API_CALL_FAILED	487

EventType: PH_AGENTMGR_RSAS_XML_PARSE_FAILED	487
EventType: PH_AGENTMGR_RUN_CMD_FAILED	487
EventType: PH_AGENTMGR_RUN_SCRIPT_FAILED	487
EventType: PH_AGENTMGR_RUN_SCRIPT_WITHOUT_TASK_ID	488
EventType: PH_AGENTMGR_SALESFORCE_ATTR_NOT_FOUND	488
EventType: PH_AGENTMGR_SALESFORCE_COLUMN_NOT_FOUND	488
EventType: PH_AGENTMGR_SALESFORCE_CURL_EXECUTE_FAILED	488
EventType: PH_AGENTMGR_SALESFORCE_CURL_HANDLE_GET_FAILED	489
EventType: PH_AGENTMGR_SALESFORCE_FILE_LOAD_ERROR	489
EventType: PH_AGENTMGR_SALESFORCE_FILE_WRITE_ERROR	489
EventType: PH_AGENTMGR_SALESFORCE_INVALID_DATA	489
EventType: PH_AGENTMGR_SALESFORCE_INVALID_LOG_FILE	490
EventType: PH_AGENTMGR_SALESFORCE_JSON_PARSE_FAILED	490
EventType: PH_AGENTMGR_SALESFORCE_LOGIN_FAILED	490
EventType: PH_AGENTMGR_SALESFORCE_SERVER_EMPTY	490
EventType: PH_AGENTMGR_SALESFORCE_TOKEN_GET_FAILED	490
EventType: PH_AGENTMGR_SALESFORCE_TOKEN_REGET_FAILED	491
EventType: PH_AGENTMGR_SALESFORCE_VERSION_PATH_EMPTY	491
EventType: PH_AGENTMGR_SALESFORCE_XML_PARSE_FAILED	491
EventType: PH_AGENTMGR_SCRIPT_NOTIFICATION_SPAWN_FAILED	491
EventType: PH_AGENTMGR_SERVER_HOST_NAME_RESOLVE_FAILED	491
EventType: PH_AGENTMGR_SERVER_HOST_NAME_RESOLVE_WARNING	492
EventType: PH_AGENTMGR_SERVER_IP_RESOLVE_FAILED	492
EventType: PH_AGENTMGR_SERVER_IP_RESOLVE_WARNING	492
EventType: PH_AGENTMGR_SETUP_STREAM_FAILED	492
EventType: PH_AGENTMGR_START_THREAD_FAILED	493
EventType: PH_AGENTMGR_STATUS_REPORT_FAILED	493
EventType: PH_AGENTMGR_STATUS_REPORT_INIT_FAILED	493
EventType: PH_AGENTMGR_STOP_STREAM_FAILED	493
EventType: PH_AGENTMGR_TENABLE_EXPORT_SCAN_FAILED	493
EventType: PH_AGENTMGR_TENABLE_GET_DOWNLOAD_FAILED	494
EventType: PH_AGENTMGR_TENABLE_GET_SCANS_FAILED	494
EventType: PH_AGENTMGR_TENABLE_GET_STATUS_FAILED	494
EventType: PH_AGENTMGR_TENABLE_PULL_FAILED	494
EventType: PH_AGENTMGR_TIME_CONVERSION_FAILED	495
EventType: PH_AGENTMGR_TIME_STR_FORMAT_INVALID	495
EventType: PH_AGENTMGR_TOKEN_GET_FAILED	495
EventType: PH_AGENTMGR_UNPACK_FILE_FAILED	495
EventType: PH_AGENTMGR_UPDATE_AGENT	496
EventType: PH_AGENTMGR_UPDATE_BOOKMARK_FAILED	496
EventType: PH_AGENTMGR_UPDATE_WEBHOOK_CRED_FAILED	496
EventType: PH_AGENTMGR_UPDATE_WEBHOOK_CRED_SUCCESS	497
EventType: PH_AGENTMGR_WINDEFATP_API_CALL_FAILED	497
EventType: PH_AGENTMGR_WINDEFATP_FILE_WRITE_ERROR	497
EventType: PH_AGENTMGR_WINDEFATP_GET_ALERT_FAILED	497
EventType: PH_AGENTMGR_WINDEFATP_JSON_EMPTY	498
EventType: PH_AGENTMGR_WINDEFATP_JSON_PARSE_FAILED	498
EventType: PH_AGENTMGR_WINDEFATP_TOKEN_EMPTY	498
EventType: PH_AGENTMGR_WMI_EVENT_PULL_ERROR	498

EventType: PH_AGENTMGR_WMI_EVENT_PULL_WARNING	499
EventType: PH_AGENTMGR_WMI_FILE_OPEN_ERROR	499
EventType: PH_AGENTMGR_WMI_LOG_PULL_ERROR	499
EventType: PH_AGENTMGR_WMI_MISSING_LOG	500
EventType: PH_AGENTMGR_WMI_STATUS_REPORT_FAILED	500
EventType: PH_AGENTMGR_WMI_USER_PWD_GET_FAILED	500
EventType: PH_AGENTMGR_WVSS_XML_PARSE_FAILED	500
EventType: PH_AGENTMGR_XML_PARSE_FAILED	501
EventType: PH_BAD_NETFLOW_PACKET	501
EventType: PH_BAD_NETFLOW_VER	501
EventType: PH_CHECKPOINT_CERTHANDLER_ERROR	501
EventType: PH_CHECKPOINT_CERTPULL_ERROR	502
EventType: PH_CHECKPOINT_CMD_USAGE_ERROR	502
EventType: PH_CHECKPOINT_CPMI_FETCH_ERROR	502
EventType: PH_CHECKPOINT_DEV_INIT_ERROR	503
EventType: PH_CHECKPOINT_FILE_RENAME_FAILURE	503
EventType: PH_CHECKPOINT_FWLOGHANDLER_ERROR	503
EventType: PH_CHECKPOINT_FWLOGHANDLER_INIT_ERROR	504
EventType: PH_CHECKPOINT_HTTP_ERROR	504
EventType: PH_CHECKPOINT_LOGHANDLER_ERROR	505
EventType: PH_CHECKPOINT_PROCESS_GET_FAILED	505
EventType: PH_CHECKPOINT_TESTCONN_ERROR	505
EventType: PH_CHECKPOINT_UNABLE_PARSE_XML	505
EventType: PH_COLLECTOR_CLOCK_SKEW	506
EventType: PH_COLLECTOR_DOWN	506
EventType: PH_COLLECTOR_EVENT_ARRIVAL_DELAYED	506
EventType: PH_COLLECTOR_EVENT_ARRIVAL_OK	507
EventType: PH_COLLECTOR_EVENT_STORE_DELAYED	507
EventType: PH_COLLECTOR_EVENT_STORE_OK	507
EventType: PH_COLLECTOR_UP	507
EventType: PH_CYBERARK_INIT_ERROR	507
EventType: PH_DEV_FAIL_TO_PULL_EVENTS	508
EventType: PH_EVENT_FORWARDER_CHECKSUM_MISMATCH	508
EventType: PH_EVENT_FORWARDER_CONNECT_ERROR	508
EventType: PH_EVENT_FORWARDER_DIR_OPEN_FAILURE	509
EventType: PH_EVENT_FORWARDER_FILE_OPEN_FAILURE	509
EventType: PH_EVENT_FORWARDER_FILE_RENAME_FAILURE	509
EventType: PH_EVENT_FORWARDER_INIT_FAILURE	510
EventType: PH_EVENT_FORWARDER_INVALID_GZIP_FILE	510
EventType: PH_EVENT_FORWARDER_INVALID_PHOENIX_CONFIG	510
EventType: PH_EVENT_FORWARDER_INVALID_PROTOCOL	511
EventType: PH_EVENT_FORWARDER_KAFKA_ERROR	511
EventType: PH_EVENT_FORWARDER_KAFKA_INIT_FAILURE	511
EventType: PH_EVENT_FORWARDER_KAFKA_PRODUCE_ERROR	512
EventType: PH_EVENT_FORWARDER_MKDIR_FAILURE	512
EventType: PH_EVENT_FORWARDER_RUN_PROCESS_ERROR	512
EventType: PH_EVENT_FORWARDER_SOCKET_ERROR	512
EventType: PH_EVENT_FORWARDER_SOCKET_WRITE_ERROR	513
EventType: PH_EVENT_FORWARDER_SSL_CERT_ERROR	513

EventType: PH_EVENT_FORWARDER_SSL_ERROR	513
EventType: PH_EVENT_FWD_CERT_LOAD_FAILED	514
EventType: PH_EVENT_FWD_CERT_UNPAIRED	514
EventType: PH_EVENT_FWD_DIR_MAKE_FAILED	514
EventType: PH_EVENT_FWD_DIR_OPEN_FAILED	515
EventType: PH_EVENT_FWD_FILE_RENAME_FAILED	515
EventType: PH_EVENT_FWD_FULL_FORWARDING_FAILED	515
EventType: PH_EVENT_FWD_GET_FILE_NUM_FAILURE	516
EventType: PH_EVENT_FWD_GZ_CLOSE_ERROR	516
EventType: PH_EVENT_FWD_GZ_FILE_OPEN_ERROR	516
EventType: PH_EVENT_FWD_GZ_MD5_ERROR	516
EventType: PH_EVENT_FWD_GZ_RENAME_ERROR	517
EventType: PH_EVENT_FWD_GZ_SIZE_MISMATCH	517
EventType: PH_EVENT_FWD_KAFKA_WARNING	517
EventType: PH_EVENT_FWD_MD5_CHECKSUM_MISMATCH	517
EventType: PH_EVENT_FWD_NETFLOW_REGEX_IGNORED	518
EventType: PH_EVENT_FWD_PARTIAL_FORWARDING_FAILED	518
EventType: PH_EVENT_FWD_PARTIAL_FORWARDING_WARNING	518
EventType: PH_EVENT_FWD_PCRE_ERROR	518
EventType: PH_EVENT_FWD_PROCESS_INIT_FAILED	518
EventType: PH_EVENT_FWD_PROCESS_START_FAILED	519
EventType: PH_EVENT_FWD_PROTO_FORWARDED_WRONG	519
EventType: PH_EVENT_FWD_RENAME_GZ_ERROR	519
EventType: PH_EVENT_FWD_RULE_PARSE_ERROR	519
EventType: PH_EVENT_FWD_SOCKET_CONNECT_FAILED	520
EventType: PH_EVENT_FWD_SOCKET_GET_FAILED	520
EventType: PH_EVENT_FWD_SOCKET_WRITE_FAILED	520
EventType: PH_EVENT_FWD_SSL_CREATE_FAILED	520
EventType: PH_EVENT_FWD_SSL_SESSION_BUILD_FAILED	521
EventType: PH_EVENT_FWD_UNEXPECTED_FILE_REMOVED	521
EventType: PH_EVENT_PKG_ATTR_NOT_FOUND	521
EventType: PH_EVENT_PKG_EMPTY_FILE_REMOVED	521
EventType: PH_EVENT_PKG_FILE_ADD_TO SVN_FAILED	522
EventType: PH_EVENT_PKG_FILE_REMOVED_ERROR	522
EventType: PH_EVENT_PKG_FILE_RENAME_FAILED	522
EventType: PH_EVENT_PKG_FILE_STAT_FAILED	523
EventType: PH_EVENT_PKG_FILE_UPLOAD_FAILED	523
EventType: PH_EVENT_PKG_FILE_UPLOAD_SUCCESS_HIGH	523
EventType: PH_EVENT_PKG_FILE_UPLOAD_SUCCESS_LOW	524
EventType: PH_EVENT_PKG_GZ_CLOSE_FAILED	524
EventType: PH_EVENT_PKG_GZ_FILE_OPEN_ERROR	524
EventType: PH_EVENT_PKG_HTTP_FAILED	525
EventType: PH_EVENT_PKG_HTTP_INIT_FAILED	525
EventType: PH_EVENT_PKG_INSERT_TASK_FAILED	525
EventType: PH_EVENT_PKG_NO_EVENT	526
EventType: PH_EVENT_PKG_OPEN_DIR_FAILED	526
EventType: PH_EVENT_PKG_PROCESS_INIT_FAILED	526
EventType: PH_EVENT_PKG_PROCESS_START_FAILED	526
EventType: PH_EVENT_PKG_QUEUE_GET_FAILED	526

EventType: PH_EVENT_PKG_SERVER_LIST_UPLOAD_FAILED	527
EventType: PH_EVENT_PKG_SERVICE_LIST_EMPTY	527
EventType: PH_EVENT_PKG_TASK_ADD_TO_QUEUE_FAILED	527
EventType: PH_EVENT_PKG_XML_PARSE_FAILED	527
EventType: PH_EVTPKGGER_FILE_UPLOAD_FAILED	528
EventType: PH_EVT_HANDLER_DBG	528
EventType: PH_EVT_HANDLER_ERR	528
EventType: PH_EVT_HANDLER_EVT_QUEUE_LARGE	528
EventType: PH_EVT_HANDLER_EVT_QUEUE_WARNING	528
EventType: PH_EVT_HANDLER_INFO	529
EventType: PH_EVT_HANDLER_SVN_QUEUE_LARGE	529
EventType: PH_EVT_HANDLER_SVN_QUEUE_WARNING	529
EventType: PH_EVT_PACKAGER_COND_WAIT_ERROR	529
EventType: PH_EVT_PACKAGER_FILE_CLOSE_FAILURE	529
EventType: PH_EVT_PACKAGER_FILE_OPEN_FAILURE	530
EventType: PH_EVT_PACKAGER_FILE_REMOVE_FAILURE	530
EventType: PH_EVT_PACKAGER_FILE_RENAME_FAILURE	530
EventType: PH_EVT_PACKAGER_FILE_STAT_FAILURE	531
EventType: PH_EVT_PACKAGER_FILE_UPLOAD_FAILURE	531
EventType: PH_EVT_PACKAGER_HTTP_RESPONSE_ERROR	532
EventType: PH_EVT_PACKAGER_INIT_FAILURE	532
EventType: PH_EVT_PACKAGER_REST_PARSE_ERROR	532
EventType: PH_EVT_PACKAGER_RUN_PROCESS_ERROR	532
EventType: PH_JAVA_AGENT_APPSERVER_CONN_ERROR	533
EventType: PH_JAVA_AGENT_APPSERVER_EXECUTE_ERROR	533
EventType: PH_JAVA_AGENT_CONTROLLER_CMD_PARSE_ERROR	533
EventType: PH_JAVA_AGENT_CONTROLLER_CMD_READ_ERROR	533
EventType: PH_JAVA_AGENT_CONTROLLER_GENERIC_ERROR	533
EventType: PH_JAVA_AGENT_CONTROLLER_LINE_READ_ERROR	534
EventType: PH_JAVA_AGENT_CONTROLLER_XML_READ_ERROR	534
EventType: PH_JAVA_AGENT_CUSTOM_JDBC_CONN_ERROR	534
EventType: PH_JAVA_AGENT_CUSTOM_JDBC_EXEC_ERROR	534
EventType: PH_JAVA_AGENT_DISCOVERY_TEST_ERROR	534
EventType: PH_JAVA_AGENT_ERROR	534
EventType: PH_JAVA_AGENT_GLASSFISH_MONITOR_ERROR	535
EventType: PH_JAVA_AGENT_GLASS_FISH_WARNING	535
EventType: PH_JAVA_AGENT_GOOGLEAPPS_EXEC_ERROR	535
EventType: PH_JAVA_AGENT_IBMDB2_AUDIT_CONN_ERROR	535
EventType: PH_JAVA_AGENT_IBMDB2_AUDIT_EXEC_ERROR	535
EventType: PH_JAVA_AGENT_IBM_DB2_CAT_READ_ERROR	536
EventType: PH_JAVA_AGENT_IBM_DB2_CONN_ERROR	536
EventType: PH_JAVA_AGENT_IBM_DB2_INTERNAL_ERROR	536
EventType: PH_JAVA_AGENT_INFO	536
EventType: PH_JAVA_AGENT_JBOSS_CONN_ERROR	536
EventType: PH_JAVA_AGENT_JBOSS_EXEC_ERROR	536
EventType: PH_JAVA_AGENT_JBOSS_MONITOR_ERROR	537
EventType: PH_JAVA_AGENT_JDBC_PULL_UNSUPP_ERROR	537
EventType: PH_JAVA_AGENT_JDBC_SQL_NOT_SUPPORT_ERROR	537
EventType: PH_JAVA_AGENT_JMX_CONN_ERROR	537

EventType: PH_JAVA_AGENT_JMX_EXEC_ERROR	537
EventType: PH_JAVA_AGENT_JOB_EXECUTOR_ERROR	538
EventType: PH_JAVA_AGENT_JOB_STATUS_UPLOAD_ERROR	538
EventType: PH_JAVA_AGENT_JOB_TYPE_ERROR	538
EventType: PH_JAVA_AGENT_JOB_XML_LOAD_ERROR	538
EventType: PH_JAVA_AGENT_JOB_XML_PARSE_ERROR	538
EventType: PH_JAVA_AGENT_MCAFEE_MYSQL_MONITOR_ERROR	538
EventType: PH_JAVA_AGENT_MCAFEE_VULN_SCANNER_ERROR	539
EventType: PH_JAVA_AGENT_MONITOR_GEN_ERROR	539
EventType: PH_JAVA_AGENT_MONITOR_TIMEOUT_ERROR	539
EventType: PH_JAVA_AGENT_MSSQL_DDL_CONN_ERROR	539
EventType: PH_JAVA_AGENT_MSSQL_LOGON_CONN_ERROR	539
EventType: PH_JAVA_AGENT_MSSQL_LOGON_EXEC_ERROR	540
EventType: PH_JAVA_AGENT_MSSQL_MONITOR_ERROR	540
EventType: PH_JAVA_AGENT_MSSQL_PERF_CONN_ERROR	540
EventType: PH_JAVA_AGENT_MSSQL_PERF_EXECUTE_ERROR	540
EventType: PH_JAVA_AGENT_MYSQL_PERF_CONN_ERROR	540
EventType: PH_JAVA_AGENT_MYSQL_PERF_EXEC_ERROR	540
EventType: PH_JAVA_AGENT_NESSUS_REPORT_PARSE_ERROR	541
EventType: PH_JAVA_AGENT_ORACLE_DB_ERROR	541
EventType: PH_JAVA_AGENT_ORADB_AUDIT_CONN_ERROR	541
EventType: PH_JAVA_AGENT_ORADB_AUDIT_EXEC_ERROR	541
EventType: PH_JAVA_AGENT_ORADB_LOGON_EXEC_ERROR	541
EventType: PH_JAVA_AGENT_ORADB_PERF_CONN_ERROR	542
EventType: PH_JAVA_AGENT_ORADB_PERF_EXEC_ERROR	542
EventType: PH_JAVA_AGENT_SNORT_CONN_ERROR	542
EventType: PH_JAVA_AGENT_SNORT_EVENTID_ERROR	542
EventType: PH_JAVA_AGENT_SNORT_EXEC_ERROR	542
EventType: PH_JAVA_AGENT_SNORT_SENSORID_ERROR	542
EventType: PH_JAVA_AGENT_SNORT_TCP_OPTION_ERROR	543
EventType: PH_JAVA_AGENT_TOMCAT_MONITOR_ERROR	543
EventType: PH_JAVA_AGENT_UTILS_ERROR	543
EventType: PH_JAVA_AGENT_VMWARE_HWSTATUS_EXEC_ERROR	543
EventType: PH_JAVA_AGENT_VMWARE_LOG_CONN_ERROR	543
EventType: PH_JAVA_AGENT_VMWARE_LOG_EXEC_ERROR	544
EventType: PH_JAVA_AGENT_VMWARE_MONITOR_ERROR	544
EventType: PH_JAVA_AGENT_VMWARE_PERF_COUNTER_MISSING	544
EventType: PH_JAVA_AGENT_VMWARE_PERF_DATA_RETRIEVE_ERROR	544
EventType: PH_JAVA_AGENT_VMWARE_PERF_ENTITY_MISSING	544
EventType: PH_JAVA_AGENT_VMWARE_PERF_HOST_MISSING	544
EventType: PH_JAVA_AGENT_VMWARE_PERF_MON_EXCEPTION	545
EventType: PH_JAVA_AGENT_VMWARE_PERF_ROLLUP_MISSING	545
EventType: PH_JAVA_AGENT_VMWARE_PERF_STAT_NAME_MISSING	545
EventType: PH_JAVA_AGENT_VMWARE_PERF_VM_MISSING	545
EventType: PH_JAVA_AGENT_VMWARE_THREAD_EXEC_ERROR	545
EventType: PH_JAVA_AGENT_VULN_REPORT_PARSER_ERROR	546
EventType: PH_JAVA_AGENT_VULN_REPORT_VERIFY_ERROR	546
EventType: PH_JAVA_AGENT_WEBLOGIC_MONITOR_ERROR	546
EventType: PH_JAVA_AGENT_WEBSENSE_EMAIL_MISSING_LOGDB	546

EventType: PH_JAVA_AGENT_WEBSSENSE_JDBC_PULL_ERROR	546
EventType: PH_JAVA_AGENT_WEBSSENSE_MAIL_CONN_ERROR	546
EventType: PH_JAVA_AGENT_WEBSSENSE_MAIL_EXEC_ERROR	547
EventType: PH_JAVA_AGENT_WEBSSENSE_MAIL_PULL_ERROR	547
EventType: PH_JAVA_AGENT_WEBSSENSE_WEB_CONN_ERROR	547
EventType: PH_JAVA_AGENT_WEBSSENSE_WEB_EXEC_ERROR	547
EventType: PH_JAVA_AGENT_WEBSSENSE_WEB_MISSING_LOGDB	547
EventType: PH_JAVA_AGENT_WEBSPHERE_CONN_ERROR	548
EventType: PH_JAVA_AGENT_WEBSPHERE_EXEC_ERROR	548
EventType: PH_JAVA_AGENT_WEBSPHERE_MONITOR_ERROR	548
EventType: PH_LINUX_AGENT_ACCOUT_MISSING	548
EventType: PH_LINUX_AGENT_BIND_PORT_FAILED	548
EventType: PH_LINUX_AGENT_CONFIG_ATTR_DECRYPTED_FAILED	549
EventType: PH_LINUX_AGENT_CONFIG_ATTR_ENCRYPTED_FAILED	549
EventType: PH_LINUX_AGENT_CONFIG_ATTR_NOT_FOUND	549
EventType: PH_LINUX_AGENT_CONFIG_MISS_ATTR	549
EventType: PH_LINUX_AGENT_CREATE_SOCKET_FAILED	550
EventType: PH_LINUX_AGENT_EXIT	550
EventType: PH_LINUX_AGENT_HOST_IP_GOT_FAILED	550
EventType: PH_LINUX_AGENT_INCREASE_RECV SOCK_BUF_MAX_FAILED	550
EventType: PH_LINUX_AGENT_INIT_FIM_FAILED	551
EventType: PH_LINUX_AGENT_INIT_HTTP_FAILED	551
EventType: PH_LINUX_AGENT_LOG_GENERIC	551
EventType: PH_LINUX_AGENT_NEW_FIM_LOADED	551
EventType: PH_LINUX_AGENT_OPEN_FILE_FAILED	552
EventType: PH_LINUX_AGENT_OPEN_PORT_FAILED	552
EventType: PH_LINUX_AGENT_PWD_MISSING	552
EventType: PH_LINUX_AGENT_RECV_ERROR	552
EventType: PH_LINUX_AGENT_REGISSTER_FAILED	553
EventType: PH_LINUX_AGENT_TEMPLATE_STATUS	553
EventType: PH_LINUX_AGENT_UNINSTALL	553
EventType: PH_LINUX_AGENT_UPLOAD_FILE_FAILED	553
EventType: PH_LINUX_AGENT_UPLOAD_FILE_SUCCESS	554
EventType: PH_LINUX_AGENT_USER_FILE_LOG_GENERIC	554
EventType: PH_LINUX_AGENT_VERIFIER_ERROR	554
EventType: PH_NETFLOW_BAD_FLOW	555
EventType: PH_NETFLOW_BAD_FLOW_END	555
EventType: PH_NETFLOW_BAD_HEADER_PROTOCOL	555
EventType: PH_NETFLOW_BAD_PACKET	555
EventType: PH_NETFLOW_BAD_RECORD	555
EventType: PH_NETFLOW_BAD_TYPE	556
EventType: PH_NETFLOW_BAD_VER	556
EventType: PH_NETFLOW_EXCEPTION	556
EventType: PH_SYSTEM_DEVAPP_EVENTS_PER_SEC	556
EventType: PH_SYSTEM_DEVAPP_NO_EVENTS	557
EventType: PH_SYSTEM_DEVICE_NO_EVENTS	557
EventType: PH_SYSTEM_EPS_GLOBAL	558
EventType: PH_SYSTEM_EPS_NODE	558
EventType: PH_SYSTEM_EPS_ORG	559

EventType: PH_SYSTEM_EVENTS_FWD_STAT	560
EventType: PH_SYSTEM_EVENTS_PER_SEC	561
EventType: PH_SYSTEM_EVENTS_VIA_ZMQ_EPS	561
EventType: PH_SYSTEM_INTERNAL_EVENTS_PER_SEC	562
EventType: PH_SYSTEM_IP_EVENTS_PER_SEC	562
EventType: PH_SYSTEM_PERF_EVENTS_PER_SEC	562
EventType: PH_SYSTEM_STORED_EVENTS_PER_SEC	563
EventType: PH_SYSTEM_SUMM_EVENTS_STORED_EPS	563
EventType: PH_VA_EVENTS_PER_SEC	563
Identity and Location Logs	565
EventType: PH_IDENTITYMASTER_HTTP_UPLOAD_ERROR	565
EventType: PH_IDENTITYMASTER_INIT_ERROR	565
EventType: PH_IDENTITYWORKER_ATTRIB_ERROR	566
EventType: PH_IDENTITYWORKER_EVT_LOAD_ERROR	566
EventType: PH_IDENTITYWORKER_EVT_SEND_ERROR	566
EventType: PH_IDENTITYWORKER_INIT_ERROR	567
EventType: PH_IDENTITYWORKER_PARAM_ERROR	567
EventType: PH_IDENTITYWORKER_PROCESSING_EPS	567
EventType: PH_IDENTITYWORKER_SS_OBTAIN_ERROR	567
License Logs	569
EventType: PH_CLUSTER_NO_LICENSE	569
EventType: PH_COLLECTOR_LICENSE_UPDATE	569
EventType: PH_LICENSE_ERROR	569
EventType: PH_LICENSE_INFO_FAILURE	570
EventType: PH_LICENSE_INFO_INVALIDATED	570
EventType: PH_LICENSE_NOT_EXIST	570
EventType: PH_MODULE_LICENSE_FAILURE	570
EventType: PH_MONITOR_LICENSE_ERROR	571
EventType: PH_MONITOR_QUERY_LICENSE_FAILED	571
EventType: PH_MONITOR_REPORTSERVER_LICENSE_INVALID	571
EventType: PH_PARSER_GLOBAL_LICENSE_EXCEED	571
EventType: PH_SYSTEM_DISK_USAGE_EXCEED_LICENSE	572
EventType: PH_SYSTEM_EVENT_RATE_EXCEED_LICENSE	572
EventType: PH_TASK_NO_LICENSE	572
EventType: PH_VA_LICENSE_UPDATE	572
Parser Logs	574
EventType: PH_EVENT_ATTR_XML_ISSUE	576
EventType: PH_LIBEVENT_BUFFER_OVERFLOW	576
EventType: PH_LIBEVENT_IP_TYPE_INVALID	576
EventType: PH_LIBEVENT_UNKNOWN_ATTR_ID	576
EventType: PH_LIBEVENT_UNKNOWN_ATTR_NAME	576
EventType: PH_NO_PARSER_FOR_EVENT	576
EventType: PH_PARSER_BIND_PORT_FAILURE	577
EventType: PH_PARSER_DATA_SIZE_OVERFLOW	577
EventType: PH_PARSER_DIR_OPEN_FAILURE	577
EventType: PH_PARSER_EVENT_PARSER_ERROR	578
EventType: PH_PARSER_EVENT_SERIALIZE_ERROR	578
EventType: PH_PARSER_FILE_DELETE_FAILURE	578

EventType: PH_PARSER_FILE_DELETE_FAILURE_RENAME	578
EventType: PH_PARSER_FILE_INVALID_FORMAT	579
EventType: PH_PARSER_FILE_INVALID_HEADER	579
EventType: PH_PARSER_FILE_NOT_EXIST	579
EventType: PH_PARSER_FILE_OPEN_FAILURE	580
EventType: PH_PARSER_FILE_PARSE_FAILURE	580
EventType: PH_PARSER_FILE_READ_FAILURE	581
EventType: PH_PARSER_FILE_RENAME_FAILURE	581
EventType: PH_PARSER_FILE_SIZE_MISMATCH	581
EventType: PH_PARSER_FILE_STAT_FAILURE	582
EventType: PH_PARSER_FILE_WRITE_FAILURE	582
EventType: PH_PARSER_GEO_WRONG_ATTR_NUMBER	582
EventType: PH_PARSER_GEO_WRONG_CACHE_NUMBER	582
EventType: PH_PARSER_GET_PROCESS_ERROR	583
EventType: PH_PARSER_HTTP_RESPONSE_ERROR	583
EventType: PH_PARSER_HTTP_UPLOAD_FAILURE	583
EventType: PH_PARSER_INIT_DEV_CRED_FAILED	583
EventType: PH_PARSER_INIT_FAILURE	584
EventType: PH_PARSER_INVALID_CSV	584
EventType: PH_PARSER_INVALID_EXT_LOG_PROTO	584
EventType: PH_PARSER_INVALID_ORG_NAME	584
EventType: PH_PARSER_INVALID_PHOENIX_CONFIG	585
EventType: PH_PARSER_IP_TYPE_INVALID	585
EventType: PH_PARSER_JSON_PARSE_FAILURE	585
EventType: PH_PARSER_MALLOC_FAILURE	586
EventType: PH_PARSER_PACK_EVENT_ERROR	586
EventType: PH_PARSER_RAWEVENT_TOO_LARGER	586
EventType: PH_PARSER_REST_PARSE_ERROR	586
EventType: PH_PARSER_RUN_PROCESS_ERROR	587
EventType: PH_PARSER_SEND_EVENT_FAILURE	587
EventType: PH_PARSER_SEND_TO_DISCOV_FAILURE	587
EventType: PH_PARSER_SEND_TO_MONITOR_FAILURE	587
EventType: PH_PARSER_SET_USER_ID_FAILURE	587
EventType: PH_PARSER_SHARED_STORE_ERROR	587
EventType: PH_PARSER_SNMPTRAP_INIT_FAILURE	588
EventType: PH_PARSER_SOCKET_ERROR	588
EventType: PH_PARSER_SOCKET_RECV_ERROR	588
EventType: PH_PARSER_SOCKET_SELECT_ERROR	589
EventType: PH_PARSER_SPAWN_THREAD_FAILURE	589
EventType: PH_PARSER_SSL_ACCEPT_ERROR	589
EventType: PH_PARSER_SSL_CERT_LOAD_ERROR	590
EventType: PH_PARSER_TCP_SOCKET_ACCEPT_ERROR	590
EventType: PH_PARSER_TEST_RULES_PARSE_ALL_EVENTS_BEGIN	590
EventType: PH_PARSER_TEST_RULES_PARSE_ALL_EVENTS_END	590
EventType: PH_PARSER_TEST_RULES_PARSE_ONE_EVENT_BEGIN	591
EventType: PH_PARSER_TEST_RULES_PARSE_ONE_EVENT_END	591
EventType: PH_PARSER_TOO_MANY_UNKNOWN_EVENTS	591
EventType: PH_PARSER_UPDATE_FAILURE	592
EventType: PH_PARSER_USE_ERROR_BEFORE_INIT	592

EventType: PH_PARSER_WRONG_EVENT_SIZE	593
EventType: PH_PARSER_WRONG_PARAMETER	593
EventType: PH_PARSER_WTAP_ERR_BAD_FILE	593
EventType: PH_PARSER_WTAP_ERR_CANT_OPEN	593
EventType: PH_PARSER_WTAP_ERR_COMPRESSION_NOT_SUPPORTED	594
EventType: PH_PARSER_WTAP_ERR_DECOMPRESS	594
EventType: PH_PARSER_WTAP_ERR_ENCAP_PER_PACKET_UNSUPPORTED	594
EventType: PH_PARSER_WTAP_ERR_FILE_UNKNOWN_FORMAT	595
EventType: PH_PARSER_WTAP_ERR_NOT_REGULAR_FILE	595
EventType: PH_PARSER_WTAP_ERR_RANDOM_OPEN_PIPE	595
EventType: PH_PARSER_WTAP_ERR_SHORT_READ	596
EventType: PH_PARSER_WTAP_ERR_SHORT_WRITE	596
EventType: PH_PARSER_WTAP_ERR_UNSUPPORTED	596
EventType: PH_PARSER_XML_PARSE_ERROR	597
EventType: PH_PARSER_XML_PARSE_FAILURE	597
EventType: PH_PARSE_CONFIG_CHANGE_FAILED	597
EventType: PH_VULN_LOAD_ERROR	598
EventType: PH_VULN_UPDATE_ERROR	598

Performance and Availability Monitoring Logs 599

EventType: PH_DEV_MON_ACME_PACKET_SESSION_AGENT_STATUS	615
EventType: PH_DEV_MON_ACME_PACKET_SYS_STATUS	616
EventType: PH_DEV_MON_APP_APACHE_MET	617
EventType: PH_DEV_MON_APP_ASPNET_MET	618
EventType: PH_DEV_MON_APP_DHCP_MET	619
EventType: PH_DEV_MON_APP_DNS_MET	620
EventType: PH_DEV_MON_APP_ICA_SESS_MET	621
EventType: PH_DEV_MON_APP_IIS_MET	622
EventType: PH_DEV_MON_APP_MSEXCH_ERR_MET	623
EventType: PH_DEV_MON_APP_MSEXCH_ISDB_INST_MET	624
EventType: PH_DEV_MON_APP_MSEXCH_ISDB_MET	625
EventType: PH_DEV_MON_APP_MSEXCH_MBOX_MET	626
EventType: PH_DEV_MON_APP_MSEXCH_MET	626
EventType: PH_DEV_MON_APP_MSEXCH_REPL_MET	627
EventType: PH_DEV_MON_APP_MSEXCH_SMTP_MET	628
EventType: PH_DEV_MON_APP_MSEXCH_STORE_INTF_MET	629
EventType: PH_DEV_MON_APP_MSEXCH_SUBMIT_MET	630
EventType: PH_DEV_MON_APP_MSEXCH_TRANS_MET	631
EventType: PH_DEV_MON_APP_MSEXCH_WS_MET	632
EventType: PH_DEV_MON_APP_NTDS_MET	632
EventType: PH_DEV_MON_ARUBA_WLAN_RADIO_METRIC	633
EventType: PH_DEV_MON_AUTH_STATS	634
EventType: PH_DEV_MON_AUTO_SVC_START_TO_STOP	635
EventType: PH_DEV_MON_AUTO_SVC_STOP	636
EventType: PH_DEV_MON_AUTO_SVC_STOP_TO_START	636
EventType: PH_DEV_MON_BC_PROXY_METRIC	636
EventType: PH_DEV_MON_BGP_NBR_STATUS	637
EventType: PH_DEV_MON_BOX_FILE_CREATE	638
EventType: PH_DEV_MON_BOX_FILE_DELETE	639
EventType: PH_DEV_MON_BOX_FILE_MODIFY	640

EventType: PH_DEV_MON_BOX_FILE_SHARE	640
EventType: PH_DEV_MON_CBQOS_CMSTAT	641
EventType: PH_DEV_MON_CBQOS_POLICESTAT	642
EventType: PH_DEV_MON_CBQOS_QUEUESTAT	643
EventType: PH_DEV_MON_CCM_CTI_STAT	644
EventType: PH_DEV_MON_CCM_CTI_STAT_CHANGE	644
EventType: PH_DEV_MON_CCM_DEL_CTI	645
EventType: PH_DEV_MON_CCM_DEL_GW	645
EventType: PH_DEV_MON_CCM_DEL_H323	646
EventType: PH_DEV_MON_CCM_DEL_MEDIA	646
EventType: PH_DEV_MON_CCM_DEL_SIP_TRUNK	647
EventType: PH_DEV_MON_CCM_DEL_VM	647
EventType: PH_DEV_MON_CCM_GLOBAL_INFO	648
EventType: PH_DEV_MON_CCM_GW_STAT	649
EventType: PH_DEV_MON_CCM_GW_STAT_CHANGE	649
EventType: PH_DEV_MON_CCM_H323_STAT	650
EventType: PH_DEV_MON_CCM_H323_STAT_CHANGE	651
EventType: PH_DEV_MON_CCM_MEDIA_STAT	651
EventType: PH_DEV_MON_CCM_MEDIA_STAT_CHANGE	652
EventType: PH_DEV_MON_CCM_NEW_CTI	652
EventType: PH_DEV_MON_CCM_NEW_GW	653
EventType: PH_DEV_MON_CCM_NEW_H323	653
EventType: PH_DEV_MON_CCM_NEW_MEDIA	654
EventType: PH_DEV_MON_CCM_NEW_SIP_TRUNK	654
EventType: PH_DEV_MON_CCM_NEW_VM	655
EventType: PH_DEV_MON_CCM_SIP_TRUNK_STAT	655
EventType: PH_DEV_MON_CCM_VM_STAT	656
EventType: PH_DEV_MON_CCM_VM_STAT_CHANGE	657
EventType: PH_DEV_MON_CHANGE_CUST_CONFIG	658
EventType: PH_DEV_MON_CHANGE_INST_SW	658
EventType: PH_DEV_MON_CHANGE_RUN_CONFIG	659
EventType: PH_DEV_MON_CHANGE_RUN_SW	659
EventType: PH_DEV_MON_CHANGE_STARTUP_CONFIG	659
EventType: PH_DEV_MON_CISCO_NBAR_STAT	660
EventType: PH_DEV_MON_CISCO_RAS_VPN_MET	661
EventType: PH_DEV_MON_CISCO_VPN_P1_TUNNEL_MET	662
EventType: PH_DEV_MON_CISCO_VPN_P2_TUNNEL_MET	663
EventType: PH_DEV_MON_CISCO_WLAN_RADIO_METRIC	664
EventType: PH_DEV_MON_CITRIX_SDWAN_INTF	665
EventType: PH_DEV_MON_CITRIX_SDWAN_LINK	666
EventType: PH_DEV_MON_CLARION_ARRAY_UTIL	667
EventType: PH_DEV_MON_CLARION_DISK_HEALTH	668
EventType: PH_DEV_MON_CLARION_HOST_CONN	668
EventType: PH_DEV_MON_CLARION_LUN_UTIL	669
EventType: PH_DEV_MON_CLARION_PER_HOST_LUN_UTIL	670
EventType: PH_DEV_MON_CLARION_PORT_UTIL	671
EventType: PH_DEV_MON_CLARION_RG_UTIL	672
EventType: PH_DEV_MON_CLARION_SP_UTIL	673
EventType: PH_DEV_MON_CLARION_STORAGE_USAGE	674

EventType: PH_DEV_MON_CLARION_STORE_POOL_UTIL	674
EventType: PH_DEV_MON_CLARION_UNREG_HOST	675
EventType: PH_DEV_MON_CLOUD_SERVICE_HEARTBEAT	675
EventType: PH_DEV_MON_CMDB_DISK_PRUNE_FAILED	676
EventType: PH_DEV_MON_CMDB_DISK_PRUNE_SUCCESS	676
EventType: PH_DEV_MON_CUST_FILE_CHANGE_ATTRIB	676
EventType: PH_DEV_MON_CUST_FILE_CHANGE_CONTENT	677
EventType: PH_DEV_MON_CUST_FILE_CREATE	677
EventType: PH_DEV_MON_CUST_FILE_DELETE	677
EventType: PH_DEV_MON_CUST_FILE_SCAN	677
EventType: PH_DEV_MON_CUST_TARGET_FILE_CHANGE	677
EventType: PH_DEV_MON_DATASTORE_UTIL	677
EventType: PH_DEV_MON_DCDIAG	678
EventType: PH_DEV_MON_DDNS_UPDATE_STAT	678
EventType: PH_DEV_MON_DELLFORCE10_EXT_INTF_UTIL	678
EventType: PH_DEV_MON_DELL_BLADE_POWER_STATUS	679
EventType: PH_DEV_MON_DELL_BLADE_PSU_STATUS	680
EventType: PH_DEV_MON_DELTA_CONFIG	680
EventType: PH_DEV_MON_DGA_DETECTED	681
EventType: PH_DEV_MON_DHCP_SUBNET_USAGE	682
EventType: PH_DEV_MON_DISK_IO_UTIL	682
EventType: PH_DEV_MON_DISK_MON_SKIP	683
EventType: PH_DEV_MON_DNS_CLUST_REPL_STAT	683
EventType: PH_DEV_MON_DNS_PERF_STAT	684
EventType: PH_DEV_MON_DNS_ZONETX_MET	685
EventType: PH_DEV_MON_DST_AD_REPL_STAT	685
EventType: PH_DEV_MON_EBS_METRIC	686
EventType: PH_DEV_MON_EC2_INSTANCE_DOWN	686
EventType: PH_DEV_MON_EC2_INSTANCE_UP	687
EventType: PH_DEV_MON_EC2_METRIC	687
EventType: PH_DEV_MON EMC_DATADOMAIN_DISK_PERF	688
EventType: PH_DEV_MON EMC_DATADOMAIN_OVERALL_PERF	689
EventType: PH_DEV_MON_EQL_CONN_MET	690
EventType: PH_DEV_MON_EQL_DISK_HEALTH	690
EventType: PH_DEV_MON_EQL_DISK_MET	691
EventType: PH_DEV_MON_EQL_GROUP_MET	691
EventType: PH_DEV_MON_ESX_DATASTORE_IO	692
EventType: PH_DEV_MON_ESX_DISK_IO	692
EventType: PH_DEV_MON_ESX_DISK_UTIL	692
EventType: PH_DEV_MON_ESX_STATE	693
EventType: PH_DEV_MON_ESX_UPTIME	693
EventType: PH_DEV_MON_EUM_FAIL	693
EventType: PH_DEV_MON_EUM_INTERNAL_ERR	694
EventType: PH_DEV_MON_EUM_STATUS	695
EventType: PH_DEV_MON_EUM_SUCCESS	696
EventType: PH_DEV_MON_F5_ACTIVE_CONN	697
EventType: PH_DEV_MON_F5_LTM_NODE_STAT	698
EventType: PH_DEV_MON_F5_LTM_POOL_MEMBER_STAT	699
EventType: PH_DEV_MON_F5_LTM_POOL_STAT	701

EventType: PH_DEV_MON_F5_LTM_VIRT_ADDR_STAT	703
EventType: PH_DEV_MON_F5_LTM_VIRT_SERVER_STAT	704
EventType: PH_DEV_MON_F5_NEW_CONN	706
EventType: PH_DEV_MON_F5_RAM_CACHE	707
EventType: PH_DEV_MON_F5_THROUGHPUT	707
EventType: PH_DEV_MON_F5_TMM_MEM_UTIL	708
EventType: PH_DEV_MON_FGT_SEC_POSTURE_DETAILS	709
EventType: PH_DEV_MON_FGT_SEC_POSTURE_DETECTED_ENDPOINTS	709
EventType: PH_DEV_MON_FGT_SEC_POSTURE_FABRIC_GRADE	710
EventType: PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_GRADE	710
EventType: PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_STATS	711
EventType: PH_DEV_MON_FGT_SEC_POSTURE_PER_DEVICE_STATS	712
EventType: PH_DEV_MON_FGT_USER_INFO	712
EventType: PH_DEV_MON_FILE_CONTENT_CHANGE	714
EventType: PH_DEV_MON_FIREAMP_DISCOVERY_CLIENT_APP	714
EventType: PH_DEV_MON_FIREAMP_DISCOVERY_NETWORK_PROTOCOL	715
EventType: PH_DEV_MON_FIREAMP_DISCOVERY_OS_FINGERPRINT	715
EventType: PH_DEV_MON_FIREAMP_DISCOVERY_SERVER	716
EventType: PH_DEV_MON_FIREAMP_FILE	716
EventType: PH_DEV_MON_FIREAMP_IMPACT_FLAG	718
EventType: PH_DEV_MON_FIREAMP_INTRUSION	719
EventType: PH_DEV_MON_FIREAMP_MALWARE	721
EventType: PH_DEV_MON_FIREAMP_USER_LOGIN	723
EventType: PH_DEV_MON_FORTIAP_INTF_UTIL	724
EventType: PH_DEV_MON_FORTIAP_PERF	724
EventType: PH_DEV_MON_FORTIAP_STAT	724
EventType: PH_DEV_MON_FORTIGATE_INTF_UTIL	725
EventType: PH_DEV_MON_FORTIGATE_PERF	725
EventType: PH_DEV_MON_FORTIMAIL_SESSION_COUNT	726
EventType: PH_DEV_MON_FORTIMAIL_SYS_LOAD	726
EventType: PH_DEV_MON_FORTINET_PROCESSOR_USAGE	726
EventType: PH_DEV_MON_FORTINET_QOS	727
EventType: PH_DEV_MON_FORTISWITCH_PERF	728
EventType: PH_DEV_MON_FORTIWLC_QOS_STAT	728
EventType: PH_DEV_MON_FORTIWLC_STATIONS	729
EventType: PH_DEV_MON_FORTIWLC_SYS_THRUPUT	730
EventType: PH_DEV_MON_FPC_LIEBERT_METRIC	730
EventType: PH_DEV_MON_FW_CONN_UTIL	732
EventType: PH_DEV_MON_GITHUB_BRANCH_EVENT	732
EventType: PH_DEV_MON_GITHUB_COMMIT	733
EventType: PH_DEV_MON_GITHUB_EVENT	734
EventType: PH_DEV_MON_GITHUB_FORK_REPOSITORY_EVENT	735
EventType: PH_DEV_MON_GITHUB_ISSUE_EVENT	736
EventType: PH_DEV_MON_GITHUB_MEMBER_EVENT	737
EventType: PH_DEV_MON_GITHUB_ORG_EVENT	738
EventType: PH_DEV_MON_GITHUB_PROJECT_EVENT	739
EventType: PH_DEV_MON_GITHUB_PULL_REQUEST_EVENT	740
EventType: PH_DEV_MON_GITHUB_PULL_REQUEST_REVIEW_EVENT	741
EventType: PH_DEV_MON_GITHUB_REPOSITORY_EVENT	742

EventType: PH_DEV_MON_GITHUB_TAG_EVENT	743
EventType: PH_DEV_MON_GLASSFISH_APP	744
EventType: PH_DEV_MON_GLASSFISH_CONN_STAT	745
EventType: PH_DEV_MON_GLASSFISH_CPU	745
EventType: PH_DEV_MON_GLASSFISH_DB_POOL	745
EventType: PH_DEV_MON_GLASSFISH_EJB	745
EventType: PH_DEV_MON_GLASSFISH_JMS	745
EventType: PH_DEV_MON_GLASSFISH_MEMORY	745
EventType: PH_DEV_MON_GLASSFISH_REQUEST_PROCESSOR	746
EventType: PH_DEV_MON_GLASSFISH_SERVLET	746
EventType: PH_DEV_MON_GLASSFISH_SESSION	746
EventType: PH_DEV_MON_GLASSFISH_THREAD_POOL	746
EventType: PH_DEV_MON_HARDWARE_STATUS	746
EventType: PH_DEV_MON_HOST_PERF_STATE	747
EventType: PH_DEV_MON_HVAC_LIEBERT_METRIC	747
EventType: PH_DEV_MON_HW_AIRFLOW	748
EventType: PH_DEV_MON_HW_AMP	749
EventType: PH_DEV_MON_HW_AUDIO	749
EventType: PH_DEV_MON_HW_CAMERA_MOTION	750
EventType: PH_DEV_MON_HW_CHASSIS_COMP_STAT	751
EventType: PH_DEV_MON_HW_CURRENT	751
EventType: PH_DEV_MON_HW_DEWPT	752
EventType: PH_DEV_MON_HW_DOOR_SWITCH	752
EventType: PH_DEV_MON_HW_DRY_CONTACT	753
EventType: PH_DEV_MON_HW_FAN_SPEED	753
EventType: PH_DEV_MON_HW_HUMIDITY	754
EventType: PH_DEV_MON_HW_POWER	754
EventType: PH_DEV_MON_HW_PS_STAT	755
EventType: PH_DEV_MON_HW_STACK_UNIT	755
EventType: PH_DEV_MON_HW_STATUS	756
EventType: PH_DEV_MON_HW_STATUS_AIRFLOW_CRIT	759
EventType: PH_DEV_MON_HW_STATUS_AIRFLOW_WARN	760
EventType: PH_DEV_MON_HW_STATUS_ALARMDEVICE_CRIT	761
EventType: PH_DEV_MON_HW_STATUS_ALARMDEVICE_WARN	761
EventType: PH_DEV_MON_HW_STATUS_AMP_CRIT	762
EventType: PH_DEV_MON_HW_STATUS_AMP_WARN	763
EventType: PH_DEV_MON_HW_STATUS_AUDIO_CRIT	763
EventType: PH_DEV_MON_HW_STATUS_AUDIO_WARN	764
EventType: PH_DEV_MON_HW_STATUS_BATTERY_CRIT	765
EventType: PH_DEV_MON_HW_STATUS_BATTERY_WARN	765
EventType: PH_DEV_MON_HW_STATUS_CAMERA_MOTION_CRIT	766
EventType: PH_DEV_MON_HW_STATUS_CAMERA_MOTION_WARN	767
EventType: PH_DEV_MON_HW_STATUS_DEWPT_CRIT	767
EventType: PH_DEV_MON_HW_STATUS_DEWPT_WARN	768
EventType: PH_DEV_MON_HW_STATUS_DISK_CRIT	769
EventType: PH_DEV_MON_HW_STATUS_DISK_WARN	769
EventType: PH_DEV_MON_HW_STATUS_DOOR_SWITCH_CRIT	770
EventType: PH_DEV_MON_HW_STATUS_DOOR_SWITCH_WARN	771
EventType: PH_DEV_MON_HW_STATUS_DRY_CONTACT_CRIT	771

EventType: PH_DEV_MON_HW_STATUS_DRY_CONTACT_WARN	772
EventType: PH_DEV_MON_HW_STATUS_FAN_CRIT	773
EventType: PH_DEV_MON_HW_STATUS_FAN_WARN	773
EventType: PH_DEV_MON_HW_STATUS_FILESYSTEM_CRIT	774
EventType: PH_DEV_MON_HW_STATUS_FILESYSTEM_WARN	775
EventType: PH_DEV_MON_HW_STATUS_GEN_NUMERIC_SENSOR_CRIT	775
EventType: PH_DEV_MON_HW_STATUS_GEN_NUMERIC_SENSOR_WARN	776
EventType: PH_DEV_MON_HW_STATUS_GEN_STATE_SENSOR_CRIT	777
EventType: PH_DEV_MON_HW_STATUS_GEN_STATE_SENSOR_WARN	777
EventType: PH_DEV_MON_HW_STATUS_HUMIDITY_CRIT	778
EventType: PH_DEV_MON_HW_STATUS_HUMIDITY_WARN	779
EventType: PH_DEV_MON_HW_STATUS_INPUTCONTACT_CRIT	779
EventType: PH_DEV_MON_HW_STATUS_INPUTCONTACT_WARN	780
EventType: PH_DEV_MON_HW_STATUS_LCC_CRIT	781
EventType: PH_DEV_MON_HW_STATUS_LCC_WARN	781
EventType: PH_DEV_MON_HW_STATUS_LINK_CRIT	782
EventType: PH_DEV_MON_HW_STATUS_LINK_WARN	783
EventType: PH_DEV_MON_HW_STATUS_MEMBEACON_CRIT	783
EventType: PH_DEV_MON_HW_STATUS_MEMBEACON_WARN	784
EventType: PH_DEV_MON_HW_STATUS_MEMORY_CRIT	785
EventType: PH_DEV_MON_HW_STATUS_MEMORY_WARN	785
EventType: PH_DEV_MON_HW_STATUS_MEMOUTLET_CRIT	786
EventType: PH_DEV_MON_HW_STATUS_MEMOUTLET_WARN	787
EventType: PH_DEV_MON_HW_STATUS_MEMOUTPUT_CRIT	787
EventType: PH_DEV_MON_HW_STATUS_MEMOUTPUT_WARN	788
EventType: PH_DEV_MON_HW_STATUS_MEMSENSOR_CRIT	789
EventType: PH_DEV_MON_HW_STATUS_MEMSENSOR_WARN	789
EventType: PH_DEV_MON_HW_STATUS_MISC_CRIT	790
EventType: PH_DEV_MON_HW_STATUS_MISC_WARN	791
EventType: PH_DEV_MON_HW_STATUS_OUTLET_CRIT	791
EventType: PH_DEV_MON_HW_STATUS_OUTLET_WARN	792
EventType: PH_DEV_MON_HW_STATUS_OUTPUTRELAY_CRIT	793
EventType: PH_DEV_MON_HW_STATUS_OUTPUTRELAY_WARN	793
EventType: PH_DEV_MON_HW_STATUS_PORT_CRIT	794
EventType: PH_DEV_MON_HW_STATUS_PORT_WARN	795
EventType: PH_DEV_MON_HW_STATUS_POWERSUPPLY_CRIT	795
EventType: PH_DEV_MON_HW_STATUS_POWERSUPPLY_WARN	796
EventType: PH_DEV_MON_HW_STATUS_POWER_ENCLOSURE_CRIT	797
EventType: PH_DEV_MON_HW_STATUS_POWER_ENCLOSURE_WARN	797
EventType: PH_DEV_MON_HW_STATUS_PROBE_CRIT	798
EventType: PH_DEV_MON_HW_STATUS_PROBE_WARN	799
EventType: PH_DEV_MON_HW_STATUS_SLOT_CRIT	799
EventType: PH_DEV_MON_HW_STATUS_SLOT_WARN	800
EventType: PH_DEV_MON_HW_STATUS_STACKUNIT_CRIT	801
EventType: PH_DEV_MON_HW_STATUS_STACKUNIT_WARN	801
EventType: PH_DEV_MON_HW_STATUS_TEMP_CRIT	802
EventType: PH_DEV_MON_HW_STATUS_TEMP_WARN	803
EventType: PH_DEV_MON_HW_STATUS_VOLTAGE_CRIT	803
EventType: PH_DEV_MON_HW_STATUS_VOLTAGE_WARN	804

EventType: PH_DEV_MON_HW_TEMP	805
EventType: PH_DEV_MON_HW_VOLTAGE	806
EventType: PH_DEV_MON_HYPERV_CPU_GUEST_VIRTUAL_PROC	806
EventType: PH_DEV_MON_HYPERV_CPU_LOGICAL_PROC	807
EventType: PH_DEV_MON_HYPERV_CPU_ROOT_VIRTUAL_PROC	807
EventType: PH_DEV_MON_HYPERV_MEM_OVERALL	807
EventType: PH_DEV_MON_HYPERV_MEM_PARTITION	807
EventType: PH_DEV_MON_HYPERV_MEM_PARTITION_PER_VM	807
EventType: PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION	807
EventType: PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION_ROOT	808
EventType: PH_DEV_MON_HYPERV_MEM_VID_PARTITION	808
EventType: PH_DEV_MON_HYPERV_MEM_VID_PARTITION_PER_VM	808
EventType: PH_DEV_MON_HYPERV_NET_LEGACY_ADAPTER	808
EventType: PH_DEV_MON_HYPERV_NET_VIRTUAL_ADAPTER	808
EventType: PH_DEV_MON_HYPERV_NET_VIRTUAL_SWITCH	809
EventType: PH_DEV_MON_HYPERV_OVERALL_HEALTH	809
EventType: PH_DEV_MON_HYPERV_OVERALL_SYSINFO	809
EventType: PH_DEV_MON_HYPERV_STORAGE_LOGICAL_DISK	809
EventType: PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_IDE_CONTROLLER	809
EventType: PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_STORAGE	809
EventType: PH_DEV_MON_INCOMING_EXCEED_GUARANTEED	810
EventType: PH_DEV_MON_INTF_ADMIN_DOWN_TO_UP	810
EventType: PH_DEV_MON_INTF_ADMIN_UP_TO_DOWN	811
EventType: PH_DEV_MON_INTF_OPER_DOWN_TO_UP	811
EventType: PH_DEV_MON_INTF_OPER_UP_TO_DOWN	811
EventType: PH_DEV_MON_INTF_USAGE_TOTAL	812
EventType: PH_DEV_MON_IPSLA_HTTP_MET	812
EventType: PH_DEV_MON_IPSLA_ICMP_MET	814
EventType: PH_DEV_MON_IPSLA_MET	814
EventType: PH_DEV_MON_IPSLA_UDP_MET	816
EventType: PH_DEV_MON_IPSLA_VOIP_MET	817
EventType: PH_DEV_MON_IRONPORT_MAIL_USAGE	818
EventType: PH_DEV_MON_ISILON_CLUSTER_HEALTH	819
EventType: PH_DEV_MON_ISILON_CLUSTER_MEMBERSHIP_CHANGE	820
EventType: PH_DEV_MON_ISILON_CLUSTER_QUOTA	820
EventType: PH_DEV_MON_ISILON_CLUSTER_SNAPSHOT	821
EventType: PH_DEV_MON_ISILON_NODE_DISK_PERF	822
EventType: PH_DEV_MON_ISILON_NODE_HEALTH	822
EventType: PH_DEV_MON_ISILON_NODE_PROTO_PERF	823
EventType: PH_DEV_MON_JBOSS_APP	824
EventType: PH_DEV_MON_JBOSS_CPU	824
EventType: PH_DEV_MON_JBOSS_DB_POOL	825
EventType: PH_DEV_MON_JBOSS_EJB	825
EventType: PH_DEV_MON_JBOSS_MEMORY	825
EventType: PH_DEV_MON_JBOSS_REQUEST_PROCESSOR	825
EventType: PH_DEV_MON_JBOSS_SERVLET	825
EventType: PH_DEV_MON_JBOSS_SESSION	825
EventType: PH_DEV_MON_JBOSS_THREAD_POOL	826
EventType: PH_DEV_MON_LOG_ALL_DEVICE_DELAY_HIGH	826

EventType: PH_DEV_MON_LOG_ALL_DEVICE_DELAY_LOW	826
EventType: PH_DEV_MON_LOG_DEVICE_DELAY_HIGH	826
EventType: PH_DEV_MON_LOG_DEVICE_DELAY_LOW	827
EventType: PH_DEV_MON_MANUAL_SVC_START_TO_STOP	827
EventType: PH_DEV_MON_MANUAL_SVC_STOP	827
EventType: PH_DEV_MON_MANUAL_SVC_STOP_TO_START	828
EventType: PH_DEV_MON_NETAPP_AGGR_MET	828
EventType: PH_DEV_MON_NETAPP_CIFS_MET	829
EventType: PH_DEV_MON_NETAPP_CP_MET	829
EventType: PH_DEV_MON_NETAPP_DISK_HEALTH	830
EventType: PH_DEV_MON_NETAPP_DISK_MET	831
EventType: PH_DEV_MON_NETAPP_FCP_MET	831
EventType: PH_DEV_MON_NETAPP_ISCSI_MET	832
EventType: PH_DEV_MON_NETAPP_LUN_MET	833
EventType: PH_DEV_MON_NETAPP_NFS3_MET	833
EventType: PH_DEV_MON_NETAPP_NFS4_MET	834
EventType: PH_DEV_MON_NETAPP_NFS_MET	835
EventType: PH_DEV_MON_NETAPP_VOL_MET	835
EventType: PH_DEV_MON_NETBOTZ_HW_EMS_STATUS	836
EventType: PH_DEV_MON_NETBOTZ_HW_MODULE_SENSOR	837
EventType: PH_DEV_MON_NETBOTZ_HW_PROBE	838
EventType: PH_DEV_MON_NETSCALER_APP_FW	839
EventType: PH_DEV_MON_NETSCALER_SERVICE	840
EventType: PH_DEV_MON_NETSCALER_VIRT_SERVER	841
EventType: PH_DEV_MON_NET_INTF_UTIL	842
EventType: PH_DEV_MON_NIMBLE_GLOBAL_STAT	845
EventType: PH_DEV_MON_NUTANIX_CLUSTER_STATUS	845
EventType: PH_DEV_MON_NUTANIX_CONTAINER_INFO	846
EventType: PH_DEV_MON_NUTANIX_CTRLR_VM_RESOURCE	847
EventType: PH_DEV_MON_NUTANIX_DISK_STATUS	847
EventType: PH_DEV_MON_NUTANIX_DISK_TEMP	848
EventType: PH_DEV_MON_NUTANIX_SERVICE_STATUS	848
EventType: PH_DEV_MON_NUTANIX_STORAGE_POOL_INFO	849
EventType: PH_DEV_MON_OMI_PING_STAT	850
EventType: PH_DEV_MON OSPF_NBR_STATUS	850
EventType: PH_DEV_MON_PANASONIC_AERO_LOG_MON_STATUS	851
EventType: PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_HIGH	852
EventType: PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_LOW	852
EventType: PH_DEV_MON_PERFMON_DEVICE_DELAY_HIGH	852
EventType: PH_DEV_MON_PERFMON_DEVICE_DELAY_LOW	852
EventType: PH_DEV_MON_PERFMON_JOB_DELAY_HIGH	852
EventType: PH_DEV_MON_PERFMON_JOB_DELAY_LOW	852
EventType: PH_DEV_MON_PERF_MSSQL_BACKUP_INFO	853
EventType: PH_DEV_MON_PERF_MSSQL_BLOCKBY_INFO	853
EventType: PH_DEV_MON_PERF_MSSQL_CONFIG_INFO	853
EventType: PH_DEV_MON_PERF_MSSQL_ERROR_LOG_INFO	853
EventType: PH_DEV_MON_PERF_MSSQL_GEN_INFO	853
EventType: PH_DEV_MON_PERF_MSSQL_LOCK_INFO	854
EventType: PH_DEV_MON_PERF_MSSQL_PERDB	854

EventType: PH_DEV_MON_PERF_MSSQL_SYS	854
EventType: PH_DEV_MON_PERF_MSSQL_TOP_QUERIES	854
EventType: PH_DEV_MON_PERF_MYSQLDB	854
EventType: PH_DEV_MON_PERF_MYSQLDB_TABLESPACE	854
EventType: PH_DEV_MON_PERF_ORADB	855
EventType: PH_DEV_MON_PERF_ORADB_CLUSTER	855
EventType: PH_DEV_MON_PERF_ORADB_TABLESPACE	855
EventType: PH_DEV_MON_PERF_ORADB_TOP_QUERIES	855
EventType: PH_DEV_MON_PING_STAT	855
EventType: PH_DEV_MON_PING_STAT_SUPPRESSED	856
EventType: PH_DEV_MON_PORT_CLOSE	857
EventType: PH_DEV_MON_PORT_OPEN	857
EventType: PH_DEV_MON_PRINTER_OUTPUT_STATUS	858
EventType: PH_DEV_MON_PRINTER_SUPPLY_STATUS	858
EventType: PH_DEV_MON_PROC_CPU_UTIL	859
EventType: PH_DEV_MON_PROC_MEM_UTIL	859
EventType: PH_DEV_MON_PROC_RESOURCE_UTIL	859
EventType: PH_DEV_MON_PROC_START	860
EventType: PH_DEV_MON_PROC_STOP	861
EventType: PH_DEV_MON_QUALYS_WEB_APP_FW	861
EventType: PH_DEV_MON_RBD_BW	862
EventType: PH_DEV_MON_RBD_CONN	862
EventType: PH_DEV_MON_RBD_PEER_STAT	863
EventType: PH_DEV_MON_RBD_PER_PORT_BW	863
EventType: PH_DEV_MON_RBD_TOP_APP	864
EventType: PH_DEV_MON_RBD_TOP_DEST	864
EventType: PH_DEV_MON_RBD_TOP_SRC	865
EventType: PH_DEV_MON_RBD_TOP_TALKER	865
EventType: PH_DEV_MON_RDS_METRIC	866
EventType: PH_DEV_MON_RUCKUS_ACCESS_POINT_STAT	867
EventType: PH_DEV_MON_RUCKUS_CONTROLLER_STAT	868
EventType: PH_DEV_MON_RUCKUS_SSID_PERF	868
EventType: PH_DEV_MON_SERVERIRON_REAL_SERVER_STAT	869
EventType: PH_DEV_MON_SLB_METRIC	870
EventType: PH_DEV_MON_SNMP_PING_STAT	871
EventType: PH_DEV_MON_SRC_AD_REPL_STAT	871
EventType: PH_DEV_MON_STATUS	872
EventType: PH_DEV_MON_STORAGE_PORT_DOWN_TO_UP	872
EventType: PH_DEV_MON_STORAGE_PORT_UP_TO_DOWN	872
EventType: PH_DEV_MON_SYS_CPU_UTIL	873
EventType: PH_DEV_MON_SYS_DISK_FREE	874
EventType: PH_DEV_MON_SYS_DISK_TREND_DAY	874
EventType: PH_DEV_MON_SYS_DISK_TREND_MONTH	875
EventType: PH_DEV_MON_SYS_DISK_TREND_WEEK	876
EventType: PH_DEV_MON_SYS_DISK_UTIL	876
EventType: PH_DEV_MON_SYS_EXT_CMD	877
EventType: PH_DEV_MON_SYS_MEM_FREE	878
EventType: PH_DEV_MON_SYS_MEM_UTIL	878
EventType: PH_DEV_MON_SYS_PAGEFILE_USAGE	879

EventType: PH_DEV_MON_SYS_PER_CPU_UTIL	880
EventType: PH_DEV_MON_SYS_PROC_COUNT	880
EventType: PH_DEV_MON_SYS_RESTART	881
EventType: PH_DEV_MON_SYS_STAT	881
EventType: PH_DEV_MON_SYS_STATUS	882
EventType: PH_DEV_MON_SYS_SWAP_MEM_ERROR_MSG	882
EventType: PH_DEV_MON_SYS_UPTIME	883
EventType: PH_DEV_MON_SYS_VIRT_MEM_UTIL	883
EventType: PH_DEV_MON_TARGET_FILE_CONTENT_CHANGE	884
EventType: PH_DEV_MON_TOMCAT_CPU	884
EventType: PH_DEV_MON_TOMCAT_DB	884
EventType: PH_DEV_MON_TOMCAT_MEMORY	885
EventType: PH_DEV_MON_TOMCAT_REQUEST_PROCESSOR	885
EventType: PH_DEV_MON_TOMCAT_SERVLET	885
EventType: PH_DEV_MON_TOMCAT_SESSION	885
EventType: PH_DEV_MON_TOMCAT_THREAD_POOL	885
EventType: PH_DEV_MON_TRACEROUTE_STAT	886
EventType: PH_DEV_MON_UCS_HW_CHASSIS_STAT	886
EventType: PH_DEV_MON_UCS_HW_FAN_STAT	887
EventType: PH_DEV_MON_UCS_HW_MEMORY_STAT	888
EventType: PH_DEV_MON_UCS_HW_PROCESSOR_STAT	889
EventType: PH_DEV_MON_UCS_HW_PSU_STAT	890
EventType: PH_DEV_MON_UPS_METRIC	891
EventType: PH_DEV_MON_VMCLUSTER_CPU_UTIL	893
EventType: PH_DEV_MON_VMCLUSTER_DATASTORE_IO	893
EventType: PH_DEV_MON_VMCLUSTER_MEM_UTIL	893
EventType: PH_DEV_MON_VMCLUSTER_STATUS	893
EventType: PH_DEV_MON_VMRESPOOL_CPU_UTIL	893
EventType: PH_DEV_MON_VMRESPOOL_MEM_UTIL	894
EventType: PH_DEV_MON_VM_CPU_UTIL	894
EventType: PH_DEV_MON_VM_DATASTORE_IO	894
EventType: PH_DEV_MON_VM_DISK_IO	894
EventType: PH_DEV_MON_VM_DISK_UTIL	894
EventType: PH_DEV_MON_VM_MEM_UTIL	895
EventType: PH_DEV_MON_VM_NET_INTF_UTIL	895
EventType: PH_DEV_MON_VM_PER_CPU_UTIL	895
EventType: PH_DEV_MON_VM_SNAPSHOT	895
EventType: PH_DEV_MON_VM_STATE	895
EventType: PH_DEV_MON_VM_TOOLS_STATUS	895
EventType: PH_DEV_MON_VM_UPTIME	896
EventType: PH_DEV_MON_VPN_CONN	896
EventType: PH_DEV_MON_VPN_STATUS	896
EventType: PH_DEV_MON_WATCHGUARD_POLICY_STAT	897
EventType: PH_DEV_MON_WEBLOGIC_APP	898
EventType: PH_DEV_MON_WEBLOGIC_DB_POOL	898
EventType: PH_DEV_MON_WEBLOGIC_EJB	898
EventType: PH_DEV_MON_WEBLOGIC_GEN	898
EventType: PH_DEV_MON_WEBLOGIC_MEMORY	898
EventType: PH_DEV_MON_WEBLOGIC_SERVLET	898

EventType: PH_DEV_MON_WEBLOGIC_SESSION	899
EventType: PH_DEV_MON_WEBLOGIC_THREAD_POOL	899
EventType: PH_DEV_MON_WEBSPHERE_APP	899
EventType: PH_DEV_MON_WEBSPHERE_AUTHENTICATION	899
EventType: PH_DEV_MON_WEBSPHERE_CPU	899
EventType: PH_DEV_MON_WEBSPHERE_DB_POOL	900
EventType: PH_DEV_MON_WEBSPHERE_EJB	900
EventType: PH_DEV_MON_WEBSPHERE_MEMORY	900
EventType: PH_DEV_MON_WEBSPHERE_SERVLET	900
EventType: PH_DEV_MON_WEBSPHERE_THREAD_POOL	900
EventType: PH_DEV_MON_WEBSPHERE_TRANSACTION	900
EventType: PH_DEV_MON_WMI_PING_STAT	901
EventType: PH_JOB_STAT	901
EventType: PH_JOB_STATUS_XML_SEND_ERROR	902
EventType: PH_JOB_STATUS_XML_SENT	902
EventType: PH_JOB_STAT_SUPPRESSED	902
EventType: PH_MONITOR_ARCHIVE_GET_WORKER_FAILURE	903
EventType: PH_MONITOR_ARCHIVE_UPDATE_WORKER_FAILURE	903
EventType: PH_MONITOR_BEACONING_REGISTER_FAILURE	903
EventType: PH_MONITOR_CHECK_DEPENDENCY_FAILED	904
EventType: PH_MONITOR_CMD_FAILURE	904
EventType: PH_MONITOR_CMD_SEND_FAILURE	904
EventType: PH_MONITOR_COLLECTOR_REGISTER_FAILURE	905
EventType: PH_MONITOR_COLLECTOR_UPDATE_STATUS_FAILURE	905
EventType: PH_MONITOR_CONFIG_DOWNLOAD_FAILURE	905
EventType: PH_MONITOR_DBCLUSTER_SEND_COMMAND_FAILED	906
EventType: PH_MONITOR_DELETE_DR_FAILED	906
EventType: PH_MONITOR_DELETE_SECONDARY_ON_WORKER_FAILED	906
EventType: PH_MONITOR_DELETE_SUPER_FOLLOWER_FAILED	906
EventType: PH_MONITOR_DISPATCH_CMD_MISMATCH	906
EventType: PH_MONITOR_DOMAIN_CHANGE_XML_PARSE_FAILURE	907
EventType: PH_MONITOR_ENT_OR_SP_MODE_MISSING	907
EventType: PH_MONITOR_EXCESSIVE_DB_LOGIN_FAILURE	907
EventType: PH_MONITOR_FAILED_CONN_QUERYMASTER	907
EventType: PH_MONITOR_FILE_IO_ERROR	908
EventType: PH_MONITOR_FILE_PERMISSION_ERROR	908
EventType: PH_MONITOR_FILE_PERMISSION_WARNING	908
EventType: PH_MONITOR_FLIP_PRIMARY_FAILURE	909
EventType: PH_MONITOR_FSM_AGENT_UPDATE_PWD_ERROR	909
EventType: PH_MONITOR_GET_REPLICATION_PROGRESS_FAILED	909
EventType: PH_MONITOR_GET_UPTIME_ERROR	909
EventType: PH_MONITOR_HANDLE_TASK	910
EventType: PH_MONITOR_HARDWARE_SN_FORK_FAILURE	910
EventType: PH_MONITOR_HOST_UUID_READ_FAILURE	910
EventType: PH_MONITOR_HTTP_PULL_ERROR	910
EventType: PH_MONITOR_INIT_PROC_MODULE_NOT_FOUND	911
EventType: PH_MONITOR_INIT_SECONDARY_ON_WORKER_FAILED	911
EventType: PH_MONITOR_INIT_SUPER_FOLLOWER_FAILED	911
EventType: PH_MONITOR_INIT_SYSTEM_XML_PARSE_FAILURE	911

EventType: PH_MONITOR_JDBC_POOL_NOT_EXIST	912
EventType: PH_MONITOR_LIB_DEPENDENCY_WARNING	912
EventType: PH_MONITOR_LOAD_CONF_FROM_APP_SERVER_FAILED	912
EventType: PH_MONITOR_LOCAL_HOSTNAME_GET_FAILURE	912
EventType: PH_MONITOR_MEM_FILE_OPEN_FAILURE	913
EventType: PH_MONITOR_MISSING_MONITOR	913
EventType: PH_MONITOR_MMAP_FAILURE	913
EventType: PH_MONITOR_MOTNIROR_REGISTER_FAILURE	913
EventType: PH_MONITOR_NOTIFICATION_CLIENT_CONTACT_FAILURE	914
EventType: PH_MONITOR_NOTIFICATION_CMD_EMPTY	914
EventType: PH_MONITOR_NOTIFICATION_CMD_MISMATCH	914
EventType: PH_MONITOR_NOTIFICATION_RETURN_FAILURE	914
EventType: PH_MONITOR_PHOENIX_CONFIG_GLOBAL_MISSING	915
EventType: PH_MONITOR_PHOENIX_CONFIG_INVALID	915
EventType: PH_MONITOR_PROCESS_OWNER_NOT_ADMIN_ERROR	915
EventType: PH_MONITOR_RECVD_CONFIG_CHANGE	916
EventType: PH_MONITOR_RECVD_HEARTBEAT	916
EventType: PH_MONITOR_REDIS_UPDATE_FAILED	916
EventType: PH_MONITOR_REGISTER_MONITOR_GET_WORKER_FAILURE	916
EventType: PH_MONITOR_REGISTER_NODE	917
EventType: PH_MONITOR_REGISTER_SUPER_FOLLOWER	917
EventType: PH_MONITOR_REGISTER_WORKER	917
EventType: PH_MONITOR_REMOVE_NODE	917
EventType: PH_MONITOR_REMOVE_SUPER_FOLLOWER	917
EventType: PH_MONITOR_REMOVE_WORKER	917
EventType: PH_MONITOR_REPORTSERVER_NOTIFICATION_CLIENT_CONTACT_FAILURE	918
EventType: PH_MONITOR_REPORTSERVER_NOTIFICATION_CLIENT_INIT_FAILURE	918
EventType: PH_MONITOR_REPORTSERVER_NOTIFICATION_SERVER_RETURN_FAILURE	918
EventType: PH_MONITOR_RESET_DB_SERVER_NAME_FAILED	919
EventType: PH_MONITOR_RESET_JDBC_CONN_FAILED	919
EventType: PH_MONITOR_RESET_STORAGE_CONFIG_FAILED	919
EventType: PH_MONITOR_RESTART_MODULES	919
EventType: PH_MONITOR_REST_CACHE_REQUEST_EMPTY	919
EventType: PH_MONITOR_REST_CACHE_REQUEST_FAILURE	920
EventType: PH_MONITOR_REST_CACHE_REQUEST_FORMAT_ILLEGAL	920
EventType: PH_MONITOR_REST_CACHE_SERVER_INIT_FAILURE	920
EventType: PH_MONITOR_REST_CALL_FAILURE	920
EventType: PH_MONITOR_ROLE_UNDEFINED	921
EventType: PH_MONITOR_SAVE_DR_CONFIG_FAILED	921
EventType: PH_MONITOR_SEND_CMD_TO_MODULE	921
EventType: PH_MONITOR_SEND_VG_UPDATE_CMD_TO_MODULE	922
EventType: PH_MONITOR_SETUID_FAILURE	922
EventType: PH_MONITOR_START_MODULE	922
EventType: PH_MONITOR_START_MODULES	923
EventType: PH_MONITOR_STATFS_FAILURE	923
EventType: PH_MONITOR_STATUS_PUSHER_SPAWN_FAILURE	923

EventType: PH_MONITOR_STOP_MODULES	923
EventType: PH_MONITOR_STOP_READER	923
EventType: PH_MONITOR_STORAGE_ES_CUSTOMIZED_TEMPLATE_	
DEPLOYED	924
EventType: PH_MONITOR_STORAGE_GET_WORKER_FAILURE	924
EventType: PH_MONITOR_STORAGE_LOCAL_GET_FAILURE	924
EventType: PH_MONITOR_STORAGE_NFS_GET_FAILURE	924
EventType: PH_MONITOR_STORAGE_TYPE_GET_FAILURE	925
EventType: PH_MONITOR_STORAGE_TYPE_UNKNOWN	925
EventType: PH_MONITOR_STORAGE_UPDATE_WORKER_FAILURE	925
EventType: PH_MONITOR_SVC_PASSWORD_DISTRIBUTION_ERROR	925
EventType: PH_MONITOR_SYSINFO_FAILURE	926
EventType: PH_MONITOR_SYSTEM_DB_LOGIN_ERROR	926
EventType: PH_MONITOR_SYSTEM_HEALTH_CPU	926
EventType: PH_MONITOR_SYSTEM_HEALTH_ISSUE	926
EventType: PH_MONITOR_SYSTEM_HEALTH_MEM	927
EventType: PH_MONITOR_SYSTEM_STATUS_SPAWN_FAILURE	927
EventType: PH_MONITOR_THREAD_SPAWN_FAILED	927
EventType: PH_MONITOR_TUNNEL_ERROR	928
EventType: PH_MONITOR_UMOUNT_NFS_FAILURE	928
EventType: PH_MONITOR_UNABLE_CONTACT_APPSVR	928
EventType: PH_MONITOR_UPDATE_DATA_FAILED	929
EventType: PH_MONITOR_UPDATE_DR_FAILED	929
EventType: PH_MONITOR_UPDATE_WORKER_INFO_FAILED	929
EventType: PH_MONITOR_UPLOAD_LOG_SPAWN_FAILURE	929
EventType: PH_MONITOR_WINAGENT_DELETE_PWD_SPAWN_FAILURE	929
EventType: PH_MONITOR_WINAGENT_UPDATE_PWD_ERROR	929
EventType: PH_MONITOR_WIN_LINUX_AGENT_PWD_UPDATE_SUCCESS	930
EventType: PH_MONITOR_WORKER_NODECONFIG_UPDATE_FAILED	930
EventType: PH_MONITOR_WORKER_REDIS_ADDSLAVE_UPDATE_FAILED	930
EventType: PH_MONITOR_WORKER_REDIS_CONF_UPDATE_FAILED	930
EventType: PH_PERFMON_COMMIT_FILE_FAILED	931
EventType: PH_PERFMON_CONFIG_SEND_FAILED	931
EventType: PH_PERFMON_CONFIG_VERSION_ERROR	931
EventType: PH_PERFMON_CONFIG_VERSION_WARNING	931
EventType: PH_PERFMON_CUST_JOB_ADD_FAILED	932
EventType: PH_PERFMON_INIT_ERROR	932
EventType: PH_PERFMON_INST_SW_MAP_EMPTY	932
EventType: PH_PERFMON_INST_SW_NO_NAME	932
EventType: PH_PERFMON_JOB_ADD_FAILED	933
EventType: PH_PERFMON_MASS_PING_WARNING	933
EventType: PH_PERFMON_MONITEE_BAD	933
EventType: PH_PERFMON_MONITEE_NOT_FOUND	933
EventType: PH_PERFMON_NO_DEV_TYPE	933
EventType: PH_PERFMON_PERF_OBJ_PARSE_FAILURE	933
EventType: PH_PERFMON_PING_RESULT_OPEN_FAILED	934
EventType: PH_PERFMON_PROC_RUN_FAILED	934
EventType: PH_PERFMON_REAL_TIME_JOB_RUN_FAILED	934
EventType: PH_PERFMON_ROUTE_LOAD_ERROR	934

EventType: PH_PERFMON_STATUS_REPORTER_INIT_FAILED	935
EventType: PH_PERFMON_STATUS_REPORT_FAILED	935
EventType: PH_PERFMON_SVN_CHECKOUT_FAILED	935
EventType: PH_PERFMON_SVN_CONFIG_MISSING	935
EventType: PH_PERFMON_SVN_DIR_CREATE_FAILED	935
EventType: PH_PERFMON_SVN_DIR_UPDATE_FAILED	936
EventType: PH_PERFMON_SVN_FILE_COPY_FAILED	936
EventType: PH_PERFMON_SVN_FILE_EMPTY	936
EventType: PH_PERFMON_SVN_FILE_MARK_FAILED	937
EventType: PH_PERFMON_SVN_FILE_OPEN_FAILED	937
EventType: PH_PERFMON_SVN_FILE_PARSE_FAILED	937
EventType: PH_PERFMON_SVN_FILE_REMOVE_FAILED	938
EventType: PH_PERFMON_SVN_FILE_RENAME_FAILED	938
EventType: PH_PERFMON_SVN_FIM_FILE_MISSING	938
EventType: PH_PERFMON_SVN_FIRSTFILELINES_EMPTY	939
EventType: PH_PERFMON_SVN_FIRSTFILELINES_NOT_IN_FILE	939
EventType: PH_PERFMON_SVN_GET_DEVICE_ID_FAILED	939
EventType: PH_PERFMON_SVN_GET_DISCOV_TIME_FAILED	940
EventType: PH_PERFMON_SVN_INFO_GET_FAILED	940
EventType: PH_PERFMON_SVN_INST_SW_BAD	940
EventType: PH_PERFMON_SVN_INVALID_FILE_FORMAT	940
EventType: PH_PERFMON_SVN_INVALID_HEADER_IN_FILE	941
EventType: PH_PERFMON_SVN_INVALID_SECONDFILENAME	941
EventType: PH_PERFMON_SVN_LINE_MISMATCH	941
EventType: PH_PERFMON_SVN_SECONDFILENAME_EMPTY	942
EventType: PH_PERFMON_SVN_SOFTWARE_MISSING	942
EventType: PH_PERFMON_TOPO_CONFIG_ERROR	942
EventType: PH_PERFMON_TOPO_FILE_OPEN_FAILED	942
EventType: PH_PERFMON_TOPO_LOAD_ERROR	943
EventType: PH_PERFMON_TRACERT_FILE_OPEN_FAILED	943
EventType: PH_PERFMON_UNKNOWN_CUST_PERF_JOB_ID	943
EventType: PH_PERFMON_UNKNOWN_PERF_JOB_ID	943
EventType: PH_PERFMON_UNKNOWN_PROBE_JOB_ID	944
EventType: PH_PERFMON_UPDATE_CONFIG_ERROR	944
EventType: PH_PERFMON_UPDATE_FILTERS_ERROR	944
EventType: PH_PERFMON_UPDATE_ROUTE_DEPENDENCY_FAILED	944
EventType: PH_PERFMON_USER_PWD_GET_FAILED	945
EventType: PH_PERFORM_MONITOR_ERROR	945
EventType: PH_PER_MON_CONFIG_ERROR	945
EventType: PH_PER_MON_FETCH	946
EventType: PH_PER_MON_FUNCTION	946
EventType: PH_PER_MON_SNMP_DONE	946
EventType: PH_PER_MON_WALK	947
EventType: PH_PER_MON_WALK_ERROR	947
EventType: PH_STM_ACCOUNT_UNMATCHED	948
EventType: PH_STM_AUTH_TYPE_UNKNOWN	948
EventType: PH_STM_BAD_ELEM	948
EventType: PH_STM_BAD_ELEM_VALUE	948
EventType: PH_STM_BAD_PORT	948

EventType: PH_STM_BAD_RTT_LINE	948
EventType: PH_STM_BAD_SSL	949
EventType: PH_STM_BAD_TAG	949
EventType: PH_STM_CMD_EXEC_FAILED	949
EventType: PH_STM_CRED_INVALID	949
EventType: PH_STM_CURL_ESCAPE_FAILED	950
EventType: PH_STM_CURL_INIT_FAILED	950
EventType: PH_STM_DNS_TYPE_UNSUPPORT	950
EventType: PH_STM_DUPLICATED	950
EventType: PH_STM_ELEM_EMPTY	950
EventType: PH_STM_ELEM_MISSING	950
EventType: PH_STM_ELEM_NEGATIVE	951
EventType: PH_STM_ERROR	951
EventType: PH_STM_FILE_OPEN_FAILED	951
EventType: PH_STM_GET_HOST_FAILED	952
EventType: PH_STM_GUESS_TYPE_FAILED	952
EventType: PH_STM_HTTP_RESP_FAILED	952
EventType: PH_STM_METHOD_UNKNOWN	952
EventType: PH_STM_MONITOR_MISSING_ACTION	953
EventType: PH_STM_MONITOR_RESULT_UPLOAD_FAILED	953
EventType: PH_STM_NO_ORACLE_NAME	953
EventType: PH_STM_PORT_UNKNOWN	953
EventType: PH_STM_PROCESS_INVOKE_FAILED	953
EventType: PH_STM_PROTO_UNKNOWN	954
EventType: PH_STM_PROTO_UNSUPPORT	954
EventType: PH_STM_SERVER_ADDR_INVALID	954
EventType: PH_STM_SPECIAL_LINE_NOT_FOUND	954
EventType: PH_STM_STM_GET_PROCESS_FAILED	954
EventType: PH_STM_STM_GET_PROCESS_NAME_FAILED	954
EventType: PH_STM_TAG_MISSING	955
EventType: PH_STM_TAG_NOT_FOUND	955
EventType: PH_STM_TAG_UNKNOWN	955
EventType: PH_STM_TRACEROUTE_FAILED	955
EventType: PH_STM_XML_PARSE_FAILED	955
EventType: PH_USER_MON_SUDDEN_LOC_CHANGE	956
EventType: PH_USER_MON_SUDDEN_LOGIN_DISTRIBUTION_CHANGE	956
EventType: PH_USER_MON_SUDDEN_LOGIN_VOLUME_CHANGE	957
Query Logs	959
EventType: PH_JAVA_QUERYSERVER_ACTION_UNSUPPORTED_ERROR	962
EventType: PH_JAVA_QUERYSERVER_ELASTIC_ERROR	962
EventType: PH_JAVA_QUERYSERVER_ERROR	962
EventType: PH_JAVA_QUERYSERVER_INFO	963
EventType: PH_JAVA_QUERYSERVER_QUERYID_ERROR	963
EventType: PH_JAVA_QUERYSERVER_QUERY_SYNTAX_ERROR	963
EventType: PH_JAVA_QUERYSERVER_REDIS_ERROR	963
EventType: PH_JAVA_QUERYSERVER_WARN	963
EventType: PH_QUERYSRV_DUPLICATED_QUERYID	963
EventType: PH_QUERYSRV_INVALID_QUERYXML	964
EventType: PH_QUERY_AGGR_RESULTS_POST_PROCESS_FAILED	964

EventType: PH_QUERY_ATTR_UNDEFINED	964
EventType: PH_QUERY_BAD_RESULT_STATUS	964
EventType: PH_QUERY_CACHE_GET_FAILED	965
EventType: PH_QUERY_CACHE_RESULT_GET_FAILED	965
EventType: PH_QUERY_CACHE_TRIGGER_EVENT_GET_FAILED	965
EventType: PH_QUERY_CHAR_UNEXPECTED	965
EventType: PH_QUERY_CH_PARSE_FAILED	966
EventType: PH_QUERY_CH_POST_FAILED	966
EventType: PH_QUERY_CLICKHOUSE_DATA_FAILED	966
EventType: PH_QUERY_CLICKHOUSE_EXEC_FAILED	967
EventType: PH_QUERY_CLICKHOUSE_STARTS	967
EventType: PH_QUERY_CLICKHOUSE_STOP_FAILED	967
EventType: PH_QUERY_CLICKHOUSE_WAITING_QUEUE_FULL	968
EventType: PH_QUERY_COMMAND_BAD	968
EventType: PH_QUERY_COMPLETION_NOTIFICATION_SEND_FAILED	968
EventType: PH_QUERY_CONFIG_UNDEFINED	968
EventType: PH_QUERY_CONVERT_FAILED	969
EventType: PH_QUERY_DATA_ENUM_FAILED	969
EventType: PH_QUERY_DATA_MANAGER_NODES_GET_FAILED	969
EventType: PH_QUERY_DATA_SEND_FAILED	970
EventType: PH_QUERY_DATA_SIZE_MISMATCH	970
EventType: PH_QUERY_DATA_SIZE_UNEXPECTED	970
EventType: PH_QUERY_DATA_TYPE_UNEXPECTED	970
EventType: PH_QUERY_DB_SERVER_HOST_UNDEFINED	970
EventType: PH_QUERY_DIR_CREATE_FAILED	971
EventType: PH_QUERY_DIR_RENAME_FAILED	971
EventType: PH_QUERY_DISTRIBUTION	971
EventType: PH_QUERY_DURATION	972
EventType: PH_QUERY_ES_PARSE_FAILED	972
EventType: PH_QUERY_ES_POST_FAILED	973
EventType: PH_QUERY_ES_SCROLL_FAILED	973
EventType: PH_QUERY_EVENT_COLLECTOR_UNAVAILABLE	973
EventType: PH_QUERY_EVENT_ID_GET_FAILED	973
EventType: PH_QUERY_EVENT_PARSE_FAILED	974
EventType: PH_QUERY_EVENT_PAYLOAD_READ_FAILED	974
EventType: PH_QUERY_EXCEPTION_CAUGHT	974
EventType: PH_QUERY_EXPORT_TASK_CREAT_FAILED	975
EventType: PH_QUERY_EXPORT_TASK_INSERT_FAILED	975
EventType: PH_QUERY_EXPR_INCOMPLETE	975
EventType: PH_QUERY_FILE_CONTENT_BAD	976
EventType: PH_QUERY_FILE_CONTENT_MISSING	976
EventType: PH_QUERY_FILE_COPY_FAILED	976
EventType: PH_QUERY_FILE_CORRUPT	977
EventType: PH_QUERY_FILE_CREATE_FAILED	977
EventType: PH_QUERY_FILE_EMPTY	977
EventType: PH_QUERY_FILE_HEADER_GET_FAILED	978
EventType: PH_QUERY_FILE_LINK_FAILED	978
EventType: PH_QUERY_FILE_MAGIC_BAD	978
EventType: PH_QUERY_FILE_MMAP_FAILED	978

EventType: PH_QUERY_FILE_NAME_BAD	979
EventType: PH_QUERY_FILE_OPEN_FAILED	979
EventType: PH_QUERY_FILE_READ_FAILED	979
EventType: PH_QUERY_FILE_REMOVE_FAILED	980
EventType: PH_QUERY_FILE_SEEK_FAILED	980
EventType: PH_QUERY_FILE_STAT_FAILED	980
EventType: PH_QUERY_FORMAT_UNSUPPORTED	981
EventType: PH_QUERY_FUNC_ERROR	981
EventType: PH_QUERY_ID_DUPLICATE	981
EventType: PH_QUERY_ID_INACTIVE	981
EventType: PH_QUERY_ID_NOT_FOUND	982
EventType: PH_QUERY_ID_REMOVE_FAILED	982
EventType: PH_QUERY_ID_UNSUPPORTED	982
EventType: PH_QUERY_INLINEREQUEST_BAD	983
EventType: PH_QUERY_IPC_EVENT_SEND_FAILED	983
EventType: PH_QUERY_IP_GET_FAILED	983
EventType: PH_QUERY_IP_INVALID	983
EventType: PH_QUERY_IP_TYPE_INVALID	984
EventType: PH_QUERY_LOGINTEGRITYEXPORT_TASK_CREAT_FAILED	984
EventType: PH_QUERY_LOGINTEGRITYEXPORT_TASK_INSERT_FAILED	984
EventType: PH_QUERY_LOG_INTEGRITY_EXPORT_DIR_UNCONFIGURED	984
EventType: PH_QUERY_LOG_INTEGRITY_EXPORT_FAILED	985
EventType: PH_QUERY_LONG_RUNNING_STOPPED	985
EventType: PH_QUERY_MEM_ALLOC_FAILED	985
EventType: PH_QUERY_MESSAGE_SEND_FAILED	986
EventType: PH_QUERY_MODULE_INIT_FAILED	986
EventType: PH_QUERY_MODULE_UNCONFIGURED	986
EventType: PH_QUERY_ONLINE_WORKER_CHANGED	987
EventType: PH_QUERY_PARSED_EVENT_LOAD_FAILED	987
EventType: PH_QUERY_PARTIAL_WORKER_FAILURE	987
EventType: PH_QUERY_PCAP_FINALIZE_FAILED	987
EventType: PH_QUERY_PCAP_LOAD_FAILED	988
EventType: PH_QUERY_PCAP_RENAME_FAILED	988
EventType: PH_QUERY_PCAP_TRANSFER_FAILED	988
EventType: PH_QUERY_PGDB_EXEC_SQL_FAILED	989
EventType: PH_QUERY_PGDB_RECONNECT_FAILED	989
EventType: PH_QUERY_PGDB_SQL_GET_VAL_FAILED	989
EventType: PH_QUERY_POST_FILTER_PARSE_FAILED	989
EventType: PH_QUERY_PQ_ERROR	990
EventType: PH_QUERY_PROCESS_GET_FAILED	990
EventType: PH_QUERY_PROFILE_ATTR_UNSPECIFIED	990
EventType: PH_QUERY_PROFILE_EVENT_TYPE_ERROR	990
EventType: PH_QUERY_PROFILE_FUNCTION_ERROR	991
EventType: PH_QUERY_PROFILE_NOT_MARKED_AS_BASELINE	991
EventType: PH_QUERY_PROGRESS_REJECTED	991
EventType: PH_QUERY_REPORTEXPORT_TASK_CREAT_FAILED	992
EventType: PH_QUERY_REPORTEXPORT_TASK_INSERT_FAILED	992
EventType: PH_QUERY_REPORT_RESULTS_LOAD_FAILED	992
EventType: PH_QUERY_REPORT_RESULTS_POST_FILTER_FAILED	992

EventType: PH_QUERY_REPORT_RESULT_FILE_NOT_EXIST	993
EventType: PH_QUERY_REQUEST_BAD	993
EventType: PH_QUERY_RESULT_FILES_MERGE_FAILED	993
EventType: PH_QUERY_RESULT_GET_FAILED	994
EventType: PH_QUERY_RESULT_NOT_READY	994
EventType: PH_QUERY_RESULT_PARSE_FAILED	994
EventType: PH_QUERY_RESULT_REJECTED	994
EventType: PH_QUERY_RESULT_SAVE_FAILED	995
EventType: PH_QUERY_RESULT_UPLOAD_FAILED	995
EventType: PH_QUERY_RT_ERROR	995
EventType: PH_QUERY_SORT_SPEC_GET_FAILED	996
EventType: PH_QUERY_START_FAILED	996
EventType: PH_QUERY_STATE_BAD	996
EventType: PH_QUERY_STATUS_LOAD_FAILED	997
EventType: PH_QUERY_STATUS_SAVE_FAILED	997
EventType: PH_QUERY_SUMM_ATTR_BAD	997
EventType: PH_QUERY_SUMM_ATTR_MISSING	997
EventType: PH_QUERY_SUMM_ATTR_UPDATE_FAILED	997
EventType: PH_QUERY_SUMM_COLUMN_UNSUPPORTED	998
EventType: PH_QUERY_SUMM_EVENT_SKIPPED	998
EventType: PH_QUERY_SUMM_PARSE_FAILED	998
EventType: PH_QUERY_SUMM_PERF_ETINFO_UNSUPPORTED	999
EventType: PH_QUERY_TASK_INVALID	999
EventType: PH_QUERY_TASK_REROUTED	999
EventType: PH_QUERY_TASK_REROUTE_FAILED	1000
EventType: PH_QUERY_VALUE_TYPE_UNSUPPORTED	1000
EventType: PH_QUERY_WORKERS_GET_FAILED	1000
EventType: PH_QUERY_WORKERS_SPLIT_AMONG_FAILED	1000
EventType: PH_QUERY_WORKER_CHANGED_TO_OFFLINE	1001
EventType: PH_QUERY_WORKER_CHANGED_TO_ONLINE	1001
EventType: PH_QUERY_XML_PARSE_FAILED	1001

Report Logs **1003**

EventType: PH_REPORT_ACTION_STATUS	1005
EventType: PH_REPORT_ACT_FAILED	1006
EventType: PH_REPORT_AGGR_FIELDS_EMPTY	1006
EventType: PH_REPORT_AGGR_FIELD_NOT_ADDED	1006
EventType: PH_REPORT_AGGR_FUNC_EMPTY	1006
EventType: PH_REPORT_AGGR_TYPE_ERROR	1007
EventType: PH_REPORT_AGGR_TYPE_UNDEFINED	1007
EventType: PH_REPORT_ATTR_ID_UNSUPPORTED	1007
EventType: PH_REPORT_ATTR_MISSING	1007
EventType: PH_REPORT_ATTR_UNDEFINED	1008
EventType: PH_REPORT_BUFFER_OVERFLOW	1008
EventType: PH_REPORT_CHECKSUM_MISMATCH	1008
EventType: PH_REPORT_CONFIG_UPDATE_NULL	1008
EventType: PH_REPORT_CONVERT_FAILED	1008
EventType: PH_REPORT_DATA_INIT_FAILED	1009
EventType: PH_REPORT_DATA_SIZE_MISMATCH	1009
EventType: PH_REPORT_DATA_SIZE_OVERFLOW	1009

EventType: PH_REPORT_DATA_SIZE_UNEXPECTED	1009
EventType: PH_REPORT_DATA_SIZE_UNKNOWN	1010
EventType: PH_REPORT_DATA_TYPE_UNEXPECTED	1010
EventType: PH_REPORT_DIR_CREATE_FAILED	1010
EventType: PH_REPORT_DIR_OPEN_FAILED	1010
EventType: PH_REPORT_DIR_REMOVE_FAILED	1011
EventType: PH_REPORT_ES_BUCKETS_EMPTY	1011
EventType: PH_REPORT_ES_POST_FAILED	1011
EventType: PH_REPORT_ES_PROFILE_EMPTY	1012
EventType: PH_REPORT_ES_PROFILE_TIMEOUT	1012
EventType: PH_REPORT_ES_PURGE_INDEX_FAILED	1012
EventType: PH_REPORT_ES_TIME_RANGE_INVALID	1013
EventType: PH_REPORT_EXPR_PARSE_FAILED	1013
EventType: PH_REPORT_FILE_CONTENT_MISSING	1013
EventType: PH_REPORT_FILE_COPY_FAILED	1013
EventType: PH_REPORT_FILE_HEADER_BAD	1014
EventType: PH_REPORT_FILE_INIT_FAILED	1014
EventType: PH_REPORT_FILE_LINK_FAILED	1014
EventType: PH_REPORT_FILE_MAGIC_BAD	1015
EventType: PH_REPORT_FILE_MMAP_FAILED	1015
EventType: PH_REPORT_FILE_NAME_BAD	1015
EventType: PH_REPORT_FILE_OPEN_FAILED	1016
EventType: PH_REPORT_FILE_PARSE_FAILED	1016
EventType: PH_REPORT_FILE_READ_FAILED	1016
EventType: PH_REPORT_FILE_REMOVE_FAILED	1017
EventType: PH_REPORT_FILE_RENAME_FAILED	1017
EventType: PH_REPORT_FILE_RSYNC_FAILED	1017
EventType: PH_REPORT_FILE_STAT_FAILED	1018
EventType: PH_REPORT_FILE_TYPE_UNKNOWN	1018
EventType: PH_REPORT_FILE_UNSPECIFIED	1018
EventType: PH_REPORT_FILE_WRITE_FAILED	1019
EventType: PH_REPORT_FUNC_OBJ_DEF_ERROR	1019
EventType: PH_REPORT_FUNC_OBJ_DEF_GET_FAILED	1019
EventType: PH_REPORT_FUNC_OBJ_DEF_UNKNOWN	1020
EventType: PH_REPORT_ID_LOC_DEVICE_EXCLUDED_INVALID	1020
EventType: PH_REPORT_ID_LOC_EVENT_SEND_FAILED	1020
EventType: PH_REPORT_ID_LOC_RESULT_UPLOAD_FAILED	1020
EventType: PH_REPORT_ID_LOC_SYNCH_DATA_UPLOAD_FAILED	1021
EventType: PH_REPORT_ID_LOC_USER_ALREADY_EXCLUDED	1021
EventType: PH_REPORT_ID_LOC_USER_EXCLUDE_FAILED	1021
EventType: PH_REPORT_INDEX_OVERFLOW	1022
EventType: PH_REPORT_IP_GET_FAILED	1022
EventType: PH_REPORT_IP_TYPE_INVALID	1022
EventType: PH_REPORT_KEY_LOAD_FAILED	1023
EventType: PH_REPORT_MODULE_INIT_FAILED	1023
EventType: PH_REPORT_MODULE_UNCONFIGURED	1023
EventType: PH_REPORT_OLD_REPORT_DATA	1023
EventType: PH_REPORT_OP_UNEXPECTED	1024
EventType: PH_REPORT_ORDER_BY_ATTR_EMPTY	1024

EventType: PH_REPORT_ORDER_BY_INVALID	1024
EventType: PH_REPORT_PACK_FAILED	1024
EventType: PH_REPORT_PACK_FAILED_COUNT	1025
EventType: PH_REPORT_PARSED_EVENT_LOAD_FAILED	1025
EventType: PH_REPORT_PGDB_CONNECT_FAILED	1025
EventType: PH_REPORT_PGDB_EXEC_FAILED	1025
EventType: PH_REPORT_PGDB_NOT_CONNECTED	1026
EventType: PH_REPORT_PGDB_NOT_INIT	1026
EventType: PH_REPORT_POINTER_NULL	1026
EventType: PH_REPORT_POINTER_NULL_WARNING	1026
EventType: PH_REPORT_POSITIVE_INTEGER_EXPECTED	1027
EventType: PH_REPORT_PQ_ERROR	1027
EventType: PH_REPORT_PROFILE_TYPE_BAD	1027
EventType: PH_REPORT_PROFILE_TYPE_WRONG_FORMAT	1027
EventType: PH_REPORT_PROFILE_UPDATE_FAILED	1028
EventType: PH_REPORT_ROW_LENGTH_ZERO	1028
EventType: PH_REPORT_RULE_ATTR_MISSING	1028
EventType: PH_REPORT_SCHEMA_INCOMPATIBLE	1029
EventType: PH_REPORT_SCHEMA_INVALID	1029
EventType: PH_REPORT_SCHEMA_LOAD_FAILED	1029
EventType: PH_REPORT_SQLITE3_BATCH_BEGIN_FAILED	1029
EventType: PH_REPORT_SQLITE3_BATCH_COMMIT_FAILED	1030
EventType: PH_REPORT_SQLITE3_BIND_VALUE_FAILED	1030
EventType: PH_REPORT_SQLITE3_BUSY	1031
EventType: PH_REPORT_SQLITE3_BUSY_TIMEOUT_ERROR	1031
EventType: PH_REPORT_SQLITE3_CHECKPOINT_FAILED	1031
EventType: PH_REPORT_SQLITE3_COMMIT_ERROR	1032
EventType: PH_REPORT_SQLITE3_CONFIG_FAILED	1032
EventType: PH_REPORT_SQLITE3_ENABLE_SHARED_CACHE_FAILED	1032
EventType: PH_REPORT_SQLITE3_EXEC_FAILED	1033
EventType: PH_REPORT_SQLITE3_EXTENDED_RESULT_CODES_ERROR	1033
EventType: PH_REPORT_SQLITE3_OPEN_FAILED	1033
EventType: PH_REPORT_SQLITE3_PREPARE_ERROR	1034
EventType: PH_REPORT_SQLITE3_PROFILE_ENTRY_DELETE_FAILED	1034
EventType: PH_REPORT_SQLITE3_PROFILE_NOT_FOUND	1035
EventType: PH_REPORT_SQLITE3_STEP_ERROR	1035
EventType: PH_REPORT_UNPACK_FAILED	1035
EventType: PH_REPORT_VALUE_TYPE_LOOKUP_BY_ID_FAILED	1036
EventType: PH_REPORT_VALUE_TYPE_LOOKUP_BY_NAME_FAILED	1036
EventType: PH_REPORT_VALUE_TYPE_OF_ID_UNEXPECTED	1036
EventType: PH_REPORT_VALUE_TYPE_OF_NAME_UNEXPECTED	1036
EventType: PH_REPORT_VALUE_TYPE_OF_STAT_UNEXPECTED	1036
EventType: PH_REPORT_VALUE_TYPE_UNSUPPORTED	1037
EventType: PH_REPORT_WORKER_UPLOAD_FAILED	1037
EventType: PH_REPORT_XML_ELEMENT_DUPLICATE	1037
EventType: PH_REPORT_XML_ELEMENT_MISSING	1038
EventType: PH_REPORT_XML_ELEMENT_PARSE_FAILED	1038
EventType: PH_REPORT_XML_PARSE_FAILED	1038
EventType: PH_REPORT_ZLIB_COMPRESSION_TYPE_UNKNOWN	1039

EventType: PH_REPORT_ZLIB_UNCOMPRESS_FAILED	1039
Rule Logs	1040
EventType: PH_ANOMALY_CONFIG	1042
EventType: PH_ANOMALY_LATERAL_MOVEMENT_ANALYZE	1042
EventType: PH_ANOMALY_LATERAL_MOVEMENT_DETECT	1043
EventType: PH_ANOMALY_LATERAL_MOVEMENT_TRAIN	1043
EventType: PH_ANOMALY_SYSTEM	1044
EventType: PH_ANOMALY_TIMER	1044
EventType: PH_DROP_EVENT_FROM_SHARED_BUFFER	1045
EventType: PH_DROP_INCIDENT	1045
EventType: PH_DROP_INCIDENT_COUNT	1046
EventType: PH_JMS_QUEUE_SIZE_WARNING	1046
EventType: PH_ML_ANOMALY_DETECTED	1046
EventType: PH_RULEMASTER_TEST_RULES_CHECK_SYNTAX	1046
EventType: PH_RULEMASTER_TEST_RULES_FINALIZE_STATE	1047
EventType: PH_RULEMASTER_TEST_RULES_UPDATE_STATE	1047
EventType: PH_RULEMOD_AGGREGATOR_EMPTY	1047
EventType: PH_RULEMOD_ARITH_OP_ILLEGAL	1048
EventType: PH_RULEMOD_ATTR_ALREADY_ASSOCIATED	1048
EventType: PH_RULEMOD_ATTR_ID_LOOKUP_BY_NAME_FAILED	1048
EventType: PH_RULEMOD_ATTR_ID_UNDEFINED	1048
EventType: PH_RULEMOD_ATTR_MISSING	1049
EventType: PH_RULEMOD_ATTR_NAME_LOOKUP_BY_ID_FAILED	1049
EventType: PH_RULEMOD_ATTR_UNDEFINED	1049
EventType: PH_RULEMOD_BUFFER_EMPTY	1049
EventType: PH_RULEMOD_CLEAR_CONDITION_INVALID	1049
EventType: PH_RULEMOD_CLEAR_CONDITION_SET_FAILED	1050
EventType: PH_RULEMOD_CONFIG_UNDEFINED	1050
EventType: PH_RULEMOD_CONSTRUCTOR_ERROR	1050
EventType: PH_RULEMOD_CUST_ID_LIST_INVALID	1051
EventType: PH_RULEMOD_DATA_REQUEST_PARSE_FAILED	1051
EventType: PH_RULEMOD_DATA_SIZE_OVERFLOW	1051
EventType: PH_RULEMOD_DATA_UNSUPPORTED	1052
EventType: PH_RULEMOD_DB_SERVER_HOST_UNDEFINED	1052
EventType: PH_RULEMOD_DIR_OPEN_FAILED	1052
EventType: PH_RULEMOD_ENCODE_FAILED	1052
EventType: PH_RULEMOD_ENTITY_VERSION_MISSING	1053
EventType: PH_RULEMOD_EVENT_TYPE_GROUP_INVALID	1053
EventType: PH_RULEMOD_EVENT_TYPE_NOT_FOUND	1053
EventType: PH_RULEMOD_EXCEPTION_ELEMENT_INVALID	1054
EventType: PH_RULEMOD_EXPR_EVAL_UNKNOWN	1054
EventType: PH_RULEMOD_EXPR_PARSE_FAILED	1054
EventType: PH_RULEMOD_EXPR_UNSUPPORTED	1055
EventType: PH_RULEMOD_FILE_OPEN_FAILED	1055
EventType: PH_RULEMOD_FILE_UNSPECIFIED	1055
EventType: PH_RULEMOD_FORMAT_ERROR	1056
EventType: PH_RULEMOD_FUNC_NOT_FOUND	1056
EventType: PH_RULEMOD_FUNC_PARSE_FAILED	1056
EventType: PH_RULEMOD_GLOBAL_CONSTRAINT_INVALID	1056

EventType: PH_RULEMOD_GROUPBY_LIST_INVALID	1057
EventType: PH_RULEMOD_GROUPBY_LIST_NOT_FOUND	1057
EventType: PH_RULEMOD_GROUP_EVENT_CONSTRAINT_INVALID	1057
EventType: PH_RULEMOD_ID_LOOKUP_BY_INCIDENT_FAILED	1058
EventType: PH_RULEMOD_INCIDENT_ARG_INVALID	1058
EventType: PH_RULEMOD_INCIDENT_CACHE_NOT_FOUND	1058
EventType: PH_RULEMOD_INCIDENT_DEF_INVALID	1059
EventType: PH_RULEMOD_INCIDENT_NOT_FOUND	1059
EventType: PH_RULEMOD_INCIDENT_REPORT_SEND_FAILED	1059
EventType: PH_RULEMOD_INDEX_OVERFLOW	1060
EventType: PH_RULEMOD_INFO_GET_FAILED	1060
EventType: PH_RULEMOD_IP_GET_FAILED	1060
EventType: PH_RULEMOD_IP_INVALID	1061
EventType: PH_RULEMOD_IP_TYPE_INVALID	1061
EventType: PH_RULEMOD_LOAD_METHOD_UNDEFINED	1061
EventType: PH_RULEMOD_MEM_ALLOC_FAILED	1061
EventType: PH_RULEMOD_MODULE_INIT_FAILED	1062
EventType: PH_RULEMOD_MUTEX_ACQUIRE_FAILED	1062
EventType: PH_RULEMOD_NOTIF_CONNECTION_FAILED	1062
EventType: PH_RULEMOD_OBJ_GET_FROM_SUBPATTERN_FAILED	1063
EventType: PH_RULEMOD_OBJ_LOAD_FAILED	1063
EventType: PH_RULEMOD_OP_NOT_FUNC	1063
EventType: PH_RULEMOD_OP_UNKNOWN	1063
EventType: PH_RULEMOD_PARSED_EVENT_LOAD_FAILED	1063
EventType: PH_RULEMOD_PQ_ERROR	1063
EventType: PH_RULEMOD_PROFILE	1064
EventType: PH_RULEMOD_REM_BY_ZERO	1064
EventType: PH_RULEMOD_REM_BY_ZEROD	1064
EventType: PH_RULEMOD_SELECT_ATTR_PARSE_FAILED	1065
EventType: PH_RULEMOD_SELECT_SPEC_PARSE_FAILED	1065
EventType: PH_RULEMOD_SINGLE_EVENT_CONSTRAINT_INVALID	1065
EventType: PH_RULEMOD_SUBPATTERN_INVALID	1065
EventType: PH_RULEMOD_SUBPATTERN_MISSING	1066
EventType: PH_RULEMOD_SUBPATTERN_MORE_THAN_ONE	1066
EventType: PH_RULEMOD_SUBPATTERN_UNDEFINED	1066
EventType: PH_RULEMOD_SUMMARY_UPLOAD_FAILED	1067
EventType: PH_RULEMOD_THREAD_SPAWN_FAILED	1067
EventType: PH_RULEMOD_TOKEN_UNDEFINED	1067
EventType: PH_RULEMOD_TOKEN_UNEXPECTED	1068
EventType: PH_RULEMOD_UNPACK_FAILED	1068
EventType: PH_RULEMOD_VALUE_TYPE_UNEXPECTED	1068
EventType: PH_RULEMOD_XML_ELEMENT_EMPTY	1069
EventType: PH_RULEMOD_XML_ELEMENT_MISSING	1069
EventType: PH_RULEMOD_XML_ELEMENT_PARSE_FAILED	1069
EventType: PH_RULEMOD_XML_ELEMENT_UNEXPECTED	1069
EventType: PH_RULEMOD_XML_ELEMENT_UNKNOWN	1070
EventType: PH_RULEMOD_XML_LOAD_FAILED	1070
EventType: PH_RULEMOD_XML_PARSE_FAILED	1070
EventType: PH_RULEMOD_XML_POINTER_NULL	1071

EventType: PH_RULEWORKER_TEST_RULES_CHECK_SYNTAX	1071
EventType: PH_RULEWORKER_TEST_RULES_EVENT_MATCH_STATUS	1071
EventType: PH_SCHEDULED_RULE_QUERY_FAILED	1071
EventType: PH_TEST_RULES_PARSE_STATUS	1072
EventType: PH_UPDATE_RULE_SUCCEED	1072
System Logs	1073
EventType: PH_BAD_ROUTE_OUTPUT	1080
EventType: PH_BASE_PROC_BASE_AGENT_JOB_NO_THREAD_NUM_	
ASSIGNED	1081
EventType: PH_BASE_PROC_DUMP_STACK_TRACE_FAILURE	1081
EventType: PH_BASE_PROC_GET_PID_FILE_FAILED	1081
EventType: PH_BASE_PROC_HANDLE_NOTIFICATION_ERROR	1082
EventType: PH_BASE_PROC_KILL_PROC_ERROR	1082
EventType: PH_BASE_PROC_NOTIFICATION_HANDLE_CONN_ERROR	1082
EventType: PH_BASE_PROC_NO_CONN_TO_HEARTBEAT_SERVER	1082
EventType: PH_BASE_PROC_RENAME_MINI_DUMP_FILE_FAILURE	1082
EventType: PH_BASE_PROC_REST_CACHE_CHECKOUT_STATUS_	
WARNING	1083
EventType: PH_BASE_PROC_SEND_HEARTBEAT_FAILURE	1083
EventType: PH_BASE_PROC_SEND_USER_DEFINED_SIG_FAILED	1083
EventType: PH_BASE_PROC_SET_PID_FILE_FAILED	1083
EventType: PH_BASE_PROC_STACK_TRACE	1084
EventType: PH_BASE_PROC_STACK_TRACK_TOO_LONG	1084
EventType: PH_BASE_PROC_SYS_INFO_CALC_CPU_ERROR	1084
EventType: PH_BASE_PROC_SYS_PROC_INFO_GET_FAILURE	1084
EventType: PH_BASE_PROC_SYS_PROC_INFO_INIT_ERROR	1085
EventType: PH_BASE_PROC_SYS_PROC_INFO_UNABLE_OPEN_PROC_	
PID_FILE	1085
EventType: PH_BASE_PROC_SYS_PROC_INFO_UNABLE_OPEN_PROC_	
STAT_FILE	1085
EventType: PH_BASE_PROC_THREAD_SPAWN_FAILED	1085
EventType: PH_BASE_PROC_THREAD_WRONG_PARAM	1086
EventType: PH_BASE_PROC_UPLOAD_FILE_FAILURE	1086
EventType: PH_BASE_PROC_VALUE_GROUP_UPDATE_FAILURE	1086
EventType: PH_BASE_PRO_AQUIRE_SHARED_STORE_FAILED	1086
EventType: PH_CLIHOUSE_BUILD_QUERY_DIST_SQL_COMMAND_	
FAILURE	1086
EventType: PH_CLI_ERROR	1087
EventType: PH_CREATE_TEMP_FILE_FAILURE	1087
EventType: PH_DISC_DATA_PROCESS_ERROR	1087
EventType: PH_DIVIDE_BY_ZERO	1087
EventType: PH_FAILED_TO_EXEC	1088
EventType: PH_FILE_NOT_FOUND	1088
EventType: PH_GCS_BUCKET_ACCESS_FAILURE	1088
EventType: PH_GENERIC_CRITICAL	1088
EventType: PH_GENERIC_DEBUG	1088
EventType: PH_GENERIC_ERROR	1088
EventType: PH_GENERIC_INFO	1089
EventType: PH_GENERIC_WARNING	1089

EventType: PH_GET_CURL_HANDLE_FAILED	1089
EventType: PH_GET_SUPER_LEADER_FAILURE	1089
EventType: PH_GRPC_CERT_CREATE_SUCCESS	1089
EventType: PH_GRPC_CERT_ERROR	1090
EventType: PH_GRPC_CERT_LOADED_FAILED	1090
EventType: PH_GRPC_CERT_UPDATE_FAILED	1090
EventType: PH_GRPC_CERT_UPDATE_SUCCESS	1090
EventType: PH_GRPC_FORTMAT_JSON_FAILED	1091
EventType: PH_GRPC_INIT_SSL_CONTEXT	1091
EventType: PH_GRPC_TASK_DATA_EMPTY	1091
EventType: PH_HTTP_CLIENT_COMPRESS_FAILED	1091
EventType: PH_HTTP_CLIENT_CURL_ERROR	1092
EventType: PH_HTTP_CLIENT_GET_CACHE_FROM_MONITOR_FAILED	1092
EventType: PH_HTTP_CLIENT_GET_DATA_FROM_CACHE_FAILED	1092
EventType: PH_HTTP_CLIENT_GET_INIT_RESPONSE_FAILED	1093
EventType: PH_HTTP_CLIENT_GET_INIT_RESPONSE_WARNING	1093
EventType: PH_HTTP_CLIENT_GET_RESPONSE_WARNING	1093
EventType: PH_HTTP_CLIENT_HOST_IS_NULL	1094
EventType: PH_HTTP_CLIENT_INIT_FAILURE	1094
EventType: PH_HTTP_CLIENT_INIT_WARNING	1094
EventType: PH_HTTP_CLIENT_INVALID_FILE_SIZE	1094
EventType: PH_HTTP_CLIENT_MKSTEMP_FAILED	1095
EventType: PH_HTTP_CLIENT_NO_FILE_PARAM	1095
EventType: PH_HTTP_CLIENT_PICK_SUPER_FAILED	1095
EventType: PH_HTTP_CLIENT_PREP_REQUEST_ERROR	1095
EventType: PH_HTTP_CLIENT_PUT_REDIRECT_FAILURE	1096
EventType: PH_HTTP_CLIENT_SETOPT_FAILED	1096
EventType: PH_HTTP_CLIENT_SET_HOST_WARNING	1096
EventType: PH_HTTP_CLIENT_UPLOAD_FILE_FAILED	1096
EventType: PH_HTTP_CLIENT_WRITE_CACHE_NULL	1097
EventType: PH_HTTP_INIT_FAILURE	1097
EventType: PH_HTTP_RESPONSE_FAILURE	1097
EventType: PH_INCIDENT_ACTION_STATUS	1097
EventType: PH_INVALID_IP_ADDR	1098
EventType: PH_INVALID_PARAM	1098
EventType: PH_INVALID_PARAM_CNT	1098
EventType: PH_INVALID_PARAM_VAL_EMPTY	1099
EventType: PH_LOAD_CONFIG_CHANGE_FAILED	1099
EventType: PH_LOOKUP_TABLE_CANNOT_LOAD_DATA	1099
EventType: PH_MODULE_ABORT	1100
EventType: PH_MODULE_ABORT_FOUND	1100
EventType: PH_MODULE_ACCEPTED_CONN	1100
EventType: PH_MODULE_ACE_ACCEPTOR_FAILED	1101
EventType: PH_MODULE_ACE_HANDLE_EVENT_ERROR	1101
EventType: PH_MODULE_COMM_ERROR	1101
EventType: PH_MODULE_COMM_HANDLER_REG	1101
EventType: PH_MODULE_COMM_PORTS_OPENED	1102
EventType: PH_MODULE_DB_CONFIG_LOADED	1102
EventType: PH_MODULE_DIODE_CONFIG_ERROR	1102

EventType: PH_MODULE_EXCEPTION_NOT_CAUGHT	1102
EventType: PH_MODULE_EXITING	1103
EventType: PH_MODULE_EXIT_OK	1103
EventType: PH_MODULE_HEARTBEAT_INIT	1103
EventType: PH_MODULE_INITIALIZING	1103
EventType: PH_MODULE_INIT_COMPLETE	1103
EventType: PH_MODULE_INIT_FAILURE	1104
EventType: PH_MODULE_LOADED_NEW_CONFIG	1104
EventType: PH_MODULE_LOAD_DIODE_CRED_ERROR	1104
EventType: PH_MODULE_LOCAL_CONFIG_LOADED	1104
EventType: PH_MODULE_LOCAL_CONFIG_SECTION_ERROR	1105
EventType: PH_MODULE_LOCAL_CONFIG_VALUE_ERROR	1105
EventType: PH_MODULE_LOG_LEVEL_CHANGE	1105
EventType: PH_MODULE_RECVD_EXIT_EXT	1106
EventType: PH_MODULE_RECVD_EXIT_MONITOR	1106
EventType: PH_MODULE_RECVD_NEW_CONFIG	1106
EventType: PH_MODULE_RECVD_START	1106
EventType: PH_MODULE_SETPIDFILE_ERR	1107
EventType: PH_MODULE_UNABLE_INIT_SHARED_STORE	1107
EventType: PH_MODULE_UNABLE_OPEN_COMM_PORT	1107
EventType: PH_NOTIFICATION_ACCEPT_FAILURE	1107
EventType: PH_NOTIFICATION_CALLBACK_ERROR	1108
EventType: PH_NOTIFICATION_CONN_FAILED	1108
EventType: PH_NOTIFICATION_INIT_FAILED	1108
EventType: PH_NOTIFICATION_NO_RESPONSE	1108
EventType: PH_NOTIFICATION_RETURN_FAILURE	1109
EventType: PH_NOTIFICATION_SEND_FAILURE	1109
EventType: PH_NOTIFICATION_SEND_FILE_FAILURE	1109
EventType: PH_OBJECT_NOT_FOUND	1109
EventType: PH_PDF_BUILDER_ERROR	1109
EventType: PH_READER_BLOCK_WRITE	1110
EventType: PH_Rule_AbuseCH_Botnetc2_MalwareIP_Inbound	1110
EventType: PH_Rule_AbuseCH_Botnetc2_MalwareIP_Outbound	1110
EventType: PH_Rule_Blocklist_MalwareIP_Inbound	1110
EventType: PH_Rule_Blocklist_MalwareIP_Outbound	1110
EventType: PH_Rule_C2_Tracker_MalwareIP_Inbound	1111
EventType: PH_Rule_C2_Tracker_MalwareIP_Outbound	1111
EventType: PH_Rule_CINSScore_MalwareIP_Inbound	1111
EventType: PH_Rule_CINSScore_MalwareIP_Outbound	1111
EventType: PH_Rule_CertPL_MalwareDomain_Inbound	1111
EventType: PH_Rule_CertPL_MalwareDomain_Outbound	1111
EventType: PH_Rule_Cisco_Talos_MalwareIP_Inbound	1112
EventType: PH_Rule_Cisco_Talos_MalwareIP_Outbound	1112
EventType: PH_Rule_Cluster_DBLeader_Changed	1112
EventType: PH_Rule_Cluster_REPL_Leader_Changed	1112
EventType: PH_Rule_DigitalSide_MalwareDomain_Inbound	1112
EventType: PH_Rule_DigitalSide_MalwareDomain_Outbound	1113
EventType: PH_Rule_DigitalSide_MalwareIP_Inbound	1113
EventType: PH_Rule_DigitalSide_MalwareIP_Outbound	1113

EventType: PH_Rule_DigitalSide_MalwareURL_Outbound	1113
EventType: PH_Rule_FML_Antispam_Malicious_File	1113
EventType: PH_Rule_FML_Antispam_Malicious_Url	1113
EventType: PH_Rule_FireHol_MalwareIP_Inbound	1114
EventType: PH_Rule_FireHol_MalwareIP_Outbound	1114
EventType: PH_Rule_FortiRecon_MalwareDomain_Inbound	1114
EventType: PH_Rule_FortiRecon_MalwareDomain_Outbound	1114
EventType: PH_Rule_FortiRecon_MalwareIP_Inbound	1114
EventType: PH_Rule_FortiRecon_MalwareIP_Outbound	1115
EventType: PH_Rule_FortiRecon_MalwareURL_Outbound	1115
EventType: PH_Rule_FortiSOAR_MalwareDomain_Inbound	1115
EventType: PH_Rule_FortiSOAR_MalwareDomain_Outbound	1115
EventType: PH_Rule_FortiSOAR_MalwareIP_Inbound	1115
EventType: PH_Rule_FortiSOAR_MalwareIP_Outbound	1115
EventType: PH_Rule_FortiSOAR_MalwareURL_Outbound	1116
EventType: PH_Rule_Greensnow_MalwareIP_Inbound	1116
EventType: PH_Rule_Greensnow_MalwareIP_Outbound	1116
EventType: PH_Rule_IPSum_MalwareIP_Inbound	1116
EventType: PH_Rule_IPSum_MalwareIP_Outbound	1116
EventType: PH_Rule_MISP_MalwareDomain_Inbound	1117
EventType: PH_Rule_MISP_MalwareDomain_Outbound	1117
EventType: PH_Rule_MISP_MalwareIP_Inbound	1117
EventType: PH_Rule_MISP_MalwareIP_Outbound	1117
EventType: PH_Rule_MISP_MalwareURL_Outbound	1117
EventType: PH_Rule_Mandiant_MalwareDomain_Inbound	1117
EventType: PH_Rule_Mandiant_MalwareDomain_Outbound	1118
EventType: PH_Rule_Mandiant_MalwareIP_Inbound	1118
EventType: PH_Rule_Mandiant_MalwareIP_Outbound	1118
EventType: PH_Rule_Mandiant_MalwareURL_Outbound	1118
EventType: PH_Rule_OPENCTI_MalDomain_Inbound	1118
EventType: PH_Rule_OPENCTI_MalDomain_Outbound	1119
EventType: PH_Rule_OPENCTI_MalwareIP_Inbound	1119
EventType: PH_Rule_OPENCTI_MalwareIP_Outbound	1119
EventType: PH_Rule_OPENCTI_MalwareURL_Outbound	1119
EventType: PH_Rule_OpenPhish_MalwareURL_Outbound	1119
EventType: PH_Rule_Proofpoint_MalwareIP_Inbound	1119
EventType: PH_Rule_Proofpoint_MalwareIP_Outbound	1120
EventType: PH_Rule_Snort_MalwareIP_Inbound	1120
EventType: PH_Rule_Snort_MalwareIP_Outbound	1120
EventType: PH_Rule_ThreatFox_MalwareURL_Outbound	1120
EventType: PH_Rule_TweetFeed_MalwareDomain_Inbound	1120
EventType: PH_Rule_TweetFeed_MalwareDomain_Outbound	1121
EventType: PH_Rule_TweetFeed_MalwareURL_Outbound	1121
EventType: PH_Rule_Tweetfeed_MalwareIP_Inbound	1121
EventType: PH_Rule_Tweetfeed_MalwareIP_Outbound	1121
EventType: PH_SAAS_OP_COLLECTOR_DOWN	1121
EventType: PH_SAAS_OP_COLLECTOR_UP	1121
EventType: PH_SER_MON_SERVICE_DOWN	1122
EventType: PH_SHAREDSTORE_ACQUIRE_ERROR	1122

EventType: PH_SHAREDSTORE_WRITER_POS_UNEXPECTED_ALTERED	1122
EventType: PH_SHAREDSTORE_WRITE_ERROR	1122
EventType: PH_SSL_SHUTDOWN_ERROR	1123
EventType: PH_SYSTEM_DROP_UNKNOWN_ORG	1123
EventType: PH_SYSTEM_RAW_EVENT_SIZE	1123
EventType: PH_SYSTEM_STORAGE_LOW	1123
EventType: PH_SYS_ERROR_XML_SEND_ERROR	1124
EventType: PH_SYS_ERROR_XML_SENT	1124
EventType: PH_TASK_DATA_EMPTY	1124
EventType: PH_TASK_DATA_IS_WRONG	1124
EventType: PH_TASK_FAILED	1125
EventType: PH_TASK_NOT_CONTAIN_LIC	1125
EventType: PH_TASK_RUN_COMMAND_FAILED	1125
EventType: PH_TASK_SEND_FAILED	1126
EventType: PH_TASK_UNSUPPORT	1126
EventType: PH_THREAD_EXITING	1126
EventType: PH_THREAD_RECVD_EXIT	1127
EventType: PH_THREAD_STARTING	1127
EventType: PH_UNABLE_ACCESS_DIR	1127
EventType: PH_UNABLE_ALLOC_MEMORY	1127
EventType: PH_UNABLE_CREATE_DIR	1128
EventType: PH_UNABLE_CREATE_FILE	1128
EventType: PH_UNABLE_CREATE_TIMER	1128
EventType: PH_UNABLE_OPEN_DIR	1129
EventType: PH_UNABLE_OPEN_FILE	1129
EventType: PH_UNABLE_PARSE_XML	1129
EventType: PH_UNABLE_RENAME_FILE	1130
EventType: PH_UNRESOLVABLE_HOSTNAME	1130
EventType: PH_UNRESOLVABLE_IP	1130
EventType: PH_UTIL_BIZ_CHANGE_UPDATE_SPAWN_FAILURE	1131
EventType: PH_UTIL_BIZ_HTTP_REQUEST_FAILURE	1131
EventType: PH_UTIL_CMD_FAILURE	1131
EventType: PH_UTIL_CONFIG_IP_MISSING	1131
EventType: PH_UTIL_CONFIG_LOAD_FAILURE	1131
EventType: PH_UTIL_CONFIG_LOAD_FILE_ACESS_FAILURE	1132
EventType: PH_UTIL_CONFIG_PARSE_FAILURE	1132
EventType: PH_UTIL_CONFIG_UNKNOWN_SERVER_TYPE	1132
EventType: PH_UTIL_CONNECTION_ERROR	1133
EventType: PH_UTIL_CSV_LINE_ILLEGAL	1133
EventType: PH_UTIL_CSV_READ_FAILURE	1133
EventType: PH_UTIL_CUSTOMER_COLLECTOR_MISSING	1134
EventType: PH_UTIL_CUSTOMER_COLLECTOR_PARSE_FAILURE	1134
EventType: PH_UTIL_CUSTOMER_DOMAIN_MISSING	1134
EventType: PH_UTIL_CUSTOMER_INFO_PARSE_FAILURE	1134
EventType: PH_UTIL_CUSTOMER_PARSE_FAILURE	1135
EventType: PH_UTIL_DASHBOARD_DUPLICATE_IP	1135
EventType: PH_UTIL_DASHBOARD_DUPLICATE_ITEM	1135
EventType: PH_UTIL_DASHBOARD_PARSE_FAILURE	1135
EventType: PH_UTIL_DEVICE_MAP_PROP_ERROR	1136

EventType: PH_UTIL_DEVICE_PROP_ERROR	1136
EventType: PH_UTIL_DEVICE_SIMPLE_PROP_PARSE_FAILURE	1136
EventType: PH_UTIL_DGA_FREQ_FILE_OPEN_FAILURE	1137
EventType: PH_UTIL_DGA_WHITELIST_FILE_OPEN_FAILURE	1137
EventType: PH_UTIL_DIR_CREATE_FAILURE	1137
EventType: PH_UTIL_DIR_CREATE_RETRIED	1138
EventType: PH_UTIL_DIR_OPEN_FAILURE	1138
EventType: PH_UTIL_DIR_PARENT_NOT_EXIST	1138
EventType: PH_UTIL_DIR_REMOVE_FAILURE	1139
EventType: PH_UTIL_DISK_USAGE_INFO_GET_FAILURE	1139
EventType: PH_UTIL_DISPATH_CMD_XML_ILLEGAL	1139
EventType: PH_UTIL_DISPATH_CMD_XML_PARSE_FAILURE	1140
EventType: PH_UTIL_EMAIL_SEND_FAILURE	1140
EventType: PH_UTIL_ETCD_COMPAGN_FAILED	1140
EventType: PH_UTIL_ETCD_GET_LEADER_FAILED	1141
EventType: PH_UTIL_ETCD_LEASE_FAILED	1141
EventType: PH_UTIL_ETCD_SET_FAILED	1141
EventType: PH_UTIL_EVENT_FILE_ERROR	1142
EventType: PH_UTIL_EVENT_GROUP_ERROR	1142
EventType: PH_UTIL_EVENT_STATUS_REPORTER_SPAWN_FAILURE	1142
EventType: PH_UTIL_EVENT_STATUS_UPLOAD_FAILURE	1142
EventType: PH_UTIL_EVENT_TYPE_ERROR	1143
EventType: PH_UTIL_FILE_NOT_EXIST	1143
EventType: PH_UTIL_FILE_OPEN_FAILURE	1143
EventType: PH_UTIL_FILE_READ_FAILURE	1144
EventType: PH_UTIL_FILE_SIZE_MISMATCH	1144
EventType: PH_UTIL_FILE_SIZE_TOO_SMALL	1144
EventType: PH_UTIL_FILE_STATFS_FAILURE	1144
EventType: PH_UTIL_FILE_STAT_FAILURE	1145
EventType: PH_UTIL_FILE_WRITE_FAILURE	1145
EventType: PH_UTIL_FORK_FAILURE	1145
EventType: PH_UTIL_GET_ADDR_FAILURE	1146
EventType: PH_UTIL_GET_ATTR_NAME_FAILED	1146
EventType: PH_UTIL_GET_JOB_STATUS_FAILURE	1146
EventType: PH_UTIL_HOSTNAME_GET_FAILURE	1147
EventType: PH_UTIL_INET_PTON_FAILURE	1147
EventType: PH_UTIL_INODE_INFO_GET_FAILURE	1147
EventType: PH_UTIL_INVALID_PARAM	1148
EventType: PH_UTIL_IOCTL_FAILURE	1148
EventType: PH_UTIL_IOCTL_SIOCGIFADDR_FAILURE	1148
EventType: PH_UTIL_IP_TYPE_INVALID	1149
EventType: PH_UTIL_IP_TYPE_MISMATCH	1149
EventType: PH_UTIL_JOB_STATUS_REPORTER_SPAWN_FAILURE	1149
EventType: PH_UTIL_JOB_STATUS_UPLOAD_FAILURE	1149
EventType: PH_UTIL_JSON_GET_NODE_FAILURE	1149
EventType: PH_UTIL_JSON_GET_TOTAL_COUNT_FAILURE	1150
EventType: PH_UTIL_JSON_OBJ_EMPTY	1150
EventType: PH_UTIL_JSON_PARSE_FAILURE	1150
EventType: PH_UTIL_KILLPG_FAILURE	1151

EventType: PH_UTIL_LOAD_EXT_FUNC_FILE_OPEN_FAILUE	1151
EventType: PH_UTIL_LOAD_EXT_FUNC_FORMAT_INVALID	1151
EventType: PH_UTIL_LOAD_EXT_FUNC_GET_NAME_FAILUE	1152
EventType: PH_UTIL_LOCAL_IP_MISSING	1152
EventType: PH_UTIL_LOOKUP_TABLES_DUPLICATE	1152
EventType: PH_UTIL_LOOKUP_TABLES_DUPLICATE_COLUMN	1152
EventType: PH_UTIL_LOOKUP_TABLES_DUPLICATE_KEY	1153
EventType: PH_UTIL_MAIL_CMD_RUN_FAILURE	1153
EventType: PH_UTIL_MAIL_SMTP_INIT_FAILURE	1153
EventType: PH_UTIL_MD5_ERROR	1154
EventType: PH_UTIL_MEM_ALLOC_FAILURE	1154
EventType: PH_UTIL_MKDTEMP_FAILURE	1154
EventType: PH_UTIL_MKSTEMP_FAILURE	1154
EventType: PH_UTIL_MMAP_FAILURE	1155
EventType: PH_UTIL_MOVE_FILE_FAILURE	1155
EventType: PH_UTIL_NOTIFICATION_SENDER_SPAWN_FAILURE	1156
EventType: PH_UTIL_NOTIFICATION_SERVER_INIT_FAILURE	1156
EventType: PH_UTIL_NOTIFICATION_UPLOAD_FAILURE	1156
EventType: PH_UTIL_PCRE_COMPILE_FAILED	1156
EventType: PH_UTIL_PHOENIX_CONFIG_ITEM_MISSING	1157
EventType: PH_UTIL_PIPE_FAILURE	1157
EventType: PH_UTIL_PROP_DEF_SET_PARSE_FAILURE	1157
EventType: PH_UTIL_REDIS_CONNECTION_ERROR	1158
EventType: PH_UTIL_REGEX_PATTERN_EMPTY	1158
EventType: PH_UTIL_REGEX_PATTERN_TOO_LONG	1158
EventType: PH_UTIL_SEND_DATA_FAILED	1158
EventType: PH_UTIL_SEND_TO_UDP_PORT_FAILURE	1159
EventType: PH_UTIL_SETPGRP_FAILURE	1159
EventType: PH_UTIL_SET_JOB_STATUS_FAILURE	1159
EventType: PH_UTIL_SOCKET_FAILURE	1160
EventType: PH_UTIL_STR_TO_IP_FAILURE	1160
EventType: PH_UTIL_SVN_DIFF_FAILURE	1160
EventType: PH_UTIL_SYS_ERROR_REPORTER_INIT_FAILURE	1161
EventType: PH_UTIL_TIME_RANGE_INVALID	1161
EventType: PH_UTIL_TIME_STR_FORMAT_INVALID	1161
EventType: PH_UTIL_TLS_SERVER_RECV_FAILED	1162
EventType: PH_UTIL_UNKNOWN_PHOENIX_ERROR_NUMBER	1162
EventType: PH_UTIL_VALUE_GROUP_ERROR	1162
EventType: PH_UTIL_WAITPID_FAILURE	1162
EventType: PH_UTIL_WAITPID_LAST_TRY_FAILUE	1163
EventType: PH_UTIL_WINDOWS_BID_LOAD_FAILURE	1163
EventType: PH_UTIL_WRITE_BIN_FILE_OPEN_FAILURE	1163
EventType: PH_UTIL_WRITE_FILE_OPEN_FAILURE	1164
EventType: PH_UTIL_XML_HANDLING_ERROR	1164
EventType: PH_UTIL_ZIP_DECOMPRESS_FAILED	1164
EventType: PH_WORKER_DOWN	1165
EventType: PH_WORKER_PROVISION_FAILED	1165
EventType: PH_WORKER_UP	1165
EventType: PH_WS_COMM_ERROR	1165

All Logs Page 1	1166
EventType: JDBC_PULL_UNSUPP_DEV	1179
EventType: JMX_JDBC_PULL_STAT	1179
EventType: MSSQL_JDBC_PULL_STAT	1179
EventType: MYSQL_JDBC_PULL_STAT	1179
EventType: ORADB_JDBC_PULL_STAT	1179
EventType: PH_AGENTMGR_ACI_ATTR_NOT_FOUND	1180
EventType: PH_AGENTMGR_ACI_CURL_HANDLE_GET_FAILED	1180
EventType: PH_AGENTMGR_ACI_FILE_WRITE_ERROR	1180
EventType: PH_AGENTMGR_ACI_JSON_PARSE_FAILED	1180
EventType: PH_AGENTMGR_ACI_SERVER_EMPTY	1180
EventType: PH_AGENTMGR_ACI_TOKEN_GET_FAILED	1181
EventType: PH_AGENTMGR_ALERTLOGIC_CURL_HANDLE_GET_FAILED	1181
EventType: PH_AGENTMGR_ALERTLOGIC_FILE_LOAD_ERROR	1181
EventType: PH_AGENTMGR_ALERTLOGIC_FILE_READ_ERROR	1181
EventType: PH_AGENTMGR_ALERTLOGIC_FILE_WRITE_ERROR	1182
EventType: PH_AGENTMGR_ALERTLOGIC_INVALID_DATA	1182
EventType: PH_AGENTMGR_ALERTLOGIC_INVALID_PATH	1182
EventType: PH_AGENTMGR_ALERTLOGIC_QUERY_INTERVAL_TOO_LONG	1183
EventType: PH_AGENTMGR_ALERTLOGIC_SERVER_EMPTY	1183
EventType: PH_AGENTMGR_AMPCLOUD_CURL_CONNECT_FAILED	1183
EventType: PH_AGENTMGR_AMPCLOUD_CURL_HANDLE_GET_FAILED	1183
EventType: PH_AGENTMGR_AMPCLOUD_FILE_LOAD_ERROR	1183
EventType: PH_AGENTMGR_AMPCLOUD_FILE_READ_ERROR	1184
EventType: PH_AGENTMGR_AMPCLOUD_INVALID_DATA	1184
EventType: PH_AGENTMGR_AMPCLOUD_JSON_PARSE_FAILED	1184
EventType: PH_AGENTMGR_AMPCLOUD_NO_DEFINE_SEVERITY	1185
EventType: PH_AGENTMGR_AMPCLOUD_SERVER_EMPTY	1185
EventType: PH_AGENTMGR_API_PERMISSION_MISSING	1185
EventType: PH_AGENTMGR_AWSCLOUDWATCH_GETLOGS	1185
EventType: PH_AGENTMGR_AWSFLOWLOG_EVENT_PULL_FAILED	1186
EventType: PH_AGENTMGR_AWSFLOWLOG_FILE_WRITE_ERROR	1186
EventType: PH_AGENTMGR_AWSFLOWLOG_LOG_FORMAT_WRONG	1186
EventType: PH_AGENTMGR_AWSKINESIS_CONSUMER_START_FAILED	1187
EventType: PH_AGENTMGR_AWS_CACHE_FILE_ERROR	1187
EventType: PH_AGENTMGR_AWS_DELETE_OJECTKEY_FAILED	1187
EventType: PH_AGENTMGR_AWS_DOWNLOAD_OJECT_FAILED	1187
EventType: PH_AGENTMGR_AWS_EVT_DOWNLOAD_FAILED	1188
EventType: PH_AGENTMGR_AWS_EVT_SEND_FAILED	1188
EventType: PH_AGENTMGR_AWS_GET_OJECTKEY_FAILED	1188
EventType: PH_AGENTMGR_AWS_GZ_FILE_OPEN_ERROR	1189
EventType: PH_AGENTMGR_AWS_JSON_PARSE_FAILED	1189
EventType: PH_AGENTMGR_AWS_SQSURL_FORMAT_ERROR	1189
EventType: PH_AGENTMGR_BOX_API_CALL_FAILED	1189
EventType: PH_AGENTMGR_BOX_ATTR_NOT_FOUND	1189
EventType: PH_AGENTMGR_BOX_EVENT_PULL_FAILED	1190
EventType: PH_AGENTMGR_BOX_FILE_ID_EMPTY	1190
EventType: PH_AGENTMGR_BOX_FILE_LIMIT_EXCEED	1190
EventType: PH_AGENTMGR_BOX_FILE_NOT_MONITORED_ERROR	1190

EventType: PH_AGENTMGR_BOX_FILE_PATH_PARSE_FAILED	1191
EventType: PH_AGENTMGR_BOX_FILE_TYPE_WRONG	1191
EventType: PH_AGENTMGR_BOX_FOLDER_TYPE_WRONG	1191
EventType: PH_AGENTMGR_BOX_HTTP_NO_RESPONSE	1191
EventType: PH_AGENTMGR_BOX_JSON_PARSE_FAILED	1192
EventType: PH_AGENTMGR_BOX_RESPONSE_NO_SPECIAL_ATTRIBUTE	1192
EventType: PH_AGENTMGR_BOX_TIME_CONVERT_FAILED	1192
EventType: PH_AGENTMGR_BOX_XML_PARSE_FAILED	1192
EventType: PH_AGENTMGR_CISCOAMP_CONSUMER_START_FAILED	1193
EventType: PH_AGENTMGR_CLOUDPASSAGE_API_CALL_FAILED	1193
EventType: PH_AGENTMGR_CLOUDPASSAGE_FILE_WRITE_ERROR	1193
EventType: PH_AGENTMGR_CLOUDPASSAGE_GET_EVENT_FAILED	1193
EventType: PH_AGENTMGR_CLOUDPASSAGE_JSON_EMPTY	1194
EventType: PH_AGENTMGR_CLOUDPASSAGE_JSON_PARSE_FAILED	1194
EventType: PH_AGENTMGR_CLOUDPASSAGE_TOKEN_EMPTY	1194
EventType: PH_AGENTMGR_CLOUDTRAIL_FILE_READ_FAILED	1194
EventType: PH_AGENTMGR_CONFIG_ERROR	1195
EventType: PH_AGENTMGR_CONFIG_VERSION_SEND_FAILED	1195
EventType: PH_AGENTMGR_CONFIG_WARNING	1195
EventType: PH_AGENTMGR_CREDENTIAL_GET_FAILED	1196
EventType: PH_AGENTMGR_CROWDSTRIKE_GET_DATAFEED_URL_FAILED	1196
EventType: PH_AGENTMGR_CUST_RESULT_UPLOAD_FAILED	1196
EventType: PH_AGENTMGR_DIR_CREATE_FAILED	1196
EventType: PH_AGENTMGR_EVENT_PULL_FAILED	1197
EventType: PH_AGENTMGR_FALCONDATAREP_SCRIPT_FAILED	1197
EventType: PH_AGENTMGR_FILE_PARSE_ERROR	1197
EventType: PH_AGENTMGR_FILE_WRITE_ERROR	1198
EventType: PH_AGENTMGR_FIREAMP_CERT_DOWNLOAD_FAILED	1198
EventType: PH_AGENTMGR_FIREAMP_DATA_FORMAT_SET_FAILED	1198
EventType: PH_AGENTMGR_FIREAMP_EVENT_PULL_FAILED	1199
EventType: PH_AGENTMGR_FIREAMP_EVT_TYPE_LOAD_FAILED	1199
EventType: PH_AGENTMGR_FIREAMP_FILE_LOAD_ERROR	1199
EventType: PH_AGENTMGR_FIREAMP_FILE_OPEN_ERROR	1200
EventType: PH_AGENTMGR_FIREAMP_INVALID_DATA	1200
EventType: PH_AGENTMGR_FIREAMP_NEW_AGENT_FAILED	1200
EventType: PH_AGENTMGR_FIREAMP_NO_ATTR	1200
EventType: PH_AGENTMGR_FIREAMP_NO_PROTOCOL	1200
EventType: PH_AGENTMGR_FORTICASB_GET_SERVICE_ALERT_ERROR	1201
EventType: PH_AGENTMGR_FORTICASB_GET_SERVICE_ERROR	1201
EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_FAILED	1201
EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_NEXT_PAGE	1202
EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_NO_RESULTS	1202
EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_RESULTS	1202
EventType: PH_AGENTMGR_FORTINDR_GET_BUCKET_KEY	1202
EventType: PH_AGENTMGR_FORTINDR_GET_BUCKET_OBJ	1203
EventType: PH_AGENTMGR_GET_SCAN_RESULTS_FAILED	1203
EventType: PH_AGENTMGR_GITHUB_API_CALL_FAILED	1204
EventType: PH_AGENTMGR_GITHUB_CREDENTIAL_GET_FAILED	1204
EventType: PH_AGENTMGR_GITHUB_EVENT_PULL_FAILED	1204

EventType: PH_AGENTMGR_GITHUB_FILE_OPEN_ERROR	1205
EventType: PH_AGENTMGR_GITHUB_JSON_PARSE_FAILED	1205
EventType: PH_AGENTMGR_GITHUB_TIME_CONVERT_FAILED	1205
EventType: PH_AGENTMGR_GIT_CLONE_REPO_FAILED	1205
EventType: PH_AGENTMGR_GIT_HANDLE_ERR_FILE_FAILED	1206
EventType: PH_AGENTMGR_GIT_PULL_EVT_FAILED	1206
EventType: PH_AGENTMGR_GIT_SAVE_COMMITID_FAILED	1206
EventType: PH_AGENTMGR_GZ_FILE_OPEN_ERROR	1206
EventType: PH_AGENTMGR_INIT_AGENT	1207
EventType: PH_AGENTMGR_INIT_CACHE_FILE_FAILED	1207
EventType: PH_AGENTMGR_INIT_NO_CRED	1207
EventType: PH_AGENTMGR_INVALID_MGR	1207
EventType: PH_AGENTMGR_IPS_AUTH_FAILED	1208
EventType: PH_AGENTMGR_IPS_EVENT_PULL_FAILED	1208
EventType: PH_AGENTMGR_IPS_FILE_OPEN_ERROR	1208
EventType: PH_AGENTMGR_IPS_OBTAIN_SUBSCRIPTION_FAILED	1208
EventType: PH_AGENTMGR_IPS_SET_SSL_FAILED	1209
EventType: PH_AGENTMGR_JAVA_AGENT_PIPE_WRITE_FAILED	1209
EventType: PH_AGENTMGR_JAVA_AGENT_START_FAILED	1209
EventType: PH_AGENTMGR_JAVA_AGENT_TYPE_UNKNOWN	1209
EventType: PH_AGENTMGR_JAVA_AGENT_USER_MISSING	1210
EventType: PH_AGENTMGR_JAVA_AGENT_ZOMBIE	1210
EventType: PH_AGENTMGR_JAVA_CMD_SEND_FAILED	1210
EventType: PH_AGENTMGR_JAVA_FORK_FAILED	1210
EventType: PH_AGENTMGR_JAVA_INCOMPLETE_DEV_INFO	1211
EventType: PH_AGENTMGR_JAVA_NO_DEV_TYPE_FOR_JDBC	1211
EventType: PH_AGENTMGR_JAVA_NO_STATUS_FILE	1211
EventType: PH_AGENTMGR_JAVA_PIPE_FAILED	1211
EventType: PH_AGENTMGR_JAVA_PROCESS_STATE_GET_FAILED	1212
EventType: PH_AGENTMGR_JAVA_SIGKILL_SEND_FAILED	1212
EventType: PH_AGENTMGR_JAVA_UNSUPPORTED_DEV_TYPE_FOR_JDBC	1212
EventType: PH_AGENTMGR_JAVA_USER_PWD_GET_FAILED	1213
EventType: PH_AGENTMGR_JSON_PARSE_FAILED	1213
EventType: PH_AGENTMGR_KAFKA_CONSUME_LOG_FAILED	1213
EventType: PH_AGENTMGR_KAFKA_CREATE_CONSUMER	1213
EventType: PH_AGENTMGR_KAFKA_CREATE_CONSUMER_FAILED	1214
EventType: PH_AGENTMGR_KAFKA_CREATE_PRODUCER_FAILED	1214
EventType: PH_AGENTMGR_KAFKA_CREATE_TOPIC_FAILED	1214
EventType: PH_AGENTMGR_KAFKA_ERROR	1215
EventType: PH_AGENTMGR_KAFKA_METADATA_FAILED	1215
EventType: PH_AGENTMGR_KAFKA_PRODUCER_ERROR	1216
EventType: PH_AGENTMGR_KAFKA_PULL_JOB_FAILED	1216
EventType: PH_AGENTMGR_KAFKA_REBALANCE	1216
EventType: PH_AGENTMGR_KAFKA_RELEASE_CONSUMER	1216
EventType: PH_AGENTMGR_KAFKA_START_FAILED	1217
EventType: PH_AGENTMGR_KAFKA_SUBSCRIBE_FAILED	1217
EventType: PH_AGENTMGR_KAFKA_UPDATE_CONFIG_FAILED	1217
EventType: PH_AGENTMGR_KAFKA_UPDATE_ERROR	1218
EventType: PH_AGENTMGR_KILL_PROCESS	1218

EventType: PH_AGENTMGR_MSAZURE_CONFIG_ARM_FAILED	1218
EventType: PH_AGENTMGR_MSAZURE_DOWNLOAD_FAILED	1219
EventType: PH_AGENTMGR_MSAZURE_JSON_EMPTY	1219
EventType: PH_AGENTMGR_MSAZURE_JSON_FILE_NAME_EMPTY	1219
EventType: PH_AGENTMGR_MSAZURE_JSON_FILE_PARSE_FAILED	1219
EventType: PH_AGENTMGR_MSAZURE_JSON_PARSE_FAILED	1219
EventType: PH_AGENTMGR_MSAZURE_LOGIN_FAILED	1220
EventType: PH_AGENTMGR_MSG_QUEUE_ACCESS_FAILED	1220
EventType: PH_AGENTMGR_MSG_RECV_FAILED	1220
EventType: PH_AGENTMGR_OCI_SET_INSTANCE_NAME_FAILED	1220
EventType: PH_AGENTMGR_OFFICE365_API_CALL_FAILED	1221
EventType: PH_AGENTMGR_OFFICE365_EVENT_PULL_FAILED	1221
EventType: PH_AGENTMGR_OFFICE365_FILE_WRITE_ERROR	1221
EventType: PH_AGENTMGR_OFFICE365_GET_SUBSCRIBE_FAILED	1222
EventType: PH_AGENTMGR_OFFICE365_JSON_PARSE_FAILED	1222
EventType: PH_AGENTMGR_OFFICE365_START_SUBSCRIBE_FAILED	1222
EventType: PH_AGENTMGR_OFFICE365_SUBSCRIBE_EMPTY	1222
EventType: PH_AGENTMGR_OFFICE365_SUBSCRIBE_FAILED	1223
EventType: PH_AGENTMGR_OFFICE365_TOKEN_EMPTY	1223
EventType: PH_AGENTMGR_OKTA_EVT_DOWNLOAD_FAILED	1223
EventType: PH_AGENTMGR_OKTA_FILE_WRONG	1223
EventType: PH_AGENTMGR_OKTA_NO_USER_INFO	1224
EventType: PH_AGENTMGR_OKTA_RESULT_UPLOAD_FAILED	1224
EventType: PH_AGENTMGR_OKTA_RESULT_UPLOAD_WARNING	1224
EventType: PH_AGENTMGR_PARSER_UNABLE_CONNECT	1224
EventType: PH_AGENTMGR_PERF_OBJ_PARSE_FAILURE	1225
EventType: PH_AGENTMGR_PROCESS_INIT_FAILED	1225
EventType: PH_AGENTMGR_PULLING_JOB_OUTDATE	1225
EventType: PH_AGENTMGR_REMOVE_FILE_FAILED	1225
EventType: PH_AGENTMGR_REST_API_CALL_FAILED	1226
EventType: PH_AGENTMGR_RSAS_XML_PARSE_FAILED	1226
EventType: PH_AGENTMGR_RUN_CMD_FAILED	1226
EventType: PH_AGENTMGR_RUN_SCRIPT_FAILED	1226
EventType: PH_AGENTMGR_RUN_SCRIPT_WITHOUT_TASK_ID	1227
EventType: PH_AGENTMGR_SALESFORCE_ATTR_NOT_FOUND	1227
EventType: PH_AGENTMGR_SALESFORCE_COLUMN_NOT_FOUND	1227
EventType: PH_AGENTMGR_SALESFORCE_CURL_EXECUTE_FAILED	1227
EventType: PH_AGENTMGR_SALESFORCE_CURL_HANDLE_GET_FAILED	1228
EventType: PH_AGENTMGR_SALESFORCE_FILE_LOAD_ERROR	1228
EventType: PH_AGENTMGR_SALESFORCE_FILE_WRITE_ERROR	1228
EventType: PH_AGENTMGR_SALESFORCE_INVALID_DATA	1228
EventType: PH_AGENTMGR_SALESFORCE_INVALID_LOG_FILE	1229
EventType: PH_AGENTMGR_SALESFORCE_JSON_PARSE_FAILED	1229
EventType: PH_AGENTMGR_SALESFORCE_LOGIN_FAILED	1229
EventType: PH_AGENTMGR_SALESFORCE_SERVER_EMPTY	1229
EventType: PH_AGENTMGR_SALESFORCE_TOKEN_GET_FAILED	1229
EventType: PH_AGENTMGR_SALESFORCE_TOKEN_REGET_FAILED	1230
EventType: PH_AGENTMGR_SALESFORCE_VERSION_PATH_EMPTY	1230
EventType: PH_AGENTMGR_SALESFORCE_XML_PARSE_FAILED	1230

EventType: PH_AGENTMGR_SCRIPT_NOTIFICATION_SPAWN_FAILED	1230
EventType: PH_AGENTMGR_SERVER_HOST_NAME_RESOLVE_FAILED	1230
EventType: PH_AGENTMGR_SERVER_HOST_NAME_RESOLVE_WARNING	1231
EventType: PH_AGENTMGR_SERVER_IP_RESOLVE_FAILED	1231
EventType: PH_AGENTMGR_SERVER_IP_RESOLVE_WARNING	1231
EventType: PH_AGENTMGR_SETUP_STREAM_FAILED	1231
EventType: PH_AGENTMGR_START_THREAD_FAILED	1232
EventType: PH_AGENTMGR_STATUS_REPORT_FAILED	1232
EventType: PH_AGENTMGR_STATUS_REPORT_INIT_FAILED	1232
EventType: PH_AGENTMGR_STOP_STREAM_FAILED	1232
EventType: PH_AGENTMGR_TENABLE_EXPORT_SCAN_FAILED	1232
EventType: PH_AGENTMGR_TENABLE_GET_DOWNLOAD_FAILED	1233
EventType: PH_AGENTMGR_TENABLE_GET_SCANS_FAILED	1233
EventType: PH_AGENTMGR_TENABLE_GET_STATUS_FAILED	1233
EventType: PH_AGENTMGR_TENABLE_PULL_FAILED	1233
EventType: PH_AGENTMGR_TIME_CONVERSION_FAILED	1234
EventType: PH_AGENTMGR_TIME_STR_FORMAT_INVALID	1234
EventType: PH_AGENTMGR_TOKEN_GET_FAILED	1234
EventType: PH_AGENTMGR_UNPACK_FILE_FAILED	1234
EventType: PH_AGENTMGR_UPDATE_AGENT	1235
EventType: PH_AGENTMGR_UPDATE_BOOKMARK_FAILED	1235
EventType: PH_AGENTMGR_UPDATE_WEBHOOK_CRED_FAILED	1235
EventType: PH_AGENTMGR_UPDATE_WEBHOOK_CRED_SUCCESS	1236
EventType: PH_AGENTMGR_WINDEFATP_API_CALL_FAILED	1236
EventType: PH_AGENTMGR_WINDEFATP_FILE_WRITE_ERROR	1236
EventType: PH_AGENTMGR_WINDEFATP_GET_ALERT_FAILED	1236
EventType: PH_AGENTMGR_WINDEFATP_JSON_EMPTY	1237
EventType: PH_AGENTMGR_WINDEFATP_JSON_PARSE_FAILED	1237
EventType: PH_AGENTMGR_WINDEFATP_TOKEN_EMPTY	1237
EventType: PH_AGENTMGR_WMI_EVENT_PULL_ERROR	1237
EventType: PH_AGENTMGR_WMI_EVENT_PULL_WARNING	1238
EventType: PH_AGENTMGR_WMI_FILE_OPEN_ERROR	1238
EventType: PH_AGENTMGR_WMI_LOG_PULL_ERROR	1238
EventType: PH_AGENTMGR_WMI_MISSING_LOG	1239
EventType: PH_AGENTMGR_WMI_STATUS_REPORT_FAILED	1239
EventType: PH_AGENTMGR_WMI_USER_PWD_GET_FAILED	1239
EventType: PH_AGENTMGR_WVSS_XML_PARSE_FAILED	1239
EventType: PH_AGENTMGR_XML_PARSE_FAILED	1240
EventType: PH_ANOMALY_CONFIG	1240
EventType: PH_ANOMALY_LATERAL_MOVEMENT_ANALYZE	1240
EventType: PH_ANOMALY_LATERAL_MOVEMENT_DETECT	1241
EventType: PH_ANOMALY_LATERAL_MOVEMENT_TRAIN	1241
EventType: PH_ANOMALY_SYSTEM	1242
EventType: PH_ANOMALY_TIMER	1242
EventType: PH_APPSERVER_ADMIN_AGENT_GET_UPDATE_FAILED_	
ERROR	1243
EventType: PH_APPSERVER_ADMIN_AGENT_UNKOWN_TASK_ID_ERROR	1243
EventType: PH_APPSERVER_ADMIN_CUST_GENERATE_KEY_ERROR	1243
EventType: PH_APPSERVER_ADMIN_GET_RESOURCE_FAILED	1243

EventType: PH_APPSERVER_ADMIN_LOCATE_KEY_FAILED	1243
EventType: PH_APPSERVER_ADMIN_RESET_FIELD_FAILED_ERROR	1243
EventType: PH_APPSERVER_AUDIT_REPORT_EXPORT_ERROR	1244
EventType: PH_APPSERVER_BEACON_LIB_ERROR	1244
EventType: PH_APPSERVER_BEACON_REGISTER_ERROR	1244
EventType: PH_APPSERVER_BEACON_SERVER_ERROR	1244
EventType: PH_APPSERVER_BEACON_WEB_SERVER_ERROR	1244
EventType: PH_APPSERVER_BEAN_REF_CHECK_WARN	1245
EventType: PH_APPSERVER_BEAN_SYNC_PROPERTIES_ERROR	1245
EventType: PH_APPSERVER_BEAN_TO_VALUE_ERROR	1245
EventType: PH_APPSERVER_BEAN_TO_XML_ERROR	1245
EventType: PH_APPSERVER_BEAN_VALUE_TO_BEAN_ERROR	1245
EventType: PH_APPSERVER_CMDB_REPORT_DATA_ERROR	1245
EventType: PH_APPSERVER_CMDB_REPORT_EXPORT_ERROR	1246
EventType: PH_APPSERVER_CMDB_REPORT_IMPORT_ERROR	1246
EventType: PH_APPSERVER_CMDB_REPORT_QUERY_ERROR	1246
EventType: PH_APPSERVER_CMDB_REPORT_TYPE_ERROR	1246
EventType: PH_APPSERVER_COLLECTOR_INFO_ERROR	1246
EventType: PH_APPSERVER_COLLECTOR_LICENSE_ERROR	1247
EventType: PH_APPSERVER_COLLECTOR_STATUS_ERROR	1247
EventType: PH_APPSERVER_COMMONPWD_EXPORT_ERROR	1247
EventType: PH_APPSERVER_DASHBOARD_DATA_ERROR	1247
EventType: PH_APPSERVER_DASHBOARD_HTML_BUILD_XML_ERROR	1247
EventType: PH_APPSERVER_DASHBOARD_WIDGET_ERROR	1247
EventType: PH_APPSERVER_DATA_IMPORT_ERROR	1248
EventType: PH_APPSERVER_DATA_ROBUST_INFO_ERROR	1248
EventType: PH_APPSERVER_DB_CONNECTION_CLOSE_ERROR	1248
EventType: PH_APPSERVER_DB_DATA_ERROR	1248
EventType: PH_APPSERVER_DB_DELETE_ERROR	1248
EventType: PH_APPSERVER_DB_QUERY_ERROR	1249
EventType: PH_APPSERVER_DB_UPDATE_ERROR	1249
EventType: PH_APPSERVER_DISCOVERY_CREDENTIAL_DECRYPT_	
PASSWORD_WARN	1249
EventType: PH_APPSERVER_DISCOVERY_RESULT_ENCRYPT_XML_	
ELEMENT_ERROR	1249
EventType: PH_APPSERVER_DISCOVERY_RESULT_ERROR	1249
EventType: PH_APPSERVER_DISCOVERY_RESULT_UNKOWN_TASK_ID_	
ERROR	1250
EventType: PH_APPSERVER_EAMIL_GENERATE_EVENT_ERROR	1250
EventType: PH_APPSERVER_ELASTIC_UPDATE_ERROR	1250
EventType: PH_APPSERVER_EMAIL_PREPARE_DATA_ERROR	1250
EventType: PH_APPSERVER_EVENTDB_EXPORT_ERROR	1250
EventType: PH_APPSERVER_EVENT_ATTRIBUTE_BUILD_XML_ERROR	1250
EventType: PH_APPSERVER_EXPORT_ERROR	1251
EventType: PH_APPSERVER_EXT_THREAT_INTEL_DOWNLOAD_ERROR	1251
EventType: PH_APPSERVER_EXT_THREAT_INTEL_PARSE_ERROR	1251
EventType: PH_APPSERVER_EXT_THREAT_INTEL_UPDATE_ERROR	1251
EventType: PH_APPSERVER_FILE_NOT_FOUND	1251
EventType: PH_APPSERVER_FILE_READ_ERROR	1252

EventType: PH_APPSERVER_FILE_SYSTEM_ERROR	1252
EventType: PH_APPSERVER_FILE_WRITE_ERROR	1252
EventType: PH_APPSERVER_FLEX_INTERCEPTOR_NO_LOGIN_EXCEPTION_ERROR	1252
EventType: PH_APPSERVER_FORTIGUARD_IOC_INTEGRATION_ERROR	1252
EventType: PH_APPSERVER_FRAMEWORK_REGISTER_ERROR	1252
EventType: PH_APPSERVER_FRAMEWORK_RUN_THREAD_ERROR	1253
EventType: PH_APPSERVER_FRAMEWORK_SECURITY_CHECK_LICENSE_WARN	1253
EventType: PH_APPSERVER_FRAMEWORK_SECURITY_GET_ENTITY_MANAGER_ERROR	1253
EventType: PH_APPSERVER_FRAMEWORK_SECURITY_GET_RS_EXPIRATION_ERROR	1253
EventType: PH_APPSERVER_FRAMEWORK_SECURITY_INIT_SYSTEM_ERROR	1253
EventType: PH_APPSERVER_FRAMEWORK_SERVICE_MISSED_WARN	1254
EventType: PH_APPSERVER_FRAMEWORK_SHUTDOWN_SERVICE_STARTER_WARN	1254
EventType: PH_APPSERVER_GENERIC_ERROR	1254
EventType: PH_APPSERVER_GENERIC_INFO	1254
EventType: PH_APPSERVER_GENERIC_WARN	1254
EventType: PH_APPSERVER_GET_MAX_CONFIG_ITEM_COUNT_ERROR	1254
EventType: PH_APPSERVER_GROUP_DATA_ERROR	1255
EventType: PH_APPSERVER_IDENTITYLOCATION_EXPORT_ERROR	1255
EventType: PH_APPSERVER_INCIDENT_NOTIFY_ERROR	1255
EventType: PH_APPSERVER_INCIDENT_UPDATE_ERROR	1255
EventType: PH_APPSERVER_INTEGRATION_ERROR	1255
EventType: PH_APPSERVER_INTEGRATION_UPDATE_POLICY_ERROR	1256
EventType: PH_APPSERVER_INTEGRATION_UPDATE_POLICY_WARN	1256
EventType: PH_APPSERVER_INTEGRATION_WARN	1256
EventType: PH_APPSERVER_IN_INTEGRATION_ERROR	1256
EventType: PH_APPSERVER_IOC_LICENSE_CHECK_FAILED_WARN	1256
EventType: PH_APPSERVER_IOC_TASK_CREATE_FAILED_ERROR	1256
EventType: PH_APPSERVER_JOB_DISTRIBUTE_ERROR	1257
EventType: PH_APPSERVER_LICENSE_EXPIRY_ERROR	1257
EventType: PH_APPSERVER_LICENSE_VALIDATION_ERROR	1257
EventType: PH_APPSERVER_LOGIN_ERROR	1257
EventType: PH_APPSERVER_LOG_INTEGRITY_ERROR	1257
EventType: PH_APPSERVER_MONITOR_AUDIT_PERF_ERROR	1258
EventType: PH_APPSERVER_MONITOR_HEALTH_CONFIG_SET_ERROR	1258
EventType: PH_APPSERVER_NETSEGMENT_EXPORT_ERROR	1258
EventType: PH_APPSERVER_NOTIFICATION_EMAIL_GET_RESOURCE_FAILED	1258
EventType: PH_APPSERVER_NOTIFICATION_ERROR	1258
EventType: PH_APPSERVER_NOTIFICATION_JMS_CONNECTION_ERROR	1258
EventType: PH_APPSERVER_NOTIFICATION_UPDATE_ERROR	1259
EventType: PH_APPSERVER_NOTIFIER_ERROR	1259
EventType: PH_APPSERVER_NO_WATCHLIST_SELECTED_WARN	1259
EventType: PH_APPSERVER_OPENPROXY_EXPORT_ERROR	1259

EventType: PH_APPSERVER_OUT_INTEGRATION_ERROR	1259
EventType: PH_APPSERVER_PARSER_IMPORT_ERROR	1260
EventType: PH_APPSERVER_PARSER_UPDATE_ERROR	1260
EventType: PH_APPSERVER_PARSING_CONSTRAINT_ERROR	1260
EventType: PH_APPSERVER_PDF_BUILDER_ERROR	1260
EventType: PH_APPSERVER_PERFMON_TASK_ERROR	1260
EventType: PH_APPSERVER_QUERY_CHECK_POLICY_ACTION_WARN	1260
EventType: PH_APPSERVER_QUERY_EXPORT_ERROR	1261
EventType: PH_APPSERVER_QUERY_RESULT_PARSER_ERROR	1261
EventType: PH_APPSERVER_QUERY_RESULT_RETRIEVE_ERROR	1261
EventType: PH_APPSERVER_QUERY_RUN_ERROR	1261
EventType: PH_APPSERVER_QUERY_STOP_ERROR	1261
EventType: PH_APPSERVER_QUERY_STRING_ESCAPE_ERROR	1262
EventType: PH_APPSERVER_RBAC_ERROR	1262
EventType: PH_APPSERVER_RBAC_NO_PERMISSION_WARN	1262
EventType: PH_APPSERVER_REALTIME_QUERY_ERROR	1262
EventType: PH_APPSERVER_REMEDY_ERROR	1262
EventType: PH_APPSERVER_REPORT_BUNDLE_PRINT_ERROR	1262
EventType: PH_APPSERVER_REPORT_COMPILE_ERROR	1263
EventType: PH_APPSERVER_REPORT_DEVICE_COMPONENT_SN_ERROR	1263
EventType: PH_APPSERVER_REPORT_DEVICE_DETAIL_ERROR	1263
EventType: PH_APPSERVER_REPORT_DEVICE_SN_ERROR	1263
EventType: PH_APPSERVER_REPORT_DEVICE_SUMMARY_ERROR	1263
EventType: PH_APPSERVER_REPORT_EXPORT_ERROR	1264
EventType: PH_APPSERVER_REPORT_FAILED_BLOCK_SUMMARY_ERROR	1264
EventType: PH_APPSERVER_REPORT_FIRE_TRIGGER_EVENT_ERROR	1264
EventType: PH_APPSERVER_REPORT_GET_PH_CONFIG_ERROR	1264
EventType: PH_APPSERVER_REPORT_IDENTITY_AND_LOCATION_ERROR	1264
EventType: PH_APPSERVER_REPORT_LOG_FILE_SUMMARY_ERROR	1264
EventType: PH_APPSERVER_REPORT_TEMPLATE_GENERATE_PDF_	
ERROR	1265
EventType: PH_APPSERVER_REPORT_TEMPLATE_INIT_IMAGE_ERROR	1265
EventType: PH_APPSERVER_REPORT_TEMPLATE_INIT_PARM_ERROR	1265
EventType: PH_APPSERVER_REPORT_TEMPLATE_PDF_SUMMARY_ERROR	1265
EventType: PH_APPSERVER_REPORT_TICKET_SUMMARY_ERROR	1265
EventType: PH_APPSERVER_REPORT_UPDATE_ERROR	1266
EventType: PH_APPSERVER_REPORT_USER_SUMMARY_ERROR	1266
EventType: PH_APPSERVER_REST_ERROR	1266
EventType: PH_APPSERVER_REST_H5_ERROR	1266
EventType: PH_APPSERVER_RISKSCORE_CALCULATE_ERROR	1266
EventType: PH_APPSERVER_RULE_ACTIVE_ERROR	1266
EventType: PH_APPSERVER_RULE_CLONE_ERROR	1267
EventType: PH_APPSERVER_RULE_DEBUG_INVALID_EVENT_DB_ID_	
ERROR	1267
EventType: PH_APPSERVER_RULE_DEBUG_WORKERS_SETTING_ERROR	1267
EventType: PH_APPSERVER_RULE_TEST_ERROR	1267
EventType: PH_APPSERVER_RULE_UPDATE_ERROR	1267
EventType: PH_APPSERVER_SCHEDULE_ERROR	1268
EventType: PH_APPSERVER_SCHEDULE_UPDATE_ERROR	1268

EventType: PH_APPSERVER_SECURITY_ERROR	1268
EventType: PH_APPSERVER_SERVLET_ERROR	1268
EventType: PH_APPSERVER_SERVLET_NO_ACCESS_TO_URI_WARN	1268
EventType: PH_APPSERVER_SOCKET_COMM_ERROR	1268
EventType: PH_APPSERVER SVN_ERROR	1269
EventType: PH_APPSERVER_SYNC_UPDATE_CONFIG_ERROR	1269
EventType: PH_APPSERVER_SYSCONFIG_GET_ERROR	1269
EventType: PH_APPSERVER_SYSTEM_WINAGENT_REGISTER_WARN	1269
EventType: PH_APPSERVER_SYS_APPLICATION_ERROR	1269
EventType: PH_APPSERVER_SYS_DATA_UPDATE_ERROR	1270
EventType: PH_APPSERVER_TASK_CREATE_ERROR	1270
EventType: PH_APPSERVER_TASK_FLEX_RESULT_BUILD_XML_ERROR	1270
EventType: PH_APPSERVER_TASK_GET_ERROR	1270
EventType: PH_APPSERVER_TASK_UPDATE_ERROR	1270
EventType: PH_APPSERVER_TICKET_EXPORT_ERROR	1270
EventType: PH_APPSERVER_UPDATER_FIND_EXIST_USER_BY_NOTHING_ERROR	1271
EventType: PH_APPSERVER_USERAGENT_EXPORT_ERROR	1271
EventType: PH_APPSERVER_VULNERABILITY_IGNORE_WARN	1271
EventType: PH_APPSERVER_WATCHLIST_ADD_TO_DISTIRBUTED_QUEUE	1271
EventType: PH_APPSERVER_WATCHLIST_EXPORT_ERROR	1271
EventType: PH_APPSERVER_WATCHLIST_IMPORT_ERROR	1272
EventType: PH_APPSERVER_WATCHLIST_IMPORT_WARN	1272
EventType: PH_APPSERVER_WATCHLIST_UPDATE_ERROR	1272
EventType: PH_APPSERVER_WEBSERVICE_UPDATE_TASK_ERROR	1272
EventType: PH_APPSERVER_WORKER_PROVISION_FAILED	1272
EventType: PH_APPSERVER_WS_COMM_ERROR	1272
EventType: PH_APPSERVER_XML_PARSE_ERROR	1273
EventType: PH_AUDIT_ACCOUNT_LOCKED	1273
EventType: PH_AUDIT_AGENT_DISABLED	1273
EventType: PH_AUDIT_AGENT_INSTALLED	1274
EventType: PH_AUDIT_AGENT_NOTRESPONDING	1274
EventType: PH_AUDIT_AGENT_RUNNING	1275
EventType: PH_AUDIT_AGENT_STARTED	1275
EventType: PH_AUDIT_AGENT_STOPPED	1276
EventType: PH_AUDIT_AGENT_UNINSTALLED	1276
EventType: PH_AUDIT_CASE_ASSIGNED	1277
EventType: PH_AUDIT_CASE_CLOSED	1277
EventType: PH_AUDIT_CASE_CREATED	1278
EventType: PH_AUDIT_CASE_EVIDENCE_ADDED	1278
EventType: PH_AUDIT_CASE_EVIDENCE_DELETED	1279
EventType: PH_AUDIT_CASE_INCIDENT_ADDED	1279
EventType: PH_AUDIT_CASE_MERGED	1279
EventType: PH_AUDIT_CASE_NOTE_ADDED	1280
EventType: PH_AUDIT_CASE_NOTE_DELETED	1280
EventType: PH_AUDIT_CASE_NOTE_MODIFIED	1281
EventType: PH_AUDIT_CASE_PRIORITY_CHANGED	1281
EventType: PH_AUDIT_CASE_REASSIGNED	1282
EventType: PH_AUDIT_CASE_STAGE_CHANGED	1282

EventType: PH_AUDIT_CASE_STAT	1283
EventType: PH_AUDIT_CASE_STATUS_CHANGED	1283
EventType: PH_AUDIT_CASE_SUMMARY_CHANGED	1284
EventType: PH_AUDIT_CASE_UPDATED	1284
EventType: PH_AUDIT_CI_QUOTE_EXCEEDED	1284
EventType: PH_AUDIT_CMDB_DISK_PRUNE_FAILED	1284
EventType: PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS	1285
EventType: PH_AUDIT_DASHBOARD_SHARED	1285
EventType: PH_AUDIT_DATA_PURGE	1285
EventType: PH_AUDIT_DB_LEADER_CHANGE	1286
EventType: PH_AUDIT_DEFAULT_PWD_MATCH	1286
EventType: PH_AUDIT_DEVICE_ADDED	1287
EventType: PH_AUDIT_DEVICE_DELETED	1287
EventType: PH_AUDIT_DEVICE_DISCOVERY_ITEM_CHANGED	1288
EventType: PH_AUDIT_DEVICE_MAINTENANCE_ENDED	1288
EventType: PH_AUDIT_DEVICE_MAINTENANCE_STARTED	1289
EventType: PH_AUDIT_DEVICE_MERGED_BY_IP_WITH_DIFF_NAME	1289
EventType: PH_AUDIT_DEVICE_STATUS_CHANGED	1290
EventType: PH_AUDIT_DEVICE_UNMANAGED	1290
EventType: PH_AUDIT_DEV_MON_JOB_NOT_STARTED	1291
EventType: PH_AUDIT_DEV_MON_JOB_STATUS_CHANGE	1291
EventType: PH_AUDIT_DISCOVERY	1291
EventType: PH_AUDIT_EXPORT_REPORT_END	1292
EventType: PH_AUDIT_GENAI_USER_QUERY	1292
EventType: PH_AUDIT_GENERIC	1292
EventType: PH_AUDIT_GROUP_CREATED	1292
EventType: PH_AUDIT_GROUP_DELETED	1293
EventType: PH_AUDIT_INACTIVE_USER_LOGIN	1293
EventType: PH_AUDIT_INCIDENT_SYS_CLEAR	1293
EventType: PH_AUDIT_INCIDENT_USER_CLEAR	1294
EventType: PH_AUDIT_INTEGRATION_POLICY_EXECUTED	1294
EventType: PH_AUDIT_MALWARE_DATA_DELETED	1294
EventType: PH_AUDIT_MALWARE_DATA_UPDATED	1295
EventType: PH_AUDIT_ML_GENERIC_ERROR	1295
EventType: PH_AUDIT_ML_GENERIC_INFO	1296
EventType: PH_AUDIT_ML_INFERENCE_COMPLETED	1296
EventType: PH_AUDIT_ML_INFERENCE_RESULT	1296
EventType: PH_AUDIT_ML_INFERENCE_STARTED	1296
EventType: PH_AUDIT_ML_TRAINING_COMPLETED	1296
EventType: PH_AUDIT_ML_TRAINING_STARTED	1296
EventType: PH_AUDIT_NOTIF_POLICY_EXECUTED	1297
EventType: PH_AUDIT_OBJECT_CREATED	1297
EventType: PH_AUDIT_OBJECT_DELETED	1297
EventType: PH_AUDIT_OBJECT_UPDATED	1298
EventType: PH_AUDIT_ONDEMAND_REMEDIATION_EXECUTED	1298
EventType: PH_AUDIT_PASSWORD_CHANGED	1299
EventType: PH_AUDIT_QUERY_COMPLETED	1299
EventType: PH_AUDIT_QUERY_SCHEDULED	1300
EventType: PH_AUDIT_QUERY_START	1300

EventType: PH_AUDIT_QUERY_STOP	1300
EventType: PH_AUDIT_REPL_LEADER_CHANGE	1301
EventType: PH_AUDIT_REPORT_SCHEDULED	1301
EventType: PH_AUDIT_REPORT_SCHEDULE_APPROVE	1301
EventType: PH_AUDIT_REPORT_SCHEDULE_REQUEST	1302
EventType: PH_AUDIT_REPORT_SERVER_LICENSE_EXPIRED	1302
EventType: PH_AUDIT_REPORT_SERVER_LICENSE_REMOVED	1303
EventType: PH_AUDIT_REPORT_SERVER_LICENSE_TO_EXPIRE	1303
EventType: PH_AUDIT_RISK_DECREASE_LOW	1303
EventType: PH_AUDIT_RISK_DECREASE_MED	1303
EventType: PH_AUDIT_RISK_INCREASE_HIGH	1303
EventType: PH_AUDIT_RISK_INCREASE_MED	1303
EventType: PH_AUDIT_RULE_ACTIVATED	1304
EventType: PH_AUDIT_RULE_ACTIVATION_APPROVE	1304
EventType: PH_AUDIT_RULE_ACTIVATION_REQUEST	1304
EventType: PH_AUDIT_RULE_DEACTIVATED	1305
EventType: PH_AUDIT_RULE_DEACTIVATION_APPROVE	1305
EventType: PH_AUDIT_RULE_DEACTIVATION_REQUEST	1306
EventType: PH_AUDIT_SVC_LOGIN_FAILURE	1306
EventType: PH_AUDIT_SVC_LOGIN_SUCCESS	1306
EventType: PH_AUDIT_SVC_LOGOFF	1307
EventType: PH_AUDIT_SVC_SESSION_TIMEOUT	1307
EventType: PH_AUDIT_TUNNEL_CLOSE	1307
EventType: PH_AUDIT_TUNNEL_OPEN	1308
EventType: PH_AUDIT_USER_ADDED	1308
EventType: PH_AUDIT_USER_CHANGE_ORG_SCOPE	1309
EventType: PH_AUDIT_USER_DEFAULT_ROLE_CHANGED	1309
EventType: PH_AUDIT_USER_DELETED	1310
EventType: PH_AUDIT_USER_LOGIN_FAILURE	1310
EventType: PH_AUDIT_USER_LOGIN_SUCCESS	1310
EventType: PH_AUDIT_USER_LOGOFF	1311
EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_CHANGED	1311
EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_ENABLED	1312
EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_REMOVED	1312
EventType: PH_AUDIT_USER_SESSION_TIMEOUT	1312
EventType: PH_AUDIT_WS_COMM	1313
EventType: PH_BAD_NETFLOW_PACKET	1313
EventType: PH_BAD_NETFLOW_VER	1313
EventType: PH_BAD_ROUTE_OUTPUT	1313
EventType: PH_BASE_PROC_BASE_AGENT_JOB_NO_THREAD_NUM_	
ASSIGNED	1313
EventType: PH_BASE_PROC_DUMP_STACK_TRACE_FAILURE	1313
EventType: PH_BASE_PROC_GET_PID_FILE_FAILED	1314
EventType: PH_BASE_PROC_HANDLE_NOTIFICATION_ERROR	1314
EventType: PH_BASE_PROC_KILL_PROC_ERROR	1314
EventType: PH_BASE_PROC_NOTIFICATION_HANDLE_CONN_ERROR	1315
EventType: PH_BASE_PROC_NO_CONN_TO_HEARTBEAT_SERVER	1315
EventType: PH_BASE_PROC_RENAME_MINI_DUMP_FILE_FAILURE	1315
EventType: PH_BASE_PROC_REST_CACHE_CHECKOUT_STATUS_	
	1315

WARNING	
EventType: PH_BASE_PROC_SEND_HEARTBEAT_FAILURE	1315
EventType: PH_BASE_PROC_SEND_USER_DEFINED_SIG_FAILED	1316
EventType: PH_BASE_PROC_SET_PID_FILE_FAILED	1316
EventType: PH_BASE_PROC_STACK_TRACE	1316
EventType: PH_BASE_PROC_STACK_TRACK_TOO_LONG	1316
EventType: PH_BASE_PROC_SYS_INFO_CALC_CPU_ERROR	1317
EventType: PH_BASE_PROC_SYS_PROC_INFO_GET_FAILURE	1317
EventType: PH_BASE_PROC_SYS_PROC_INFO_INIT_ERROR	1317
EventType: PH_BASE_PROC_SYS_PROC_INFO_UNABLE_OPEN_PROC_PID_FILE	1317
EventType: PH_BASE_PROC_SYS_PROC_INFO_UNABLE_OPEN_PROC_STAT_FILE	1318
EventType: PH_BASE_PROC_THREAD_SPAWN_FAILED	1318
EventType: PH_BASE_PROC_THREAD_WRONG_PARAM	1318
EventType: PH_BASE_PROC_UPLOAD_FILE_FAILURE	1318
EventType: PH_BASE_PROC_VALUE_GROUP_UPDATE_FAILURE	1319
EventType: PH_BASE_PRO_AQUIRE_SHARED_STORE_FAILED	1319
EventType: PH_CHECKPOINT_CERTHANDLER_ERROR	1319
EventType: PH_CHECKPOINT_CERTPULL_ERROR	1319
EventType: PH_CHECKPOINT_CMD_USAGE_ERROR	1320
EventType: PH_CHECKPOINT_CPMI_FETCH_ERROR	1320
EventType: PH_CHECKPOINT_DEV_INIT_ERROR	1321
EventType: PH_CHECKPOINT_FILE_RENAME_FAILURE	1321
EventType: PH_CHECKPOINT_FWLOGHANDLER_ERROR	1321
EventType: PH_CHECKPOINT_FWLOGHANDLER_INIT_ERROR	1322
EventType: PH_CHECKPOINT_HTTP_ERROR	1322
EventType: PH_CHECKPOINT_LOGHANDLER_ERROR	1322
EventType: PH_CHECKPOINT_PROCESS_GET_FAILED	1323
EventType: PH_CHECKPOINT_TESTCONN_ERROR	1323
EventType: PH_CHECKPOINT_UNABLE_PARSE_XML	1323
EventType: PH_CLICKHOUSE_CHECKIN_QUERY_THREADS_FAILED	1323
EventType: PH_CLICKHOUSE_CHECKOUT_QUERY_THREADS_FAILED	1324
EventType: PH_CLICKHOUSE_DISK_UTILS_PER_STORAGE_TIER	1324
EventType: PH_CLICKHOUSE_DROP_PARTITION_FAILED	1324
EventType: PH_CLICKHOUSE_DROP_PARTITION_STARTED	1325
EventType: PH_CLICKHOUSE_DROP_PARTITION_SUCCEEDED	1325
All Logs Page 2	1327
EventType: PH_CLICKHOUSE_GET_ONLINE_NODE_FAILED	1340
EventType: PH_CLICKHOUSE_GET_PARTITIONS_FAILED	1340
EventType: PH_CLICKHOUSE_GET_SHARDS_FAILED	1340
EventType: PH_CLICKHOUSE_GET_STORAGE_STATS_FAILED	1341
EventType: PH_CLICKHOUSE_GET_STORAGE_TIER_FAILED	1341
EventType: PH_CLICKHOUSE_INSERTION_DROP_EVENTS	1341
EventType: PH_CLICKHOUSE_INSERTION_EPS	1342
EventType: PH_CLICKHOUSE_JSON_ENCODER_EPS	1342
EventType: PH_CLICKHOUSE_JSON_ENCODER_EPS_PER_THREAD	1342
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_ACTIVE_CONSOLIDATION	1342
EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CALCULATE_REQUEST	1343

PARSE_FAILED	
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_CALCULATE_REQUEST_	
STARTED	1343
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_CANDIDATE_PARTITIONS	1343
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_CONSOLIDATION_DATE	1343
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_CONSOLIDATION_STATUS_	
CHANGE	1343
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_	
DONE	1344
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_	
STARTED	1344
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_	
STOPPED	1344
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_	
TIMER	1345
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_DB_QUERY_FAILED	1345
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_EMPTY_PARTITION_	
CHECKSUM	1345
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_EXEC_FAILED	1345
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_MIN_MAX_QUERY_FAILED	1346
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_OPTIMIZE_COMMAND_	
FAILED	1346
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_	
CONSOLIDATION_DONE	1347
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_	
CONSOLIDATION_STARTED	1347
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_UPDATED_	
AFTER_CHECKSUM	1348
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_MISMATCH	1348
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_MISMATCH_	
REPLICAS	1349
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_PARTITION_INFO_	
EMPTY	1349
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_REQUEST_	
PARSE_FAILED	1350
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_	
EMPTY	1350
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_	
ERROR	1350
Event Type: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_	
PARSE_FAILED	1350
Event Type: PH_CLICKHOUSE_MOVE_PARTITION_FAILED	1351
Event Type: PH_CLICKHOUSE_MOVE_PARTITION_STARTED	1351
Event Type: PH_CLICKHOUSE_MOVE_PARTITION_SUCCEEDED	1351
Event Type: PH_CLICKHOUSE_NOT_REACHABLE	1352
Event Type: PH_CLICKHOUSE_QUERY_REDIS_CONN_FAILURE	1352
Event Type: PH_CLICKHOUSE_QUERY_REDIS_GET_FAILURE	1352
Event Type: PH_CLICKHOUSE_QUERY_UNCOMPRESS_FAILURE	1353
Event Type: PH_CLICKHOUSE_QUERY_ZLIB_INIT_FAILURE	1353

EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_QUERY_CHECKIN	1353
EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_QUERY_CHECKOUT	1353
EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_THREADS_CHECKIN	1354
EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_THREADS_CHECKOUT	1354
EventType: PH_CLICKHOUSE_ROUND_ROBIN_INSERTION	1355
EventType: PH_CLICKHOUSE_ROUND_ROBIN_QUERY	1355
EventType: PH_CLICKHOUSE_STORAGE_FREE_SPACE_CRITICAL	1355
EventType: PH_CLICKHOUSE_STORAGE_FREE_SPACE_LOW	1356
EventType: PH_CLICKHOUSE_STORAGE_UTILS_PER_ORG_PER_DAY	1356
EventType: PH_CLICKHOUSE_WRITE_FAILED	1356
EventType: PH_CLICKHOUSE_BUILD_QUERY_DIST_SQL_COMMAND_FAILURE	1357
EventType: PH_CLI_ERROR	1357
EventType: PH_CLUSTER_COLLECT_ALL_IP_FAILED	1357
EventType: PH_CLUSTER_COLLECT_CONFIG_DATA_FAILED	1357
EventType: PH_CLUSTER_CONFIG_SSH_KEY_FAILED	1357
EventType: PH_CLUSTER_GET_FW_IP_FAILED	1358
EventType: PH_CLUSTER_GET_TASK_FAILED	1358
EventType: PH_CLUSTER_NOT_SUPPORT_TASK	1358
EventType: PH_CLUSTER_NOT_VALID_FELLOWER	1358
EventType: PH_CLUSTER_NO_LICENSE	1359
EventType: PH_CLUSTER_RELOAD_CONFIG_FAILED	1359
EventType: PH_CLUSTER_RM_DB_FAILED	1359
EventType: PH_CLUSTER_RUN_COMMAND_FAILED	1359
EventType: PH_CLUSTER_SCRIPT_FAILED	1359
EventType: PH_CLUSTER_SEND_TASK_FAILED	1360
EventType: PH_CLUSTER_SSH_KEY_IS_WRONG	1360
EventType: PH_CLUSTER_TASK_DATA_EMPTY	1360
EventType: PH_CLUSTER_TASK_INFO_IS_WRONG	1360
EventType: PH_CLUSTER_TASK_NOT_CONTAIN_LIC	1360
EventType: PH_CLUSTER_UPDATE_CONFIG_ERROR	1361
EventType: PH_COLLECTOR_CLOCK_SKEW	1361
EventType: PH_COLLECTOR_DOWN	1362
EventType: PH_COLLECTOR_EVENT_ARRIVAL_DELAYED	1362
EventType: PH_COLLECTOR_EVENT_ARRIVAL_OK	1362
EventType: PH_COLLECTOR_EVENT_STORE_DELAYED	1362
EventType: PH_COLLECTOR_EVENT_STORE_OK	1362
EventType: PH_COLLECTOR_LICENSE_UPDATE	1362
EventType: PH_COLLECTOR_UP	1363
EventType: PH_CREATE_TEMP_FILE_FAILURE	1363
EventType: PH_CYBERARK_INIT_ERROR	1363
EventType: PH_DATAINTEGRITY_PASSPHRASE_LOAD_ERROR	1363
EventType: PH_DATAINTEGRITY_SIGNER_ERROR	1364
EventType: PH_DATAINTEGRITY_UTILS_ERROR	1364
EventType: PH_DATAINTEGRITY_VERIFIER_ERROR	1364
EventType: PH_DATAMANAGER_CLICKHOUSE_HTTP_UPLOAD_ERROR	1365
EventType: PH_DATAMANAGER_CLUSTER_ENCODE_ERROR	1365
EventType: PH_DATAMANAGER_CLUSTER_INIT_ERROR	1365

EventType: PH_DATAMANAGER_CLUSTER_WAIT_ERROR	1366
EventType: PH_DATAMANAGER_CLUSTER_WRITER_ERROR	1366
EventType: PH_DATAMANAGER_DASHBOARD_RESPONSE_ERROR	1366
EventType: PH_DATAMANAGER_ELASTICWRITER_ERROR	1367
EventType: PH_DATAMANAGER_EVTATTR_ERROR	1367
EventType: PH_DATAMANAGER_EVTCACHE_DUPLICATE_ERROR	1367
EventType: PH_DATAMANAGER_EVTCACHE_GET_ERROR	1367
EventType: PH_DATAMANAGER_EVTCACHE_PARSE_ERROR	1368
EventType: PH_DATAMANAGER_EVTDBNOTIFIER_ERROR	1368
EventType: PH_DATAMANAGER_EVTIDX_CORRUPT_ERROR	1368
EventType: PH_DATAMANAGER_EVTIDX_MERGE_ERROR	1369
EventType: PH_DATAMANAGER_EVTIDX_QUERY_ERROR	1369
EventType: PH_DATAMANAGER_EVTIDX_READ_BLOCK_ERROR	1369
EventType: PH_DATAMANAGER_EVTIDX_READ_KEY_ERROR	1370
EventType: PH_DATAMANAGER_EVTIDX_READ_POST_ERROR	1370
EventType: PH_DATAMANAGER_EVTIDX_WRITE_ERROR	1370
EventType: PH_DATAMANAGER_EVTIDX_WRITE_KEY_ERROR	1371
EventType: PH_DATAMANAGER_EVTIDX_WRITE_POST_ERROR	1371
EventType: PH_DATAMANAGER_EVTLOADER_ERROR	1371
EventType: PH_DATAMANAGER_EVTWRITER_ERROR	1372
EventType: PH_DATAMANAGER_EXPORT_ERROR	1372
EventType: PH_DATAMANAGER_FILE_READ_FAILURE	1372
EventType: PH_DATAMANAGER_FILE_RENAME_FAILURE	1373
EventType: PH_DATAMANAGER_FILE_SIGN_ERROR	1373
EventType: PH_DATAMANAGER_FILE_WRITE_FAILURE	1373
EventType: PH_DATAMANAGER_GET_SIGN_ERROR	1374
EventType: PH_DATAMANAGER_GLOBAL_CACHE_MISSING	1374
EventType: PH_DATAMANAGER_HDFSWRITER_ERROR	1374
EventType: PH_DATAMANAGER_HTTP_UPLOAD_ERROR	1374
EventType: PH_DATAMANAGER_INIT_ERROR	1375
EventType: PH_DATAMANAGER_INTEGRITY_CHECK_ERROR	1375
EventType: PH_DATAMANAGER_INTEGRITY_RESPONSE_ERROR	1375
EventType: PH_DATAMANAGER_INVALID_LOG_FILE	1376
EventType: PH_DATAMANAGER_IP_TYPE_INVALID	1376
EventType: PH_DATAMANAGER_KAFKAWRITER_CONFIG_ERROR	1376
EventType: PH_DATAMANAGER_KAFKAWRITER_ERROR	1377
EventType: PH_DATAMANAGER_LOG_BUFFER_PAUSED_LOW_SPACE	1377
EventType: PH_DATAMANAGER_LOG_BUFFER_PAUSED_STATFS_FAILURE	1377
EventType: PH_DATAMANAGER_LOG_BUFFER_RESUMED	1377
EventType: PH_DATAMANAGER_PUT_SIGN_ERROR	1377
EventType: PH_DATAMANAGER_QUERY_EXPR_ERROR	1378
EventType: PH_DATAMANAGER_QUERY_RESPONSE_ERROR	1378
EventType: PH_DATAMANAGER_REDIS_KEY_NOT_EXIST	1378
EventType: PH_DATAMANAGER_SUMMARYWRITER_ERROR	1379
EventType: PH_DATAMGR_BAD_EVTBLKIDX_FILE	1379
EventType: PH_DATAMGR_BAD_SEGMENT	1379
EventType: PH_DATAMGR_INDEX_MERGE_FAILED	1379
EventType: PH_DATAMGR_INDEX_MERGE_FAILED_INDEX	1379
EventType: PH_DATAMGR_INDEX_MERGE_FAILED_INDEX_GROUP	1380

EventType: PH_DATAMGR_SEGMENT_MERGE_ERROR	1380
EventType: PH_DATAMGR_SEGMENT_MERGE_FAILED	1380
EventType: PH_DATAMGR_UNABLE_FLUSH_INDEX	1380
EventType: PH_DATAMGR_UNABLE_OPEN_EVTBLK_FILE	1380
EventType: PH_DATAPURGER_ARCHIVE_TASK_ERROR	1381
EventType: PH_DATAPURGER_CMD_FAILURE	1381
EventType: PH_DATAPURGER_DR_ES_RESTORE_FAILED	1381
EventType: PH_DATAPURGER_DR_ES_ROLE_UNKNOWN	1382
EventType: PH_DATAPURGER_DR_ES_SNAPSHOTS_GET_FAILED	1382
EventType: PH_DATAPURGER_DR_ES_SNAPSHOT_DELETION_FAILED	1382
EventType: PH_DATAPURGER_DR_ES_SNAPSHOT_FAILED	1382
EventType: PH_DATAPURGER_DUCHECKER_ERROR	1383
EventType: PH_DATAPURGER_ENFORCE_ERROR	1383
EventType: PH_DATAPURGER_EVAL_ERROR	1383
EventType: PH_DATAPURGER_HTTP_UPLOAD_ERROR	1384
EventType: PH_DATAPURGER_INIT_ERROR	1384
EventType: PH_DATAPURGER_OPEN_FILE_ERROR	1384
EventType: PH_DATAPURGER_PARSE_XML_ERROR	1385
EventType: PH_DATAPURGER_POLICY_ERROR	1385
EventType: PH_DATAPURGER_RESPONSE_ERROR	1385
EventType: PH_DATAPURGER_STORAGE_POLICY_CLICKHOUSE_NODES_EMPTY	1385
EventType: PH_DATA_CLUSTER_ALL_COORDINATOR_DOWN	1386
EventType: PH_DATA_CLUSTER_BUSY	1386
EventType: PH_DATA_CLUSTER_CLICKHOUSE_CONFIG_NO_PORT	1386
EventType: PH_DATA_CLUSTER_COORDINATOR_DOWN	1387
EventType: PH_DATA_CLUSTER_COORDINATOR_UP	1387
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_HTTPPORT	1387
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_IP	1387
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_JAVAPORT	1388
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NAME	1388
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NUMREPLICAS	1388
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NUMSHARD	1388
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NULL	1388
EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_WRONG_FORMAT	1389
EventType: PH_DATA_CLUSTER_ELASTIC_EVENTID_NOT_FOUND	1389
EventType: PH_DATA_CLUSTER_ELASTIC_HTTP_CLIENT_FAIL	1389
EventType: PH_DATA_CLUSTER_ELASTIC_HTTP_CMD_FAIL	1389
EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_FAIL	1390
EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_RESEND_FAIL	1390
EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FAIL	1390
EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FIRST_FAIL	1391
EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_UPLOAD_FAIL	1391
EventType: PH_DATA_CLUSTER_ELASTIC_WRONG_JSON_FORMAT	1391
EventType: PH_DATA_CLUSTER_GET_HOSTNAME_FAIL	1392
EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_PORT	1392
EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_SERVER	1392
EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_YARN_PORT	1392
EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_YARN_SERVER	1392

EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NULL	1392
EventType: PH_DATA_CLUSTER_HDFS_HTTP_CMD_FAIL	1393
EventType: PH_DATA_CLUSTER_HDFS_LISTSTATUS_FAIL	1393
EventType: PH_DATA_CLUSTER_HDFS_SEND_FAIL	1393
EventType: PH_DATA_CLUSTER_HDFS_UPLOAD_FAIL	1394
EventType: PH_DATA_CLUSTER_JSON_GET_ATTRIBUTE_NAME_FAIL	1394
EventType: PH_DEVICE_NOT_ADDED	1394
EventType: PH_DEV_FAIL_TO_PULL_EVENTS	1394
EventType: PH_DEV_MON_ACME_PACKET_SESSION_AGENT_STATUS	1395
EventType: PH_DEV_MON_ACME_PACKET_SYS_STATUS	1395
EventType: PH_DEV_MON_APP_APACHE_MET	1397
EventType: PH_DEV_MON_APP_ASPNET_MET	1398
EventType: PH_DEV_MON_APP_DHCP_MET	1398
EventType: PH_DEV_MON_APP_DNS_MET	1399
EventType: PH_DEV_MON_APP_ICA_SESS_MET	1400
EventType: PH_DEV_MON_APP_IIS_MET	1401
EventType: PH_DEV_MON_APP_MSEXCH_ERR_MET	1402
EventType: PH_DEV_MON_APP_MSEXCH_ISDB_INST_MET	1403
EventType: PH_DEV_MON_APP_MSEXCH_ISDB_MET	1404
EventType: PH_DEV_MON_APP_MSEXCH_MBOX_MET	1405
EventType: PH_DEV_MON_APP_MSEXCH_MET	1406
EventType: PH_DEV_MON_APP_MSEXCH_REPL_MET	1407
EventType: PH_DEV_MON_APP_MSEXCH_SMTP_MET	1407
EventType: PH_DEV_MON_APP_MSEXCH_STORE_INTF_MET	1408
EventType: PH_DEV_MON_APP_MSEXCH_SUBMIT_MET	1409
EventType: PH_DEV_MON_APP_MSEXCH_TRANS_MET	1410
EventType: PH_DEV_MON_APP_MSEXCH_WS_MET	1411
EventType: PH_DEV_MON_APP_NTDS_MET	1411
EventType: PH_DEV_MON_ARUBA_WLAN_RADIO_METRIC	1412
EventType: PH_DEV_MON_AUTH_STATS	1413
EventType: PH_DEV_MON_AUTO_SVC_START_TO_STOP	1414
EventType: PH_DEV_MON_AUTO_SVC_STOP	1415
EventType: PH_DEV_MON_AUTO_SVC_STOP_TO_START	1415
EventType: PH_DEV_MON_BC_PROXY_METRIC	1416
EventType: PH_DEV_MON_BGP_NBR_STATUS	1417
EventType: PH_DEV_MON_BOX_FILE_CREATE	1417
EventType: PH_DEV_MON_BOX_FILE_DELETE	1418
EventType: PH_DEV_MON_BOX_FILE_MODIFY	1419
EventType: PH_DEV_MON_BOX_FILE_SHARE	1420
EventType: PH_DEV_MON_CBQOS_CMSTAT	1420
EventType: PH_DEV_MON_CBQOS_POLICESTAT	1421
EventType: PH_DEV_MON_CBQOS_QUEUESTAT	1422
EventType: PH_DEV_MON_CCM_CTI_STAT	1423
EventType: PH_DEV_MON_CCM_CTI_STAT_CHANGE	1423
EventType: PH_DEV_MON_CCM_DEL_CTI	1424
EventType: PH_DEV_MON_CCM_DEL_GW	1424
EventType: PH_DEV_MON_CCM_DEL_H323	1425
EventType: PH_DEV_MON_CCM_DEL_MEDIA	1425
EventType: PH_DEV_MON_CCM_DEL_SIP_TRUNK	1426

EventType: PH_DEV_MON_CCM_DEL_VM	1426
EventType: PH_DEV_MON_CCM_GLOBAL_INFO	1427
EventType: PH_DEV_MON_CCM_GW_STAT	1428
EventType: PH_DEV_MON_CCM_GW_STAT_CHANGE	1428
EventType: PH_DEV_MON_CCM_H323_STAT	1429
EventType: PH_DEV_MON_CCM_H323_STAT_CHANGE	1430
EventType: PH_DEV_MON_CCM_MEDIA_STAT	1430
EventType: PH_DEV_MON_CCM_MEDIA_STAT_CHANGE	1431
EventType: PH_DEV_MON_CCM_NEW_CTI	1431
EventType: PH_DEV_MON_CCM_NEW_GW	1432
EventType: PH_DEV_MON_CCM_NEW_H323	1432
EventType: PH_DEV_MON_CCM_NEW_MEDIA	1433
EventType: PH_DEV_MON_CCM_NEW_SIP_TRUNK	1433
EventType: PH_DEV_MON_CCM_NEW_VM	1434
EventType: PH_DEV_MON_CCM_SIP_TRUNK_STAT	1434
EventType: PH_DEV_MON_CCM_VM_STAT	1435
EventType: PH_DEV_MON_CCM_VM_STAT_CHANGE	1436
EventType: PH_DEV_MON_CHANGE_CUST_CONFIG	1437
EventType: PH_DEV_MON_CHANGE_INST_SW	1437
EventType: PH_DEV_MON_CHANGE_RUN_CONFIG	1438
EventType: PH_DEV_MON_CHANGE_RUN_SW	1438
EventType: PH_DEV_MON_CHANGE_STARTUP_CONFIG	1438
EventType: PH_DEV_MON_CISCO_NBAR_STAT	1439
EventType: PH_DEV_MON_CISCO_RAS_VPN_MET	1440
EventType: PH_DEV_MON_CISCO_VPN_P1_TUNNEL_MET	1441
EventType: PH_DEV_MON_CISCO_VPN_P2_TUNNEL_MET	1442
EventType: PH_DEV_MON_CISCO_WLAN_RADIO_METRIC	1443
EventType: PH_DEV_MON_CITRIX_SDWAN_INTF	1444
EventType: PH_DEV_MON_CITRIX_SDWAN_LINK	1445
EventType: PH_DEV_MON_CLARION_ARRAY_UTIL	1446
EventType: PH_DEV_MON_CLARION_DISK_HEALTH	1447
EventType: PH_DEV_MON_CLARION_HOST_CONN	1447
EventType: PH_DEV_MON_CLARION_LUN_UTIL	1448
EventType: PH_DEV_MON_CLARION_PER_HOST_LUN_UTIL	1449
EventType: PH_DEV_MON_CLARION_PORT_UTIL	1450
EventType: PH_DEV_MON_CLARION_RG_UTIL	1451
EventType: PH_DEV_MON_CLARION_SP_UTIL	1452
EventType: PH_DEV_MON_CLARION_STORAGE_USAGE	1453
EventType: PH_DEV_MON_CLARION_STORE_POOL_UTIL	1453
EventType: PH_DEV_MON_CLARION_UNREG_HOST	1454
EventType: PH_DEV_MON_CLOUD_SERVICE_HEARTBEAT	1454
EventType: PH_DEV_MON_CMDB_DISK_PRUNE_FAILED	1455
EventType: PH_DEV_MON_CMDB_DISK_PRUNE_SUCCESS	1455
EventType: PH_DEV_MON_CUST_FILE_CHANGE_ATTRIB	1455
EventType: PH_DEV_MON_CUST_FILE_CHANGE_CONTENT	1456
EventType: PH_DEV_MON_CUST_FILE_CREATE	1456
EventType: PH_DEV_MON_CUST_FILE_DELETE	1456
EventType: PH_DEV_MON_CUST_FILE_SCAN	1456
EventType: PH_DEV_MON_CUST_TARGET_FILE_CHANGE	1456

EventType: PH_DEV_MON_DATASTORE_UTIL	1456
EventType: PH_DEV_MON_DC DIAG	1457
EventType: PH_DEV_MON_DD NS_UPDATE_STAT	1457
EventType: PH_DEV_MON_DELLFORCE10_EXT_INTF_UTIL	1457
EventType: PH_DEV_MON_DELL_BLADE_POWER_STATUS	1458
EventType: PH_DEV_MON_DELL_BLADE_P SU_STATUS	1459
EventType: PH_DEV_MON_DELTA_CONFIG	1459
EventType: PH_DEV_MON_DGA_DETECTED	1460
EventType: PH_DEV_MON_DHCP_SUBNET_USAGE	1461
EventType: PH_DEV_MON_DISK_IO_UTIL	1461
EventType: PH_DEV_MON_DISK_MON_SKIP	1462
EventType: PH_DEV_MON_DNS_CLUST_REPL_STAT	1462
EventType: PH_DEV_MON_DNS_PERF_STAT	1463
EventType: PH_DEV_MON_DNS_ZONETX_MET	1464
EventType: PH_DEV_MON_DST_AD_REPL_STAT	1464
EventType: PH_DEV_MON_EBS_METRIC	1465
EventType: PH_DEV_MON_EC2_INSTANCE_DOWN	1465
EventType: PH_DEV_MON_EC2_INSTANCE_UP	1466
EventType: PH_DEV_MON_EC2_METRIC	1466
EventType: PH_DEV_MON EMC_DATADOMAIN_DISK_PERF	1467
EventType: PH_DEV_MON EMC_DATADOMAIN_OVERALL_PERF	1468
EventType: PH_DEV_MON_EQL_CONN_MET	1469
EventType: PH_DEV_MON_EQL_DISK_HEALTH	1469
EventType: PH_DEV_MON_EQL_DISK_MET	1470
EventType: PH_DEV_MON_EQL_GROUP_MET	1470
EventType: PH_DEV_MON_ESX_DATASTORE_IO	1471
EventType: PH_DEV_MON_ESX_DISK_IO	1471
EventType: PH_DEV_MON_ESX_DISK_UTIL	1471
EventType: PH_DEV_MON_ESX_STATE	1472
EventType: PH_DEV_MON_ESX_UPTIME	1472
EventType: PH_DEV_MON_EUM_FAIL	1472
EventType: PH_DEV_MON_EUM_INTERNAL_ERR	1473
EventType: PH_DEV_MON_EUM_STATUS	1474
EventType: PH_DEV_MON_EUM_SUCCESS	1475
EventType: PH_DEV_MON_F5_ACTIVE_CONN	1476
EventType: PH_DEV_MON_F5_LTM_NODE_STAT	1477
EventType: PH_DEV_MON_F5_LTM_POOL_MEMBER_STAT	1478
EventType: PH_DEV_MON_F5_LTM_POOL_STAT	1480
EventType: PH_DEV_MON_F5_LTM_VIRT_ADDR_STAT	1482
EventType: PH_DEV_MON_F5_LTM_VIRT_SERVER_STAT	1483
EventType: PH_DEV_MON_F5_NEW_CONN	1485
EventType: PH_DEV_MON_F5_RAM_CACHE	1486
EventType: PH_DEV_MON_F5_THROUGHPUT	1486
EventType: PH_DEV_MON_F5_TMM_MEM_UTIL	1487
EventType: PH_DEV_MON_FGT_SEC_POSTURE_DETAILS	1488
EventType: PH_DEV_MON_FGT_SEC_POSTURE_DETECTED_ENDPOINTS	1488
EventType: PH_DEV_MON_FGT_SEC_POSTURE_FABRIC_GRADE	1489
EventType: PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_GRADE	1489
EventType: PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_STATS	1490

EventType: PH_DEV_MON_FGT_SEC_POSTURE_PER_DEVICE_STATS	1491
EventType: PH_DEV_MON_FGT_USER_INFO	1491
EventType: PH_DEV_MON_FILE_CONTENT_CHANGE	1493
EventType: PH_DEV_MON_FIREAMP_DISCOVERY_CLIENT_APP	1493
EventType: PH_DEV_MON_FIREAMP_DISCOVERY_NETWORK_PROTOCOL	1494
EventType: PH_DEV_MON_FIREAMP_DISCOVERY_OS_FINGERPRINT	1494
EventType: PH_DEV_MON_FIREAMP_DISCOVERY_SERVER	1495
EventType: PH_DEV_MON_FIREAMP_FILE	1495
EventType: PH_DEV_MON_FIREAMP_IMPACT_FLAG	1497
EventType: PH_DEV_MON_FIREAMP_INTRUSION	1498
EventType: PH_DEV_MON_FIREAMP_MALWARE	1500
EventType: PH_DEV_MON_FIREAMP_USER_LOGIN	1502
EventType: PH_DEV_MON_FORTIAP_INTF_UTIL	1503
EventType: PH_DEV_MON_FORTIAP_PERF	1503
EventType: PH_DEV_MON_FORTIAP_STAT	1503
EventType: PH_DEV_MON_FORTIGATE_INTF_UTIL	1504
EventType: PH_DEV_MON_FORTIGATE_PERF	1504
EventType: PH_DEV_MON_FORTIMAIL_SESSION_COUNT	1505
EventType: PH_DEV_MON_FORTIMAIL_SYS_LOAD	1505
EventType: PH_DEV_MON_FORTINET_PROCESSOR_USAGE	1505
EventType: PH_DEV_MON_FORTINET_QOS	1506
EventType: PH_DEV_MON_FORTISWITCH_PERF	1507
EventType: PH_DEV_MON_FORTIWLC_QOS_STAT	1507
EventType: PH_DEV_MON_FORTIWLC_STATIONS	1508
EventType: PH_DEV_MON_FORTIWLC_SYS_THRUPUT	1509
EventType: PH_DEV_MON_FPC_LIEBERT_METRIC	1509
EventType: PH_DEV_MON_FW_CONN_UTIL	1511
EventType: PH_DEV_MON_GITHUB_BRANCH_EVENT	1511
EventType: PH_DEV_MON_GITHUB_COMMIT	1512
EventType: PH_DEV_MON_GITHUB_EVENT	1513
EventType: PH_DEV_MON_GITHUB_FORK_REPOSITORY_EVENT	1514
EventType: PH_DEV_MON_GITHUB_ISSUE_EVENT	1515
EventType: PH_DEV_MON_GITHUB_MEMBER_EVENT	1516
EventType: PH_DEV_MON_GITHUB_ORG_EVENT	1517
EventType: PH_DEV_MON_GITHUB_PROJECT_EVENT	1518
EventType: PH_DEV_MON_GITHUB_PULL_REQUEST_EVENT	1519
EventType: PH_DEV_MON_GITHUB_PULL_REQUEST_REVIEW_EVENT	1520
EventType: PH_DEV_MON_GITHUB_REPOSITORY_EVENT	1521
EventType: PH_DEV_MON_GITHUB_TAG_EVENT	1522
EventType: PH_DEV_MON_GLASSFISH_APP	1523
EventType: PH_DEV_MON_GLASSFISH_CONN_STAT	1524
EventType: PH_DEV_MON_GLASSFISH_CPU	1524
EventType: PH_DEV_MON_GLASSFISH_DB_POOL	1524
EventType: PH_DEV_MON_GLASSFISH_EJB	1524
EventType: PH_DEV_MON_GLASSFISH_JMS	1524
EventType: PH_DEV_MON_GLASSFISH_MEMORY	1524
EventType: PH_DEV_MON_GLASSFISH_REQUEST_PROCESSOR	1525
EventType: PH_DEV_MON_GLASSFISH_SERVLET	1525
EventType: PH_DEV_MON_GLASSFISH_SESSION	1525

EventType: PH_DEV_MON_GLASSFISH_THREAD_POOL	1525
EventType: PH_DEV_MON_HARDWARE_STATUS	1525
EventType: PH_DEV_MON_HOST_PERF_STATE	1526
EventType: PH_DEV_MON_HVAC_LIEBERT_METRIC	1526
EventType: PH_DEV_MON_HW_AIRFLOW	1527
EventType: PH_DEV_MON_HW_AMP	1528
EventType: PH_DEV_MON_HW_AUDIO	1528
EventType: PH_DEV_MON_HW_CAMERA_MOTION	1529
EventType: PH_DEV_MON_HW_CHASSIS_COMP_STAT	1530
EventType: PH_DEV_MON_HW_CURRENT	1530
EventType: PH_DEV_MON_HW_DEWPT	1531
EventType: PH_DEV_MON_HW_DOOR_SWITCH	1531
EventType: PH_DEV_MON_HW_DRY_CONTACT	1532
EventType: PH_DEV_MON_HW_FAN_SPEED	1532
EventType: PH_DEV_MON_HW_HUMIDITY	1533
EventType: PH_DEV_MON_HW_POWER	1533
EventType: PH_DEV_MON_HW_PS_STAT	1534
EventType: PH_DEV_MON_HW_STACK_UNIT	1534
EventType: PH_DEV_MON_HW_STATUS	1535
EventType: PH_DEV_MON_HW_STATUS_AIRFLOW_CRIT	1538
EventType: PH_DEV_MON_HW_STATUS_AIRFLOW_WARN	1539
EventType: PH_DEV_MON_HW_STATUS_ALARMDEVICE_CRIT	1540
EventType: PH_DEV_MON_HW_STATUS_ALARMDEVICE_WARN	1540
EventType: PH_DEV_MON_HW_STATUS_AMP_CRIT	1541
EventType: PH_DEV_MON_HW_STATUS_AMP_WARN	1542
EventType: PH_DEV_MON_HW_STATUS_AUDIO_CRIT	1542
EventType: PH_DEV_MON_HW_STATUS_AUDIO_WARN	1543
EventType: PH_DEV_MON_HW_STATUS_BATTERY_CRIT	1544
EventType: PH_DEV_MON_HW_STATUS_BATTERY_WARN	1544
EventType: PH_DEV_MON_HW_STATUS_CAMERA_MOTION_CRIT	1545
EventType: PH_DEV_MON_HW_STATUS_CAMERA_MOTION_WARN	1546
EventType: PH_DEV_MON_HW_STATUS_DEWPT_CRIT	1546
EventType: PH_DEV_MON_HW_STATUS_DEWPT_WARN	1547
EventType: PH_DEV_MON_HW_STATUS_DISK_CRIT	1548
EventType: PH_DEV_MON_HW_STATUS_DISK_WARN	1548
EventType: PH_DEV_MON_HW_STATUS_DOOR_SWITCH_CRIT	1549
EventType: PH_DEV_MON_HW_STATUS_DOOR_SWITCH_WARN	1550
EventType: PH_DEV_MON_HW_STATUS_DRY_CONTACT_CRIT	1550
EventType: PH_DEV_MON_HW_STATUS_DRY_CONTACT_WARN	1551
EventType: PH_DEV_MON_HW_STATUS_FAN_CRIT	1552
EventType: PH_DEV_MON_HW_STATUS_FAN_WARN	1552
EventType: PH_DEV_MON_HW_STATUS_FILESYSTEM_CRIT	1553
EventType: PH_DEV_MON_HW_STATUS_FILESYSTEM_WARN	1554
EventType: PH_DEV_MON_HW_STATUS_GEN_NUMERIC_SENSOR_CRIT	1554
EventType: PH_DEV_MON_HW_STATUS_GEN_NUMERIC_SENSOR_WARN	1555
EventType: PH_DEV_MON_HW_STATUS_GEN_STATE_SENSOR_CRIT	1556
EventType: PH_DEV_MON_HW_STATUS_GEN_STATE_SENSOR_WARN	1556
EventType: PH_DEV_MON_HW_STATUS_HUMIDITY_CRIT	1557
EventType: PH_DEV_MON_HW_STATUS_HUMIDITY_WARN	1558

EventType: PH_DEV_MON_HW_STATUS_INPUTCONTACT_CRIT	1558
EventType: PH_DEV_MON_HW_STATUS_INPUTCONTACT_WARN	1559
EventType: PH_DEV_MON_HW_STATUS_LCC_CRIT	1560
EventType: PH_DEV_MON_HW_STATUS_LCC_WARN	1560
EventType: PH_DEV_MON_HW_STATUS_LINK_CRIT	1561
EventType: PH_DEV_MON_HW_STATUS_LINK_WARN	1562
EventType: PH_DEV_MON_HW_STATUS_MEMBEACON_CRIT	1562
EventType: PH_DEV_MON_HW_STATUS_MEMBEACON_WARN	1563
EventType: PH_DEV_MON_HW_STATUS_MEMORY_CRIT	1564
EventType: PH_DEV_MON_HW_STATUS_MEMORY_WARN	1564
EventType: PH_DEV_MON_HW_STATUS_MEMOUTLET_CRIT	1565
EventType: PH_DEV_MON_HW_STATUS_MEMOUTLET_WARN	1566
EventType: PH_DEV_MON_HW_STATUS_MEMOUTPUT_CRIT	1566
EventType: PH_DEV_MON_HW_STATUS_MEMOUTPUT_WARN	1567
EventType: PH_DEV_MON_HW_STATUS_MEMSENSOR_CRIT	1568
EventType: PH_DEV_MON_HW_STATUS_MEMSENSOR_WARN	1568
EventType: PH_DEV_MON_HW_STATUS_MISC_CRIT	1569
EventType: PH_DEV_MON_HW_STATUS_MISC_WARN	1570
EventType: PH_DEV_MON_HW_STATUS_OUTLET_CRIT	1570
EventType: PH_DEV_MON_HW_STATUS_OUTLET_WARN	1571
EventType: PH_DEV_MON_HW_STATUS_OUTPUTRELAY_CRIT	1572
EventType: PH_DEV_MON_HW_STATUS_OUTPUTRELAY_WARN	1572
EventType: PH_DEV_MON_HW_STATUS_PORT_CRIT	1573
EventType: PH_DEV_MON_HW_STATUS_PORT_WARN	1574
EventType: PH_DEV_MON_HW_STATUS_POWERSUPPLY_CRIT	1574
EventType: PH_DEV_MON_HW_STATUS_POWERSUPPLY_WARN	1575
EventType: PH_DEV_MON_HW_STATUS_POWER_ENCLOSURE_CRIT	1576
EventType: PH_DEV_MON_HW_STATUS_POWER_ENCLOSURE_WARN	1576
EventType: PH_DEV_MON_HW_STATUS_PROBE_CRIT	1577
EventType: PH_DEV_MON_HW_STATUS_PROBE_WARN	1578
EventType: PH_DEV_MON_HW_STATUS_SLOT_CRIT	1578
EventType: PH_DEV_MON_HW_STATUS_SLOT_WARN	1579
EventType: PH_DEV_MON_HW_STATUS_STACKUNIT_CRIT	1580
EventType: PH_DEV_MON_HW_STATUS_STACKUNIT_WARN	1580
EventType: PH_DEV_MON_HW_STATUS_TEMP_CRIT	1581
EventType: PH_DEV_MON_HW_STATUS_TEMP_WARN	1582
EventType: PH_DEV_MON_HW_STATUS_VOLTAGE_CRIT	1582
EventType: PH_DEV_MON_HW_STATUS_VOLTAGE_WARN	1583
EventType: PH_DEV_MON_HW_TEMP	1584
EventType: PH_DEV_MON_HW_VOLTAGE	1585
EventType: PH_DEV_MON_HYPERV_CPU_GUEST_VIRTUAL_PROC	1585
EventType: PH_DEV_MON_HYPERV_CPU_LOGICAL_PROC	1586
EventType: PH_DEV_MON_HYPERV_CPU_ROOT_VIRTUAL_PROC	1586
EventType: PH_DEV_MON_HYPERV_MEM_OVERALL	1586
EventType: PH_DEV_MON_HYPERV_MEM_PARTITION	1586
EventType: PH_DEV_MON_HYPERV_MEM_PARTITION_PER_VM	1586
EventType: PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION	1586
EventType: PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION_ROOT	1587
EventType: PH_DEV_MON_HYPERV_MEM_VID_PARTITION	1587

EventType: PH_DEV_MON_HYPERV_MEM_VID_PARTITION_PER_VM	1587
EventType: PH_DEV_MON_HYPERV_NET_LEGACY_ADAPTER	1587
EventType: PH_DEV_MON_HYPERV_NET_VIRTUAL_ADAPTER	1587
EventType: PH_DEV_MON_HYPERV_NET_VIRTUAL_SWITCH	1588
EventType: PH_DEV_MON_HYPERV_OVERALL_HEALTH	1588
EventType: PH_DEV_MON_HYPERV_OVERALL_SYSINFO	1588
EventType: PH_DEV_MON_HYPERV_STORAGE_LOGICAL_DISK	1588
EventType: PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_IDE_CONTROLLER	1588
EventType: PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_STORAGE	1588
EventType: PH_DEV_MON_INCOMING_EXCEED_GUARANTEED	1589
EventType: PH_DEV_MON_INTF_ADMIN_DOWN_TO_UP	1589
EventType: PH_DEV_MON_INTF_ADMIN_UP_TO_DOWN	1590
EventType: PH_DEV_MON_INTF_OPER_DOWN_TO_UP	1590
EventType: PH_DEV_MON_INTF_OPER_UP_TO_DOWN	1590
EventType: PH_DEV_MON_INTF_USAGE_TOTAL	1591
EventType: PH_DEV_MON_IPSLA_HTTP_MET	1591
EventType: PH_DEV_MON_IPSLA_ICMP_MET	1593
EventType: PH_DEV_MON_IPSLA_MET	1593
EventType: PH_DEV_MON_IPSLA_UDP_MET	1595
EventType: PH_DEV_MON_IPSLA_VOIP_MET	1596
EventType: PH_DEV_MON_IRONPORT_MAIL_USAGE	1597
EventType: PH_DEV_MON_ISILON_CLUSTER_HEALTH	1598
EventType: PH_DEV_MON_ISILON_CLUSTER_MEMBERSHIP_CHANGE	1599
EventType: PH_DEV_MON_ISILON_CLUSTER_QUOTA	1599
EventType: PH_DEV_MON_ISILON_CLUSTER_SNAPSHOT	1600
EventType: PH_DEV_MON_ISILON_NODE_DISK_PERF	1601
EventType: PH_DEV_MON_ISILON_NODE_HEALTH	1601
EventType: PH_DEV_MON_ISILON_NODE_PROTO_PERF	1602
EventType: PH_DEV_MON_JBOSS_APP	1603
EventType: PH_DEV_MON_JBOSS_CPU	1603
EventType: PH_DEV_MON_JBOSS_DB_POOL	1604
EventType: PH_DEV_MON_JBOSS_EJB	1604
EventType: PH_DEV_MON_JBOSS_MEMORY	1604
EventType: PH_DEV_MON_JBOSS_REQUEST_PROCESSOR	1604
EventType: PH_DEV_MON_JBOSS_SERVLET	1604
EventType: PH_DEV_MON_JBOSS_SESSION	1604
EventType: PH_DEV_MON_JBOSS_THREAD_POOL	1605
EventType: PH_DEV_MON_LOG_ALL_DEVICE_DELAY_HIGH	1605
EventType: PH_DEV_MON_LOG_ALL_DEVICE_DELAY_LOW	1605
EventType: PH_DEV_MON_LOG_DEVICE_DELAY_HIGH	1605
EventType: PH_DEV_MON_LOG_DEVICE_DELAY_LOW	1606
EventType: PH_DEV_MON_MANUAL_SVC_START_TO_STOP	1606
EventType: PH_DEV_MON_MANUAL_SVC_STOP	1606
EventType: PH_DEV_MON_MANUAL_SVC_STOP_TO_START	1607
EventType: PH_DEV_MON_NETAPP_AGGR_MET	1607
EventType: PH_DEV_MON_NETAPP_CIFS_MET	1608
EventType: PH_DEV_MON_NETAPP_CP_MET	1608
EventType: PH_DEV_MON_NETAPP_DISK_HEALTH	1609

EventType: PH_DEV_MON_NETAPP_DISK_MET	1610
EventType: PH_DEV_MON_NETAPP_FCP_MET	1610
EventType: PH_DEV_MON_NETAPP_ISCSI_MET	1611
EventType: PH_DEV_MON_NETAPP_LUN_MET	1612
EventType: PH_DEV_MON_NETAPP_NFS3_MET	1612
EventType: PH_DEV_MON_NETAPP_NFS4_MET	1613
EventType: PH_DEV_MON_NETAPP_NFS_MET	1614
EventType: PH_DEV_MON_NETAPP_VOL_MET	1614
EventType: PH_DEV_MON_NETBOTZ_HW_EMS_STATUS	1615
EventType: PH_DEV_MON_NETBOTZ_HW_MODULE_SENSOR	1616
EventType: PH_DEV_MON_NETBOTZ_HW_PROBE	1617
EventType: PH_DEV_MON_NETSCALER_APP_FW	1618
EventType: PH_DEV_MON_NETSCALER_SERVICE	1619
EventType: PH_DEV_MON_NETSCALER_VIRT_SERVER	1620
EventType: PH_DEV_MON_NET_INTF_UTIL	1621
EventType: PH_DEV_MON_NIMBLE_GLOBAL_STAT	1624
EventType: PH_DEV_MON_NUTANIX_CLUSTER_STATUS	1624
EventType: PH_DEV_MON_NUTANIX_CONTAINER_INFO	1625
EventType: PH_DEV_MON_NUTANIX_CTRLR_VM_RESOURCE	1626
EventType: PH_DEV_MON_NUTANIX_DISK_STATUS	1626
EventType: PH_DEV_MON_NUTANIX_DISK_TEMP	1627
EventType: PH_DEV_MON_NUTANIX_SERVICE_STATUS	1627
EventType: PH_DEV_MON_NUTANIX_STORAGE_POOL_INFO	1628
EventType: PH_DEV_MON_OMI_PING_STAT	1629
EventType: PH_DEV_MON OSPF_NBR_STATUS	1629
EventType: PH_DEV_MON_PANASONIC_AERO_LOG_MON_STATUS	1630
EventType: PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_HIGH	1631
EventType: PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_LOW	1631
EventType: PH_DEV_MON_PERFMON_DEVICE_DELAY_HIGH	1631

All Logs Page 3 **1632**

EventType: PH_DEV_MON_PERFMON_DEVICE_DELAY_LOW	1645
EventType: PH_DEV_MON_PERFMON_JOB_DELAY_HIGH	1645
EventType: PH_DEV_MON_PERFMON_JOB_DELAY_LOW	1645
EventType: PH_DEV_MON_PERF_MSSQL_BACKUP_INFO	1645
EventType: PH_DEV_MON_PERF_MSSQL_BLOCKBY_INFO	1645
EventType: PH_DEV_MON_PERF_MSSQL_CONFIG_INFO	1646
EventType: PH_DEV_MON_PERF_MSSQL_ERROR_LOG_INFO	1646
EventType: PH_DEV_MON_PERF_MSSQL_GEN_INFO	1646
EventType: PH_DEV_MON_PERF_MSSQL_LOCK_INFO	1646
EventType: PH_DEV_MON_PERF_MSSQL_PERDB	1646
EventType: PH_DEV_MON_PERF_MSSQL_SYS	1647
EventType: PH_DEV_MON_PERF_MSSQL_TOP_QUERIES	1647
EventType: PH_DEV_MON_PERF_MYSQLDB	1647
EventType: PH_DEV_MON_PERF_MYSQLDB_TABLESPACE	1647
EventType: PH_DEV_MON_PERF_ORADB	1647
EventType: PH_DEV_MON_PERF_ORADB_CLUSTER	1647
EventType: PH_DEV_MON_PERF_ORADB_TABLESPACE	1648
EventType: PH_DEV_MON_PERF_ORADB_TOP_QUERIES	1648
EventType: PH_DEV_MON_PING_STAT	1648

EventType: PH_DEV_MON_PING_STAT_SUPPRESSED	1649
EventType: PH_DEV_MON_PORT_CLOSE	1649
EventType: PH_DEV_MON_PORT_OPEN	1650
EventType: PH_DEV_MON_PRINTER_OUTPUT_STATUS	1650
EventType: PH_DEV_MON_PRINTER_SUPPLY_STATUS	1651
EventType: PH_DEV_MON_PROC_CPU_UTIL	1651
EventType: PH_DEV_MON_PROC_MEM_UTIL	1652
EventType: PH_DEV_MON_PROC_RESOURCE_UTIL	1652
EventType: PH_DEV_MON_PROC_START	1653
EventType: PH_DEV_MON_PROC_STOP	1653
EventType: PH_DEV_MON_QUALYS_WEB_APP_FW	1654
EventType: PH_DEV_MON_RBD_BW	1654
EventType: PH_DEV_MON_RBD_CONN	1655
EventType: PH_DEV_MON_RBD_PEER_STAT	1655
EventType: PH_DEV_MON_RBD_PER_PORT_BW	1656
EventType: PH_DEV_MON_RBD_TOP_APP	1656
EventType: PH_DEV_MON_RBD_TOP_DEST	1657
EventType: PH_DEV_MON_RBD_TOP_SRC	1657
EventType: PH_DEV_MON_RBD_TOP_TALKER	1658
EventType: PH_DEV_MON_RDS_METRIC	1658
EventType: PH_DEV_MON_RUCKUS_ACCESS_POINT_STAT	1659
EventType: PH_DEV_MON_RUCKUS_CONTROLLER_STAT	1660
EventType: PH_DEV_MON_RUCKUS_SSID_PERF	1661
EventType: PH_DEV_MON_SERVERIRON_REAL_SERVER_STAT	1662
EventType: PH_DEV_MON_SLB_METRIC	1663
EventType: PH_DEV_MON_SNMP_PING_STAT	1663
EventType: PH_DEV_MON_SRC_AD_REPL_STAT	1664
EventType: PH_DEV_MON_STATUS	1664
EventType: PH_DEV_MON_STORAGE_PORT_DOWN_TO_UP	1664
EventType: PH_DEV_MON_STORAGE_PORT_UP_TO_DOWN	1665
EventType: PH_DEV_MON_SYS_CPU_UTIL	1665
EventType: PH_DEV_MON_SYS_DISK_FREE	1667
EventType: PH_DEV_MON_SYS_DISK_TREND_DAY	1667
EventType: PH_DEV_MON_SYS_DISK_TREND_MONTH	1667
EventType: PH_DEV_MON_SYS_DISK_TREND_WEEK	1668
EventType: PH_DEV_MON_SYS_DISK_UTIL	1669
EventType: PH_DEV_MON_SYS_EXT_CMD	1670
EventType: PH_DEV_MON_SYS_MEM_FREE	1670
EventType: PH_DEV_MON_SYS_MEM_UTIL	1671
EventType: PH_DEV_MON_SYS_PAGEFILE_USAGE	1672
EventType: PH_DEV_MON_SYS_PER_CPU_UTIL	1672
EventType: PH_DEV_MON_SYS_PROC_COUNT	1673
EventType: PH_DEV_MON_SYS_RESTART	1673
EventType: PH_DEV_MON_SYS_STAT	1674
EventType: PH_DEV_MON_SYS_STATUS	1674
EventType: PH_DEV_MON_SYS_SWAP_MEM_ERROR_MSG	1674
EventType: PH_DEV_MON_SYS_UPTIME	1675
EventType: PH_DEV_MON_SYS_VIRT_MEM_UTIL	1676
EventType: PH_DEV_MON_TARGET_FILE_CONTENT_CHANGE	1676

EventType: PH_DEV_MON_TOMCAT_CPU	1677
EventType: PH_DEV_MON_TOMCAT_DB	1677
EventType: PH_DEV_MON_TOMCAT_MEMORY	1677
EventType: PH_DEV_MON_TOMCAT_REQUEST_PROCESSOR	1677
EventType: PH_DEV_MON_TOMCAT_SERVLET	1678
EventType: PH_DEV_MON_TOMCAT_SESSION	1678
EventType: PH_DEV_MON_TOMCAT_THREAD_POOL	1678
EventType: PH_DEV_MON_TRACEROUTE_STAT	1678
EventType: PH_DEV_MON_UCS_HW_CHASSIS_STAT	1679
EventType: PH_DEV_MON_UCS_HW_FAN_STAT	1680
EventType: PH_DEV_MON_UCS_HW_MEMORY_STAT	1681
EventType: PH_DEV_MON_UCS_HW_PROCESSOR_STAT	1681
EventType: PH_DEV_MON_UCS_HW_PSU_STAT	1682
EventType: PH_DEV_MON_UPS_METRIC	1684
EventType: PH_DEV_MON_VMCLUSTER_CPU_UTIL	1686
EventType: PH_DEV_MON_VMCLUSTER_DATASTORE_IO	1686
EventType: PH_DEV_MON_VMCLUSTER_MEM_UTIL	1686
EventType: PH_DEV_MON_VMCLUSTER_STATUS	1686
EventType: PH_DEV_MON_VMRESPOOL_CPU_UTIL	1686
EventType: PH_DEV_MON_VMRESPOOL_MEM_UTIL	1686
EventType: PH_DEV_MON_VM_CPU_UTIL	1687
EventType: PH_DEV_MON_VM_DATASTORE_IO	1687
EventType: PH_DEV_MON_VM_DISK_IO	1687
EventType: PH_DEV_MON_VM_DISK_UTIL	1687
EventType: PH_DEV_MON_VM_MEM_UTIL	1687
EventType: PH_DEV_MON_VM_NET_INTF_UTIL	1688
EventType: PH_DEV_MON_VM_PER_CPU_UTIL	1688
EventType: PH_DEV_MON_VM_SNAPSHOT	1688
EventType: PH_DEV_MON_VM_STATE	1688
EventType: PH_DEV_MON_VM_TOOLS_STATUS	1688
EventType: PH_DEV_MON_VM_UPTIME	1688
EventType: PH_DEV_MON_VPN_CONN	1689
EventType: PH_DEV_MON_VPN_STATUS	1689
EventType: PH_DEV_MON_WATCHGUARD_POLICY_STAT	1690
EventType: PH_DEV_MON_WEBLOGIC_APP	1690
EventType: PH_DEV_MON_WEBLOGIC_DB_POOL	1691
EventType: PH_DEV_MON_WEBLOGIC_EJB	1691
EventType: PH_DEV_MON_WEBLOGIC_GEN	1691
EventType: PH_DEV_MON_WEBLOGIC_MEMORY	1691
EventType: PH_DEV_MON_WEBLOGIC_SERVLET	1691
EventType: PH_DEV_MON_WEBLOGIC_SESSION	1691
EventType: PH_DEV_MON_WEBLOGIC_THREAD_POOL	1692
EventType: PH_DEV_MON_WEBSPHERE_APP	1692
EventType: PH_DEV_MON_WEBSPHERE_AUTHENTICATION	1692
EventType: PH_DEV_MON_WEBSPHERE_CPU	1692
EventType: PH_DEV_MON_WEBSPHERE_DB_POOL	1692
EventType: PH_DEV_MON_WEBSPHERE_EJB	1693
EventType: PH_DEV_MON_WEBSPHERE_MEMORY	1693
EventType: PH_DEV_MON_WEBSPHERE_SERVLET	1693

EventType: PH_DEV_MON_WEBSPHERE_THREAD_POOL	1693
EventType: PH_DEV_MON_WEBSPHERE_TRANSACTION	1693
EventType: PH_DEV_MON_WMI_PING_STAT	1693
EventType: PH_DISCOVERY_COMPLETE	1694
EventType: PH_DISCOVERY_RESULT_SENT	1694
EventType: PH_DISCOV_ACCESS_IP_PARSE_ERROR	1694
EventType: PH_DISCOV_ADS_ACCOUNT_TO_EXPIRE	1695
EventType: PH_DISCOV_ADS_ACCT_DISABLED	1695
EventType: PH_DISCOV_ADS_DORMANT_ACCT	1695
EventType: PH_DISCOV_ADS_PASSWORD_NEVER_EXPIRES	1696
EventType: PH_DISCOV_ADS_PASSWORD_NOT_REQD	1696
EventType: PH_DISCOV_ADS_PASSWORD_STALE	1697
EventType: PH_DISCOV_ADS_PASSWORD_TO_EXPIRE	1697
EventType: PH_DISCOV_ARUBA_WLAN_HOST_LOCATION	1698
EventType: PH_DISCOV_AWS_DEVICE_DELETED	1699
EventType: PH_DISCOV_AWS_DEVICE_UNKNOWN	1699
EventType: PH_DISCOV_AWS_DISCOV_FAILED	1699
EventType: PH_DISCOV_AZURE_DISCOV_FAILED	1700
EventType: PH_DISCOV_BASIC_FAILED	1700
EventType: PH_DISCOV_BASIC_SKIPPED	1700
EventType: PH_DISCOV_BASIC_SNMP_DETAIL	1701
EventType: PH_DISCOV_BASIC_SNMP_ERROR	1701
EventType: PH_DISCOV_BASIC_SNMP_FAILED	1701
EventType: PH_DISCOV_BASIC_SNMP_STARTED	1702
EventType: PH_DISCOV_BASIC_SNMP_SUCCESS	1702
EventType: PH_DISCOV_BASIC_SSH_DETAIL	1703
EventType: PH_DISCOV_BASIC_SSH_ERROR	1703
EventType: PH_DISCOV_BASIC_SSH_FAILED	1703
EventType: PH_DISCOV_BASIC_SSH_STARTED	1704
EventType: PH_DISCOV_BASIC_SSH_SUCCESS	1704
EventType: PH_DISCOV_BASIC_STARTED	1704
EventType: PH_DISCOV_BGP OSPF_FAILED	1705
EventType: PH_DISCOV_BROCADE_SERVER_IRON_HW_INFO_WARNING	1705
EventType: PH_DISCOV_CANCEL_UNKNOWN_REQ	1705
EventType: PH_DISCOV_CERT_FILE_DOWNLOAD_FAILURE	1705
EventType: PH_DISCOV_CHECKPOINT_TEST_CONN_FAILED	1706
EventType: PH_DISCOV_CISCO_ASA_GET_CONTEXT_FAILED	1706
EventType: PH_DISCOV_CISCO_ASA_IPSEC_VPN_FAILED	1706
EventType: PH_DISCOV_CISCO_ASA_RAS_VPN_FAILED	1707
EventType: PH_DISCOV_CISCO_ASA_RUN_CONFIG_FAILED	1707
EventType: PH_DISCOV_CISCO_ASA_SET_CONTEXT_FAILED	1707
EventType: PH_DISCOV_CISCO_ASA_STARTUP_CONFIG_FAILED	1708
EventType: PH_DISCOV_CISCO_CALL_MANAGER_WARNING	1708
EventType: PH_DISCOV_CISCO_CATOS_INTF_FAILED	1709
EventType: PH_DISCOV_CISCO_CDP_ERROR	1709
EventType: PH_DISCOV_CISCO_IOS_L2_WARNING	1709
EventType: PH_DISCOV_CISCO_IOS_TRUNK_PORT_ERROR	1710
EventType: PH_DISCOV_CISCO_JUNOS_L2_WARNING	1710
EventType: PH_DISCOV_CISCO_NXOS_HW_STATUS_WARNING	1710

EventType: PH_DISCOV_CISCO_NXOS_INTF_SHORT_NAME_NOT_FOUND	1711
EventType: PH_DISCOV_CISCO_NXOS_L2_WARNING	1711
EventType: PH_DISCOV_CISCO_WLAN_HOST_LOCATION	1711
EventType: PH_DISCOV_CLOCK_ROLLS_BACK	1712
EventType: PH_DISCOV_CONTACT_APP_SERVER	1712
EventType: PH_DISCOV_CREDEN_INSERT_ERROR	1713
EventType: PH_DISCOV_CUSTOM_MAP_LOAD_FAILED	1713
EventType: PH_DISCOV_DATA_DOMAIN_HW_STATUS_WARNING	1713
EventType: PH_DISCOV_DELL_BLADE_CHASSIS_WARNING	1714
EventType: PH_DISCOV_DELL_COMPELLENT_STORAGE_WARNING	1714
EventType: PH_DISCOV_DISCOV_REQ_GET_FAILED	1714
EventType: PH_DISCOV_DISCOV_RESULT_SENDER_THREADS_SPAWN_FAILED	1714
EventType: PH_DISCOV_DISCOV_THREADS_SPAWN_FAILED	1715
EventType: PH_DISCOV_EC2_INSTANCE_PARSE_FAILED	1715
EventType: PH_DISCOV EMC_CLARION_ERROR	1715
EventType: PH_DISCOV EMC_VNX_DISCOV_FAILED	1715
EventType: PH_DISCOV EMC_VNX_PING_FAILED	1716
EventType: PH_DISCOV_EQLOGIC_CONN_FAILED	1716
EventType: PH_DISCOV_EQLOGIC_HW_INFO_FAILED	1717
EventType: PH_DISCOV_ESX_HOST_PING_ONLY_DISCOV_ERROR	1717
EventType: PH_DISCOV_FAILED_INVALID_REQUEST	1717
EventType: PH_DISCOV_FAILED_INVALID_REQUEST_XML	1718
EventType: PH_DISCOV_FAILED_XML_ERROR	1718
EventType: PH_DISCOV_FAIL_CMDB_DEV	1718
EventType: PH_DISCOV_FILE_BASED_DISCOV_DIR_NOT_CONFIGURED	1718
EventType: PH_DISCOV_FILE_BASED_DISCOV_FAILED	1719
EventType: PH_DISCOV_FORTINET_CPU_INFO_WARNING	1719
EventType: PH_DISCOV_FORTINET_LINK_STAT_WARNING	1719
EventType: PH_DISCOV_FORTINET_SYS_UPDATE_VERSION_WARNING	1720
EventType: PH_DISCOV_GENERIC_ERROR	1720
EventType: PH_DISCOV_GEN_WLAN_HOST_LOCATION	1720
EventType: PH_DISCOV_GET_SNMP_ENGINE_ID_FAILED	1721
EventType: PH_DISCOV_HOST_CONVERT_PROCESS_UPTIME_ERROR	1721
EventType: PH_DISCOV_HOST_ERROR	1722
EventType: PH_DISCOV_HOST_INSTALL_SW_WARNING	1722
EventType: PH_DISCOV_HOST_LOCATE_PROCESS_ERROR	1722
EventType: PH_DISCOV_HOST_LOCATION	1723
EventType: PH_DISCOV_HOST_NET_INTF	1723
EventType: PH_DISCOV_HOST_STARTED	1723
EventType: PH_DISCOV_HOST_SUCCESS	1724
EventType: PH_DISCOV_HOST_SUCCESS_DETAIL	1724
EventType: PH_DISCOV_HOST_WARNING	1725
EventType: PH_DISCOV_HP3COM_HW_WARNING	1725
EventType: PH_DISCOV_HP_BLADE_HW_STATUS_WARNING	1725
EventType: PH_DISCOV_INIT_MODULE_FAILED	1726
EventType: PH_DISCOV_INTERFACE_VIA_SNMP_FAILED	1726
EventType: PH_DISCOV_IP_TYPE_INVALID	1726
EventType: PH_DISCOV_ISILON_HW_STATUS_WARNING	1726

EventType: PH_DISCOV_JMX_TEST_CONN_FAILED	1727
EventType: PH_DISCOV_JUNIPER_SSG_HW_INFO_WARNING	1727
EventType: PH_DISCOV_L2_FAILED	1728
EventType: PH_DISCOV_L2_STARTED	1728
EventType: PH_DISCOV_L2_SUCCESS	1728
EventType: PH_DISCOV_LDAP_ERROR	1729
EventType: PH_DISCOV_LDAP_OU_ERROR	1729
EventType: PH_DISCOV_LINUX_DSKTABLE_NOT_CONFIG	1729
EventType: PH_DISCOV_LOGIN_ERROR	1730
EventType: PH_DISCOV_NEXT_HOP_VIA_SNMP_FAILED	1730
EventType: PH_DISCOV_NIMBLE_VOLUME_WARNING	1731
EventType: PH_DISCOV_NOZOMI_DISCOV_FAILED	1731
EventType: PH_DISCOV_PARAM_PARSE_FAILED	1731
EventType: PH_DISCOV_PARSER_MSG_EXCEEDS_THRESHOLD	1732
EventType: PH_DISCOV_PARSER_MSG_THREAD_SPAWN_FAILED	1732
EventType: PH_DISCOV_PERF_TEMPLATE_LOAD_FAILED	1732
EventType: PH_DISCOV_PING_ONLY_LIST_NOT_MATCH	1732
EventType: PH_DISCOV_READ_COMPRESS_THRESHOLD_FAILED	1732
EventType: PH_DISCOV_RECVD_VALID_REQUEST	1733
EventType: PH_DISCOV_RESULT_SEND_FAILED	1733
EventType: PH_DISCOV_RESULT_SEND_WARNING	1733
EventType: PH_DISCOV_RESULT_XML_WRITE_FAILURE	1733
EventType: PH_DISCOV_RUNNING_SERVICE	1734
EventType: PH_DISCOV_RUN_JAVA_PROBE_ERROR	1734
EventType: PH_DISCOV_RUN_SW_FILTER_LOAD_FAILED	1735
EventType: PH_DISCOV_RUN_SW_FILTER_PARSE_FAILED	1735
EventType: PH_DISCOV_RUN_VM_TEST_CONN_ERROR	1735
EventType: PH_DISCOV_SKIPPED	1735
EventType: PH_DISCOV_SKIP_DEV	1735
EventType: PH_DISCOV_SNMP_ERROR	1736
EventType: PH_DISCOV_SSH_ERROR	1736
EventType: PH_DISCOV_START	1737
EventType: PH_DISCOV_TELNET_ERROR	1737
EventType: PH_DISCOV_TEST_CONN_GET_REQ_FAILED	1737
EventType: PH_DISCOV_TEST_CONN_MSRPC_ERROR	1737
EventType: PH_DISCOV_TEST_CONN_NO_UCSAPI_CRED	1738
EventType: PH_DISCOV_TEST_CONN_RESULT_SENDER_THREADS_	
SPAWN_FAILED	1738
EventType: PH_DISCOV_TEST_CONN_RESULT_SEND_ERROR	1738
EventType: PH_DISCOV_TEST_CONN_RESULT_SEND_WARNING	1738
EventType: PH_DISCOV_TEST_CONN_THREADS_SPAWN_FAILED	1739
EventType: PH_DISCOV_TEST_CONN_VMSDK_ERROR	1739
EventType: PH_DISCOV_TRIPP_UPS_HW_STATUS_WARNING	1739
EventType: PH_DISCOV_TRUNK_PORTS_ERROR	1740
EventType: PH_DISCOV_UNHANDLED_ACCESS_PROTO	1740
EventType: PH_DISCOV_UPLOAD_DATA_FAILED	1740
EventType: PH_DISCOV_VMWARE_DUP_DEV_ID	1740
EventType: PH_DISCOV_VMWARE_ERROR	1740
EventType: PH_DISCOV_VOIP_PHONE_ID	1741

EventType: PH_DISCOV_WMI_PULL_ERROR	1741
EventType: PH_DISC_DATA_PROCESS_ERROR	1741
EventType: PH_DIVIDE_BY_ZERO	1742
EventType: PH_DROP_EVENT_FROM_SHARED_BUFFER	1742
EventType: PH_DROP_INCIDENT	1742
EventType: PH_DROP_INCIDENT_COUNT	1743
EventType: PH_ES_ARCHIVE_STORAGE_CHECK_ERROR	1743
EventType: PH_ES_ARCHIVE_STORAGE_LOW	1743
EventType: PH_ES_ARCHIVE_STORAGE_PURGING_FAILED	1744
EventType: PH_ES_ARCHIVE_STORAGE_PURGING_FINISHED	1744
EventType: PH_ES_ARCHIVE_STORAGE_PURGING_STARTED	1744
EventType: PH_ES_ARCHIVE_STORAGE_PURGING_SUCCESS	1745
EventType: PH_ES_ARCHIVE_STORAGE_USAGE	1745
EventType: PH_ES_CCR_DELAY	1745
EventType: PH_ES_COLD_STORAGE_ARCHIVING_FAILED	1746
EventType: PH_ES_COLD_STORAGE_ARCHIVING_FINISHED	1746
EventType: PH_ES_COLD_STORAGE_ARCHIVING_STARTED	1746
EventType: PH_ES_COLD_STORAGE_ARCHIVING_SUCCESS	1746
EventType: PH_ES_COLD_STORAGE_CHECK_ERROR	1747
EventType: PH_ES_COLD_STORAGE_LOW	1747
EventType: PH_ES_COLD_STORAGE_PURGING_FAILED	1747
EventType: PH_ES_COLD_STORAGE_PURGING_FINISHED	1748
EventType: PH_ES_COLD_STORAGE_PURGING_STARTED	1748
EventType: PH_ES_COLD_STORAGE_PURGING_SUCCESS	1748
EventType: PH_ES_COLD_STORAGE_USAGE	1749
EventType: PH_ES_HOTCOLD_STORAGE_MOVING_FAILED	1749
EventType: PH_ES_HOTCOLD_STORAGE_MOVING_FINISHED	1749
EventType: PH_ES_HOTCOLD_STORAGE_MOVING_STARTED	1749
EventType: PH_ES_HOTCOLD_STORAGE_MOVING_SUCCESS	1750
EventType: PH_ES_HOT_STORAGE_ARCHIVING_FAILED	1750
EventType: PH_ES_HOT_STORAGE_ARCHIVING_FINISHED	1750
EventType: PH_ES_HOT_STORAGE_ARCHIVING_STARTED	1751
EventType: PH_ES_HOT_STORAGE_ARCHIVING_SUCCESS	1751
EventType: PH_ES_HOT_STORAGE_CHECK_ERROR	1751
EventType: PH_ES_HOT_STORAGE_LOW	1752
EventType: PH_ES_HOT_STORAGE_MOVING_FAILED	1752
EventType: PH_ES_HOT_STORAGE_MOVING_FINISHED	1752
EventType: PH_ES_HOT_STORAGE_MOVING_STARTED	1753
EventType: PH_ES_HOT_STORAGE_MOVING_SUCCESS	1753
EventType: PH_ES_HOT_STORAGE_PURGING_FAILED	1753
EventType: PH_ES_HOT_STORAGE_PURGING_FINISHED	1753
EventType: PH_ES_HOT_STORAGE_PURGING_STARTED	1754
EventType: PH_ES_HOT_STORAGE_PURGING_SUCCESS	1754
EventType: PH_ES_HOT_STORAGE_USAGE	1755
EventType: PH_ES_INDEX_SEGMENT_MERGE_FAILED	1755
EventType: PH_ES_REST_FAILED	1755
EventType: PH_ES_SM_ADD_INDEX_FAILED	1755
EventType: PH_ES_SM_HOURLCHECK_FAILED	1756
EventType: PH_ES_SM_INIT_FAILED	1756

EventType: PH_ES_SM_INIT_INDEX_FAILED	1756
EventType: PH_ES_SNAPSHOT_FAILED	1756
EventType: PH_ES_TO_NFS_ARCHIVE_FAILED_ADD_INDEX	1756
EventType: PH_ES_WARM_STORAGE_ARCHIVING_FAILED	1756
EventType: PH_ES_WARM_STORAGE_ARCHIVING_FINISHED	1757
EventType: PH_ES_WARM_STORAGE_ARCHIVING_STARTED	1757
EventType: PH_ES_WARM_STORAGE_ARCHIVING_SUCCESS	1757
EventType: PH_ES_WARM_STORAGE_CHECK_ERROR	1758
EventType: PH_ES_WARM_STORAGE_LOW	1758
EventType: PH_ES_WARM_STORAGE_MOVING_FAILED	1758
EventType: PH_ES_WARM_STORAGE_MOVING_FINISHED	1759
EventType: PH_ES_WARM_STORAGE_MOVING_STARTED	1759
EventType: PH_ES_WARM_STORAGE_MOVING_SUCCESS	1759
EventType: PH_ES_WARM_STORAGE_PURGING_FAILED	1760
EventType: PH_ES_WARM_STORAGE_PURGING_FINISHED	1760
EventType: PH_ES_WARM_STORAGE_PURGING_STARTED	1760
EventType: PH_ES_WARM_STORAGE_PURGING_SUCCESS	1760
EventType: PH_ES_WARM_STORAGE_USAGE	1761
EventType: PH_EVENT_ATTR_XML_ISSUE	1761
EventType: PH_EVENT_FORWARDER_CHECKSUM_MISMATCH	1761
EventType: PH_EVENT_FORWARDER_CONNECT_ERROR	1762
EventType: PH_EVENT_FORWARDER_DIR_OPEN_FAILURE	1762
EventType: PH_EVENT_FORWARDER_FILE_OPEN_FAILURE	1762
EventType: PH_EVENT_FORWARDER_FILE_RENAME_FAILURE	1762
EventType: PH_EVENT_FORWARDER_INIT_FAILURE	1763
EventType: PH_EVENT_FORWARDER_INVALID_GZIP_FILE	1763
EventType: PH_EVENT_FORWARDER_INVALID_PHOENIX_CONFIG	1763
EventType: PH_EVENT_FORWARDER_INVALID_PROTOCOL	1764
EventType: PH_EVENT_FORWARDER_KAFKA_ERROR	1764
EventType: PH_EVENT_FORWARDER_KAFKA_INIT_FAILURE	1764
EventType: PH_EVENT_FORWARDER_KAFKA_PRODUCE_ERROR	1765
EventType: PH_EVENT_FORWARDER_MKDIR_FAILURE	1765
EventType: PH_EVENT_FORWARDER_RUN_PROCESS_ERROR	1765
EventType: PH_EVENT_FORWARDER_SOCKET_ERROR	1766
EventType: PH_EVENT_FORWARDER_SOCKET_WRITE_ERROR	1766
EventType: PH_EVENT_FORWARDER_SSL_CERT_ERROR	1766
EventType: PH_EVENT_FORWARDER_SSL_ERROR	1766
EventType: PH_EVENT_FWD_CERT_LOAD_FAILED	1767
EventType: PH_EVENT_FWD_CERT_UNPAIRED	1767
EventType: PH_EVENT_FWD_DIR_MAKE_FAILED	1767
EventType: PH_EVENT_FWD_DIR_OPEN_FAILED	1768
EventType: PH_EVENT_FWD_FILE_RENAME_FAILED	1768
EventType: PH_EVENT_FWD_FULL_FORWARDING_FAILED	1768
EventType: PH_EVENT_FWD_GET_FILE_NUM_FAILURE	1769
EventType: PH_EVENT_FWD_GZ_CLOSE_ERROR	1769
EventType: PH_EVENT_FWD_GZ_FILE_OPEN_ERROR	1769
EventType: PH_EVENT_FWD_GZ_MD5_ERROR	1770
EventType: PH_EVENT_FWD_GZ_RENAME_ERROR	1770
EventType: PH_EVENT_FWD_GZ_SIZE_MISMATCH	1770

EventType: PH_EVENT_FWD_KAFKA_WARNING	1770
EventType: PH_EVENT_FWD_MD5_CHECKSUM_MISMATCH	1771
EventType: PH_EVENT_FWD_NETFLOW_REGEX_IGNORED	1771
EventType: PH_EVENT_FWD_PARTIAL_FORWARDING_FAILED	1771
EventType: PH_EVENT_FWD_PARTIAL_FORWARDING_WARNING	1771
EventType: PH_EVENT_FWD_PCRE_ERROR	1771
EventType: PH_EVENT_FWD_PROCESS_INIT_FAILED	1772
EventType: PH_EVENT_FWD_PROCESS_START_FAILED	1772
EventType: PH_EVENT_FWD_PROTO_FORWARDED_WRONG	1772
EventType: PH_EVENT_FWD_RENAME_GZ_ERROR	1772
EventType: PH_EVENT_FWD_RULE_PARSE_ERROR	1773
EventType: PH_EVENT_FWD_SOCKET_CONNECT_FAILED	1773
EventType: PH_EVENT_FWD_SOCKET_GET_FAILED	1773
EventType: PH_EVENT_FWD_SOCKET_WRITE_FAILED	1773
EventType: PH_EVENT_FWD_SSL_CREATE_FAILED	1774
EventType: PH_EVENT_FWD_SSL_SESSION_BUILD_FAILED	1774
EventType: PH_EVENT_FWD_UNEXPECTED_FILE_REMOVED	1774
EventType: PH_EVENT_PKG_ATTR_NOT_FOUND	1775
EventType: PH_EVENT_PKG_EMPTY_FILE_REMOVED	1775
EventType: PH_EVENT_PKG_FILE_ADD_TO_SVN_FAILED	1775
EventType: PH_EVENT_PKG_FILE_REMOVED_ERROR	1775
EventType: PH_EVENT_PKG_FILE_RENAME_FAILED	1776
EventType: PH_EVENT_PKG_FILE_STAT_FAILED	1776
EventType: PH_EVENT_PKG_FILE_UPLOAD_FAILED	1776
EventType: PH_EVENT_PKG_FILE_UPLOAD_SUCCESS_HIGH	1777
EventType: PH_EVENT_PKG_FILE_UPLOAD_SUCCESS_LOW	1777
EventType: PH_EVENT_PKG_GZ_CLOSE_FAILED	1777
EventType: PH_EVENT_PKG_GZ_FILE_OPEN_ERROR	1778
EventType: PH_EVENT_PKG_HTTP_FAILED	1778
EventType: PH_EVENT_PKG_HTTP_INIT_FAILED	1778
EventType: PH_EVENT_PKG_INSERT_TASK_FAILED	1779
EventType: PH_EVENT_PKG_NO_EVENT	1779
EventType: PH_EVENT_PKG_OPEN_DIR_FAILED	1779
EventType: PH_EVENT_PKG_PROCESS_INIT_FAILED	1779
EventType: PH_EVENT_PKG_PROCESS_START_FAILED	1780
EventType: PH_EVENT_PKG_QUEUE_GET_FAILED	1780
EventType: PH_EVENT_PKG_SERVER_LIST_UPLOAD_FAILED	1780
EventType: PH_EVENT_PKG_SERVICE_LIST_EMPTY	1780
EventType: PH_EVENT_PKG_TASK_ADD_TO_QUEUE_FAILED	1781
EventType: PH_EVENT_PKG_XML_PARSE_FAILED	1781
EventType: PH_EVTPKGGER_FILE_UPLOAD_FAILED	1781
EventType: PH_EVT_HANDLER_DBG	1781
EventType: PH_EVT_HANDLER_ERR	1781
EventType: PH_EVT_HANDLER_EVT_QUEUE_LARGE	1782
EventType: PH_EVT_HANDLER_EVT_QUEUE_WARNING	1782
EventType: PH_EVT_HANDLER_INFO	1782
EventType: PH_EVT_HANDLER_SVN_QUEUE_LARGE	1782
EventType: PH_EVT_HANDLER_SVN_QUEUE_WARNING	1782
EventType: PH_EVT_PACKAGER_COND_WAIT_ERROR	1783

EventType: PH_EVT_PACKAGER_FILE_CLOSE_FAILURE	1783
EventType: PH_EVT_PACKAGER_FILE_OPEN_FAILURE	1783
EventType: PH_EVT_PACKAGER_FILE_REMOVE_FAILURE	1784
EventType: PH_EVT_PACKAGER_FILE_RENAME_FAILURE	1784
EventType: PH_EVT_PACKAGER_FILE_STAT_FAILURE	1784
EventType: PH_EVT_PACKAGER_FILE_UPLOAD_FAILURE	1785
EventType: PH_EVT_PACKAGER_HTTP_RESPONSE_ERROR	1785
EventType: PH_EVT_PACKAGER_INIT_FAILURE	1785
EventType: PH_EVT_PACKAGER_REST_PARSE_ERROR	1786
EventType: PH_EVT_PACKAGER_RUN_PROCESS_ERROR	1786
EventType: PH_FAILED_TO_EXEC	1786
EventType: PH_FILE_NOT_FOUND	1786
EventType: PH_GCS_BUCKET_ACCESS_FAILURE	1786
EventType: PH_GENERIC_CRITICAL	1787
EventType: PH_GENERIC_DEBUG	1787
EventType: PH_GENERIC_ERROR	1787
EventType: PH_GENERIC_INFO	1787
EventType: PH_GENERIC_WARNING	1787
EventType: PH_GET_CURL_HANDLE_FAILED	1787
EventType: PH_GET_SUPER_LEADER_FAILURE	1788
EventType: PH_GRPC_CERT_CREATE_SUCCESS	1788
EventType: PH_GRPC_CERT_ERROR	1788
EventType: PH_GRPC_CERT_LOADED_FAILED	1788
EventType: PH_GRPC_CERT_UPDATE_FAILED	1789
EventType: PH_GRPC_CERT_UPDATE_SUCCESS	1789
EventType: PH_GRPC_FORTMAT_JSON_FAILED	1789
EventType: PH_GRPC_INIT_SSL_CONTEXT	1789
EventType: PH_GRPC_TASK_DATA_EMPTY	1790
EventType: PH_HDFS_ARCHIVE_STORAGE_LOW	1790
EventType: PH_HDFS_ARCHIVE_STORAGE_USAGE	1790
EventType: PH_HDFS_PURGING_FAILED	1791
EventType: PH_HDFS_PURGING_FINISHED	1791
EventType: PH_HDFS_PURGING_STARTED	1791
EventType: PH_HDFS_PURGING_SUCCESS	1792
EventType: PH_HTTP_CLIENT_COMPRESS_FAILED	1792
EventType: PH_HTTP_CLIENT_CURL_ERROR	1792
EventType: PH_HTTP_CLIENT_GET_CACHE_FROM_MONITOR_FAILED	1793
EventType: PH_HTTP_CLIENT_GET_DATA_FROM_CACHE_FAILED	1793
EventType: PH_HTTP_CLIENT_GET_INIT_RESPONSE_FAILED	1793
EventType: PH_HTTP_CLIENT_GET_INIT_RESPONSE_WARNING	1794
EventType: PH_HTTP_CLIENT_GET_RESPONSE_WARNING	1794
EventType: PH_HTTP_CLIENT_HOST_IS_NULL	1794
EventType: PH_HTTP_CLIENT_INIT_FAILURE	1794
EventType: PH_HTTP_CLIENT_INIT_WARNING	1795
EventType: PH_HTTP_CLIENT_INVALID_FILE_SIZE	1795
EventType: PH_HTTP_CLIENT_MKSTEMP_FAILED	1795
EventType: PH_HTTP_CLIENT_NO_FILE_PARAM	1795
EventType: PH_HTTP_CLIENT_PICK_SUPER_FAILED	1796
EventType: PH_HTTP_CLIENT_PREP_REQUEST_ERROR	1796

EventType: PH_HTTP_CLIENT_PUT_REDIRECT_FAILURE	1796
EventType: PH_HTTP_CLIENT_SETOPT_FAILED	1796
EventType: PH_HTTP_CLIENT_SET_HOST_WARNING	1797
EventType: PH_HTTP_CLIENT_UPLOAD_FILE_FAILED	1797
EventType: PH_HTTP_CLIENT_WRITE_CACHE_NULL	1797
EventType: PH_HTTP_INIT_FAILURE	1797
EventType: PH_HTTP_RESPONSE_FAILURE	1798
EventType: PH_IDENTITYMASTER_HTTP_UPLOAD_ERROR	1798
EventType: PH_IDENTITYMASTER_INIT_ERROR	1798
EventType: PH_IDENTITYWORKER_ATTRIB_ERROR	1799
EventType: PH_IDENTITYWORKER_EVT_LOAD_ERROR	1799
EventType: PH_IDENTITYWORKER_EVT_SEND_ERROR	1799
EventType: PH_IDENTITYWORKER_INIT_ERROR	1800
EventType: PH_IDENTITYWORKER_PARAM_ERROR	1800
EventType: PH_IDENTITYWORKER_PROCESSING_EPS	1800
EventType: PH_IDENTITYWORKER_SS_OBTAIN_ERROR	1800
EventType: PH_INCIDENT_ACTION_STATUS	1801
EventType: PH_INVALID_IP_ADDR	1801
EventType: PH_INVALID_PARAM	1801
EventType: PH_INVALID_PARAM_CNT	1801
EventType: PH_INVALID_PARAM_VAL_EMPTY	1802
EventType: PH_JAVA_AGENT_APPSERVER_CONN_ERROR	1802
EventType: PH_JAVA_AGENT_APPSERVER_EXECUTE_ERROR	1802
EventType: PH_JAVA_AGENT_CONTROLLER_CMD_PARSE_ERROR	1803
EventType: PH_JAVA_AGENT_CONTROLLER_CMD_READ_ERROR	1803
EventType: PH_JAVA_AGENT_CONTROLLER_GENERIC_ERROR	1803
EventType: PH_JAVA_AGENT_CONTROLLER_LINE_READ_ERROR	1803
EventType: PH_JAVA_AGENT_CONTROLLER_XML_READ_ERROR	1803
EventType: PH_JAVA_AGENT_CUSTOM_JDBC_CONN_ERROR	1803
EventType: PH_JAVA_AGENT_CUSTOM_JDBC_EXEC_ERROR	1804
EventType: PH_JAVA_AGENT_DISCOVERY_TEST_ERROR	1804
EventType: PH_JAVA_AGENT_ERROR	1804
EventType: PH_JAVA_AGENT_GLASSFISH_MONITOR_ERROR	1804
EventType: PH_JAVA_AGENT_GLASS_FISH_WARNING	1804
EventType: PH_JAVA_AGENT_GOOGLEAPPS_EXEC_ERROR	1805
EventType: PH_JAVA_AGENT_IBMDB2_AUDIT_CONN_ERROR	1805
EventType: PH_JAVA_AGENT_IBMDB2_AUDIT_EXEC_ERROR	1805
EventType: PH_JAVA_AGENT_IBM_DB2_CAT_READ_ERROR	1805
EventType: PH_JAVA_AGENT_IBM_DB2_CONN_ERROR	1805
EventType: PH_JAVA_AGENT_IBM_DB2_INTERNAL_ERROR	1805
EventType: PH_JAVA_AGENT_INFO	1806
EventType: PH_JAVA_AGENT_JBOSS_CONN_ERROR	1806
EventType: PH_JAVA_AGENT_JBOSS_EXEC_ERROR	1806
EventType: PH_JAVA_AGENT_JBOSS_MONITOR_ERROR	1806
EventType: PH_JAVA_AGENT_JDBC_PULL_UNSUPP_ERROR	1806
EventType: PH_JAVA_AGENT_JDBC_SQL_NOT_SUPPORT_ERROR	1807
EventType: PH_JAVA_AGENT_JMX_CONN_ERROR	1807
EventType: PH_JAVA_AGENT_JMX_EXEC_ERROR	1807
EventType: PH_JAVA_AGENT_JOB_EXECUTOR_ERROR	1807

EventType: PH_JAVA_AGENT_JOB_STATUS_UPLOAD_ERROR	1807
EventType: PH_JAVA_AGENT_JOB_TYPE_ERROR	1807
EventType: PH_JAVA_AGENT_JOB_XML_LOAD_ERROR	1808
EventType: PH_JAVA_AGENT_JOB_XML_PARSE_ERROR	1808
EventType: PH_JAVA_AGENT_MCAFEE_MYSQL_MONITOR_ERROR	1808
EventType: PH_JAVA_AGENT_MCAFEE_VULN_SCANNER_ERROR	1808
EventType: PH_JAVA_AGENT_MONITOR_GEN_ERROR	1808
EventType: PH_JAVA_AGENT_MONITOR_TIMEOUT_ERROR	1809
EventType: PH_JAVA_AGENT_MSSQL_DDL_CONN_ERROR	1809
EventType: PH_JAVA_AGENT_MSSQL_LOGON_CONN_ERROR	1809
EventType: PH_JAVA_AGENT_MSSQL_LOGON_EXEC_ERROR	1809
EventType: PH_JAVA_AGENT_MSSQL_MONITOR_ERROR	1809
EventType: PH_JAVA_AGENT_MSSQL_PERF_CONN_ERROR	1809
EventType: PH_JAVA_AGENT_MSSQL_PERF_EXECUTE_ERROR	1810
EventType: PH_JAVA_AGENT_MYSQL_PERF_CONN_ERROR	1810
EventType: PH_JAVA_AGENT_MYSQL_PERF_EXEC_ERROR	1810
EventType: PH_JAVA_AGENT_NESSUS_REPORT_PARSE_ERROR	1810
EventType: PH_JAVA_AGENT_ORACLE_DB_ERROR	1810
EventType: PH_JAVA_AGENT_ORADB_AUDIT_CONN_ERROR	1811
EventType: PH_JAVA_AGENT_ORADB_AUDIT_EXEC_ERROR	1811
EventType: PH_JAVA_AGENT_ORADB_LOGON_EXEC_ERROR	1811
EventType: PH_JAVA_AGENT_ORADB_PERF_CONN_ERROR	1811
EventType: PH_JAVA_AGENT_ORADB_PERF_EXEC_ERROR	1811
EventType: PH_JAVA_AGENT_SNORT_CONN_ERROR	1811
EventType: PH_JAVA_AGENT_SNORT_EVENTID_ERROR	1812
EventType: PH_JAVA_AGENT_SNORT_EXEC_ERROR	1812
EventType: PH_JAVA_AGENT_SNORT_SENSORID_ERROR	1812
EventType: PH_JAVA_AGENT_SNORT_TCP_OPTION_ERROR	1812
EventType: PH_JAVA_AGENT_TOMCAT_MONITOR_ERROR	1812
EventType: PH_JAVA_AGENT_UTILS_ERROR	1813
EventType: PH_JAVA_AGENT_VMWARE_HWSTATUS_EXEC_ERROR	1813
EventType: PH_JAVA_AGENT_VMWARE_LOG_CONN_ERROR	1813
EventType: PH_JAVA_AGENT_VMWARE_LOG_EXEC_ERROR	1813
EventType: PH_JAVA_AGENT_VMWARE_MONITOR_ERROR	1813
EventType: PH_JAVA_AGENT_VMWARE_PERF_COUNTER_MISSING	1813
EventType: PH_JAVA_AGENT_VMWARE_PERF_DATA_RETRIEVE_ERROR	1814
EventType: PH_JAVA_AGENT_VMWARE_PERF_ENTITY_MISSING	1814
EventType: PH_JAVA_AGENT_VMWARE_PERF_HOST_MISSING	1814
EventType: PH_JAVA_AGENT_VMWARE_PERF_MON_EXCEPTION	1814
EventType: PH_JAVA_AGENT_VMWARE_PERF_ROLLUP_MISSING	1814
EventType: PH_JAVA_AGENT_VMWARE_PERF_STAT_NAME_MISSING	1815
EventType: PH_JAVA_AGENT_VMWARE_PERF_VM_MISSING	1815
EventType: PH_JAVA_AGENT_VMWARE_THREAD_EXEC_ERROR	1815
EventType: PH_JAVA_AGENT_VULN_REPORT_PARSER_ERROR	1815
EventType: PH_JAVA_AGENT_VULN_REPORT_VERIFY_ERROR	1815
EventType: PH_JAVA_AGENT_WEBLOGIC_MONITOR_ERROR	1815
EventType: PH_JAVA_AGENT_WEBSENSE_EMAIL_MISSING_LOGDB	1816
EventType: PH_JAVA_AGENT_WEBSENSE_JDBC_PULL_ERROR	1816
EventType: PH_JAVA_AGENT_WEBSENSE_MAIL_CONN_ERROR	1816

EventType: PH_JAVA_AGENT_WEBSSENSE_MAIL_EXEC_ERROR	1816
All Logs Page 4	1817
EventType: PH_JAVA_AGENT_WEBSSENSE_MAIL_PULL_ERROR	1830
EventType: PH_JAVA_AGENT_WEBSSENSE_WEB_CONN_ERROR	1830
EventType: PH_JAVA_AGENT_WEBSSENSE_WEB_EXEC_ERROR	1830
EventType: PH_JAVA_AGENT_WEBSSENSE_WEB_MISSING_LOGDB	1830
EventType: PH_JAVA_AGENT_WEBSPHERE_CONN_ERROR	1830
EventType: PH_JAVA_AGENT_WEBSPHERE_EXEC_ERROR	1831
EventType: PH_JAVA_AGENT_WEBSPHERE_MONITOR_ERROR	1831
EventType: PH_JAVA_QUERYSERVER_ACTION_UNSUPPORTED_ERROR	1831
EventType: PH_JAVA_QUERYSERVER_ELASTIC_ERROR	1831
EventType: PH_JAVA_QUERYSERVER_ERROR	1831
EventType: PH_JAVA_QUERYSERVER_INFO	1832
EventType: PH_JAVA_QUERYSERVER_QUERYID_ERROR	1832
EventType: PH_JAVA_QUERYSERVER_QUERY_SYNTAX_ERROR	1832
EventType: PH_JAVA_QUERYSERVER_REDIS_ERROR	1832
EventType: PH_JAVA_QUERYSERVER_WARN	1832
EventType: PH_JMS_QUEUE_SIZE_WARNING	1832
EventType: PH_JOB_STAT	1833
EventType: PH_JOB_STATUS_XML_SEND_ERROR	1833
EventType: PH_JOB_STATUS_XML_SENT	1833
EventType: PH_JOB_STAT_SUPPRESSED	1834
EventType: PH_LIBEVENT_BUFFER_OVERFLOW	1834
EventType: PH_LIBEVENT_IP_TYPE_INVALID	1834
EventType: PH_LIBEVENT_UNKNOWN_ATTR_ID	1835
EventType: PH_LIBEVENT_UNKNOWN_ATTR_NAME	1835
EventType: PH_LIB_TOPO_APACHE_PING_FAILED	1835
EventType: PH_LIB_TOPO_APP_GROUP_FILTER_PARSE_ERROR	1835
EventType: PH_LIB_TOPO_APP_GROUP_FILTER_PUSH_ERROR	1835
EventType: PH_LIB_TOPO_AWS_NEW_INSTANCE_NOT_RUN	1836
EventType: PH_LIB_TOPO_AWS_OBTAIN_INSTANCE_FAILURE	1836
EventType: PH_LIB_TOPO_CHECK_APP_LIST_WARNING	1836
EventType: PH_LIB_TOPO_CISCO_IOS_CBQOS_ERROR	1836
EventType: PH_LIB_TOPO_CISCO_MERAKI_GET_CHILD_DEVICE_WARNING	1837
EventType: PH_LIB_TOPO_CISCO_MERAKI_GET_INTFS_WARNING	1837
EventType: PH_LIB_TOPO_CISCO_MERAKI_GET_INTF_WARNING	1838
EventType: PH_LIB_TOPO_CISCO_MERAKI_MAC_2_HOST_LOOKUP_FAILED	1838
EventType: PH_LIB_TOPO_CISCO_MERAKI_MAC_2_INTF_LOOKUP_FAILED	1838
EventType: PH_LIB_TOPO_CISCO_UCS_LOGIN_FAILED	1839
EventType: PH_LIB_TOPO_CISCO_UCS_REQUEST_ERROR	1839
EventType: PH_LIB_TOPO_CPU_TOO_HIGH	1839
EventType: PH_LIB_TOPO_CUST_CONFIG_JOB_DOWNLOAD_SCRIPT_	
FAILED	1840
EventType: PH_LIB_TOPO_CUST_FIM_JOB_CHECK_PATH_ERROR	1840
EventType: PH_LIB_TOPO_CUST_FIM_JOB_DEVICE_UNAVAILABLE	1840
EventType: PH_LIB_TOPO_CUST_FIM_JOB_FILE_TOO_LARGE	1841
EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_DATA_FAILED	1841
EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_FILE_INFO_FAILED	1842
EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_MD5_FAILED	1842

EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_REMOTE_FILE_ERROR	1842
EventType: PH_LIB_TOPO_CUST_FIM_JOB_INCORRECT_CRED	1843
EventType: PH_LIB_TOPO_CUST_FIM_JOB_RUN_SCP_FAILED	1843
EventType: PH_LIB_TOPO_CUST_FIM_JOB_TOO_MANY_FILES	1844
EventType: PH_LIB_TOPO_CUST_LOGIN_JOB_CREATE_EVENT_FAILED	1844
EventType: PH_LIB_TOPO_CUST_LOGIN_JOB_GET_DATA_FAILED	1844
EventType: PH_LIB_TOPO_CUST_SNMP_JOB_CREATE_EVENT_FAILED	1845
EventType: PH_LIB_TOPO_CUST_SNMP_JOB_GET_DATA_FAILED	1845
EventType: PH_LIB_TOPO_CUST_WMI_JOB_CREATE_EVENT_FAILED	1845
EventType: PH_LIB_TOPO_CUST_WMI_JOB_GET_DATA_FAILED	1846
EventType: PH_LIB_TOPO_ETHERMIB_STAT_LOOKUP_ERROR	1846
EventType: PH_LIB_TOPO_EVENT_DROP_RULE_ENCODE_VALUE_GROUP_ERROR	1847
EventType: PH_LIB_TOPO_EVENT_DROP_RULE_PARSE_ERROR	1847
EventType: PH_LIB_TOPO_EXCLUDED_DISK_PARSE_ERROR	1847
EventType: PH_LIB_TOPO_FCT_DEV_MAPPING_ENTRY_INVALID	1848
EventType: PH_LIB_TOPO_FGT_FABRIC_DISCOV_FAIL	1848
EventType: PH_LIB_TOPO_FGT_GET_CONFIG_BACKUP_FAILED	1848
EventType: PH_LIB_TOPO_FGT_GET_USER_DEV_STORE_FAIL	1848
EventType: PH_LIB_TOPO_FGT_GET_USER_DEV_UNKNOWN	1849
EventType: PH_LIB_TOPO_FGT_INSTALLED_SW_FAIL	1849
EventType: PH_LIB_TOPO_FGT_SEC_POSTURE_RPT_API_FAIL	1849
EventType: PH_LIB_TOPO_FILE_READ_ERROR	1849
EventType: PH_LIB_TOPO_FOUNDRY_HW_STATUS_ERROR	1849
EventType: PH_LIB_TOPO_GEN_UPS_STATUS_GET_ERROR	1850
EventType: PH_LIB_TOPO_GET_NETAPP_NFS_FAILED	1850
EventType: PH_LIB_TOPO_H3C_CPU_UTIL_ERROR	1851
EventType: PH_LIB_TOPO_HP3COM_CPU_UTIL_ERROR	1851
EventType: PH_LIB_TOPO_HP3COM_MEM_UTIL_ERROR	1851
EventType: PH_LIB_TOPO_HPUX_PROC_CPU_MEM_TOO_HIGH	1852
EventType: PH_LIB_TOPO_HYPERV_METRICS_GET_ERROR	1852
EventType: PH_LIB_TOPO_IMPORTANT_INTF_PARSE_ERROR	1853
EventType: PH_LIB_TOPO_INTF_UTIL_ERROR	1853
EventType: PH_LIB_TOPO_JSON_PARSE_FAILED	1853
EventType: PH_LIB_TOPO_JUNIPER_INTF_SPEED_GET_ERROR	1853
EventType: PH_LIB_TOPO_LIEBERT_HVAC_STATUS_GET_ERROR	1854
EventType: PH_LIB_TOPO_LOGIN_PING_FAILED	1854
EventType: PH_LIB_TOPO_MAINTENANCE_DURATION_INCORRECT	1855
EventType: PH_LIB_TOPO_MEM_TOO_HIGH	1855
EventType: PH_LIB_TOPO_NETAPP_AGGREGATE_STAT_ERROR	1855
EventType: PH_LIB_TOPO_NETAPP_ANALYZE_VERSION_ERROR	1856
EventType: PH_LIB_TOPO_NETAPP_DISK_STAT_ERROR	1856
EventType: PH_LIB_TOPO_NETAPP_GET_NFS_METRIC_ERROR	1856
EventType: PH_LIB_TOPO_NETAPP_GET_VERSION_ERROR	1857
EventType: PH_LIB_TOPO_NETAPP_LUN_STAT_ERROR	1857
EventType: PH_LIB_TOPO_NETAPP_PROTO_STAT_ERROR	1857
EventType: PH_LIB_TOPO_NETAPP_VOLUME_STAT_ERROR	1858
EventType: PH_LIB_TOPO_NOT_SUPPORT_REST_API	1858
EventType: PH_LIB_TOPO_OPEN_FILE_FAILED	1858

EventType: PH_LIB_TOPO_PARSE_INTF_MAP_FAILURE	1859
EventType: PH_LIB_TOPO_PERF_JOB_EXEC_FAILED	1859
EventType: PH_LIB_TOPO_PERF_JOB_INIT_FAILED	1859
EventType: PH_LIB_TOPO_PERF_JOB_REMOVE_FAILED	1860
EventType: PH_LIB_TOPO_PERF_TEMPLATE_LOAD_ERROR	1860
EventType: PH_LIB_TOPO_PERF_TEMPLATE_PARSE_FAILURE	1860
EventType: PH_LIB_TOPO_PERF_TEMPLATE_PARSE_WARNING	1861
EventType: PH_LIB_TOPO_PORT_FILTER_PARSE_ERROR	1861
EventType: PH_LIB_TOPO_PORT_FILTER_PUSH_ERROR	1861
EventType: PH_LIB_TOPO_PROC_CPU_MEM_TOO_HIGH	1861
EventType: PH_LIB_TOPO_REST_API_FAILED	1862
EventType: PH_LIB_TOPO_RUN_SW_FILTER_PARSE_ERROR	1862
EventType: PH_LIB_TOPO_RUN_SW_FILTER_PUSH_ERROR	1862
EventType: PH_LIB_TOPO_SNMPWALK_ERROR	1862
EventType: PH_LIB_TOPO_STM_JOB_EXEC_FAILED	1863
EventType: PH_LIB_TOPO_STM_JOB_INIT_FAILED	1863
EventType: PH_LIB_TOPO_TEST_CONN_HTTP_AGENT_FAILED	1864
EventType: PH_LIB_TOPO_TEST_CONN_JDBC_AGENT_FAILED	1864
EventType: PH_LIB_TOPO_TEST_CONN_JMX_AGENT_FAILED	1864
EventType: PH_LIB_TOPO_TRUNK_PORT_MAP_PARSE_ERROR	1865
EventType: PH_LIB_TOPO_VALIDATE_ACCESS_FAILED	1865
EventType: PH_LIB_TOPO_WIN_GET_EXCH_DATABASE_INSTANCE_	
WARNING	1865
EventType: PH_LIB_TOPO_WIN_GET_EXCH_DATABASE_WARNING	1866
EventType: PH_LIB_TOPO_WIN_GET_EXCH_MAIL_SUBMISSION_WARNING	1866
EventType: PH_LIB_TOPO_WIN_GET_EXCH_PUB_MAILBOX_WARNING	1866
EventType: PH_LIB_TOPO_WIN_GET_EXCH_REG_MAILBOX_WARNING	1867
EventType: PH_LIB_TOPO_WIN_GET_EXCH_REPLICATION_WARNING	1867
EventType: PH_LIB_TOPO_WIN_GET_EXCH_RPC_WARNING	1867
EventType: PH_LIB_TOPO_WIN_GET_EXCH_SMTP_WARNING	1868
EventType: PH_LIB_TOPO_WIN_GET_EXCH_STORE_INTF_WARNING	1868
EventType: PH_LIB_TOPO_WIN_GET_EXCH_TRANSPORT_QUEUE_	
WARNING	1869
EventType: PH_LIB_TOPO_WMI_GET_CPU_COUNT_ERROR	1869
EventType: PH_LIB_TOPO_WMI_GET_CPU_WARNING	1869
EventType: PH_LIB_TOPO_WMI_GET_PAGE_ACTIVITY_ERROR	1870
EventType: PH_LIB_TOPO_WMI_GET_REAL_MEM_ERROR	1870
EventType: PH_LIB_TOPO_WMI_GET_RUN_SW_PERF_ERROR	1870
EventType: PH_LICENSE_ERROR	1871
EventType: PH_LICENSE_INFO_FAILURE	1871
EventType: PH_LICENSE_INFO_INVALIDATED	1871
EventType: PH_LICENSE_NOT_EXIST	1872
EventType: PH_LINUX_AGENT_ACCOUT_MISSING	1872
EventType: PH_LINUX_AGENT_BIND_PORT_FAILED	1872
EventType: PH_LINUX_AGENT_CONFIG_ATTR_DECRYPTED_FAILED	1872
EventType: PH_LINUX_AGENT_CONFIG_ATTR_ENCRYPTED_FAILED	1873
EventType: PH_LINUX_AGENT_CONFIG_ATTR_NOT_FOUND	1873
EventType: PH_LINUX_AGENT_CONFIG_MISS_ATTR	1873
EventType: PH_LINUX_AGENT_CREATE_SOCKET_FAILED	1873

EventType: PH_LINUX_AGENT_EXIT	1874
EventType: PH_LINUX_AGENT_HOST_IP_GOT_FAILED	1874
EventType: PH_LINUX_AGENT_INCREASE_RECV SOCK_BUF_MAX_FAILED	1874
EventType: PH_LINUX_AGENT_INIT_FIM_FAILED	1874
EventType: PH_LINUX_AGENT_INIT_HTTP_FAILED	1875
EventType: PH_LINUX_AGENT_LOG_GENERIC	1875
EventType: PH_LINUX_AGENT_NEW_FIM_LOADED	1875
EventType: PH_LINUX_AGENT_OPEN_FILE_FAILED	1875
EventType: PH_LINUX_AGENT_OPEN_PORT_FAILED	1876
EventType: PH_LINUX_AGENT_PWD_MISSING	1876
EventType: PH_LINUX_AGENT_RECV_ERROR	1876
EventType: PH_LINUX_AGENT_REGISSTER_FAILED	1877
EventType: PH_LINUX_AGENT_TEMPLATE_STATUS	1877
EventType: PH_LINUX_AGENT_UNINSTALL	1877
EventType: PH_LINUX_AGENT_UPLOAD_FILE_FAILED	1877
EventType: PH_LINUX_AGENT_UPLOAD_FILE_SUCCESS	1878
EventType: PH_LINUX_AGENT_USER_FILE_LOG_GENERIC	1878
EventType: PH_LINUX_AGENT_VERIFIER_ERROR	1878
EventType: PH_LOAD_CONFIG_CHANGE_FAILED	1879
EventType: PH_LOOKUP_TABLE_CANNOT_LOAD_DATA	1879
EventType: PH_MAX_DEVICES_EXCEEDED	1879
EventType: PH_MAX_DEVICES_LIMIT_REACHED	1879
EventType: PH_ML_ANOMALY_DETECTED	1880
EventType: PH_MODULE_ABORT	1880
EventType: PH_MODULE_ABORT_FOUND	1880
EventType: PH_MODULE_ACCEPTED_CONN	1880
EventType: PH_MODULE_ACE_ACCEPTOR_FAILED	1881
EventType: PH_MODULE_ACE_HANDLE_EVENT_ERROR	1881
EventType: PH_MODULE_COMM_ERROR	1881
EventType: PH_MODULE_COMM_HANDLER_REG	1881
EventType: PH_MODULE_COMM_PORTS_OPENED	1882
EventType: PH_MODULE_DB_CONFIG_LOADED	1882
EventType: PH_MODULE_DIODE_CONFIG_ERROR	1882
EventType: PH_MODULE_EXCEPTION_NOT_CAUGHT	1883
EventType: PH_MODULE_EXITING	1883
EventType: PH_MODULE_EXIT_OK	1883
EventType: PH_MODULE_HEARTBEAT_INIT	1883
EventType: PH_MODULE_INITIALIZING	1883
EventType: PH_MODULE_INIT_COMPLETE	1884
EventType: PH_MODULE_INIT_FAILURE	1884
EventType: PH_MODULE_LICENSE_FAILURE	1884
EventType: PH_MODULE_LOADED_NEW_CONFIG	1884
EventType: PH_MODULE_LOAD_DIODE_CRED_ERROR	1884
EventType: PH_MODULE_LOCAL_CONFIG_LOADED	1885
EventType: PH_MODULE_LOCAL_CONFIG_SECTION_ERROR	1885
EventType: PH_MODULE_LOCAL_CONFIG_VALUE_ERROR	1885
EventType: PH_MODULE_LOG_LEVEL_CHANGE	1886
EventType: PH_MODULE_RECVD_EXIT_EXT	1886
EventType: PH_MODULE_RECVD_EXIT_MONITOR	1886

EventType: PH_MODULE_RECVD_NEW_CONFIG	1887
EventType: PH_MODULE_RECVD_START	1887
EventType: PH_MODULE_SETPIDFILE_ERR	1887
EventType: PH_MODULE_UNABLE_INIT_SHARED_STORE	1887
EventType: PH_MODULE_UNABLE_OPEN_COMM_PORT	1887
EventType: PH_MONITOR_ARCHIVE_GET_WORKER_FAILURE	1888
EventType: PH_MONITOR_ARCHIVE_UPDATE_WORKER_FAILURE	1888
EventType: PH_MONITOR_BEACONING_REGISTER_FAILURE	1888
EventType: PH_MONITOR_CHECK_DEPENDENCY_FAILED	1889
EventType: PH_MONITOR_CMD_FAILURE	1889
EventType: PH_MONITOR_CMD_SEND_FAILURE	1889
EventType: PH_MONITOR_COLLECTOR_REGISTER_FAILURE	1890
EventType: PH_MONITOR_COLLECTOR_UPDATE_STATUS_FAILURE	1890
EventType: PH_MONITOR_CONFIG_DOWNLOAD_FAILURE	1890
EventType: PH_MONITOR_DBCLUSTER_SEND_COMMAND_FAILED	1890
EventType: PH_MONITOR_DELETE_DR_FAILED	1891
EventType: PH_MONITOR_DELETE_SECONDARY_ON_WORKER_FAILED	1891
EventType: PH_MONITOR_DELETE_SUPER_FOLLOWER_FAILED	1891
EventType: PH_MONITOR_DISPATCH_CMD_MISMATCH	1891
EventType: PH_MONITOR_DOMAIN_CHANGE_XML_PARSE_FAILURE	1892
EventType: PH_MONITOR_ENT_OR_SP_MODE_MISSING	1892
EventType: PH_MONITOR_EXCESSIVE_DB_LOGIN_FAILURE	1892
EventType: PH_MONITOR_FAILED_CONN_QUERYMASTER	1892
EventType: PH_MONITOR_FILE_IO_ERROR	1892
EventType: PH_MONITOR_FILE_PERMISSION_ERROR	1893
EventType: PH_MONITOR_FILE_PERMISSION_WARNING	1893
EventType: PH_MONITOR_FLIP_PRIMARY_FAILURE	1893
EventType: PH_MONITOR_FSM_AGENT_UPDATE_PWD_ERROR	1894
EventType: PH_MONITOR_GET_REPLICATION_PROGRESS_FAILED	1894
EventType: PH_MONITOR_GET_UPTIME_ERROR	1894
EventType: PH_MONITOR_HANDLE_TASK	1894
EventType: PH_MONITOR_HARDWARE_SN_FORK_FAILURE	1895
EventType: PH_MONITOR_HOST_UUID_READ_FAILURE	1895
EventType: PH_MONITOR_HTTP_PULL_ERROR	1895
EventType: PH_MONITOR_INIT_PROC_MODULE_NOT_FOUND	1895
EventType: PH_MONITOR_INIT_SECONDARY_ON_WORKER_FAILED	1896
EventType: PH_MONITOR_INIT_SUPER_FOLLOWER_FAILED	1896
EventType: PH_MONITOR_INIT_SYSTEM_XML_PARSE_FAILURE	1896
EventType: PH_MONITOR_JDBC_POOL_NOT_EXIST	1897
EventType: PH_MONITOR_LIB_DEPENDENCY_WARNING	1897
EventType: PH_MONITOR_LICENSE_ERROR	1897
EventType: PH_MONITOR_LOAD_CONF_FROM_APP_SERVER_FAILED	1897
EventType: PH_MONITOR_LOCAL_HOSTNAME_GET_FAILURE	1898
EventType: PH_MONITOR_MEM_FILE_OPEN_FAILURE	1898
EventType: PH_MONITOR_MISSING_MONITOR	1898
EventType: PH_MONITOR_MMAP_FAILURE	1898
EventType: PH_MONITOR_MOTNIROR_REGISTER_FAILURE	1899
EventType: PH_MONITOR_NOTIFICATION_CLIENT_CONTACT_FAILURE	1899
EventType: PH_MONITOR_NOTIFICATION_CMD_EMPTY	1899

EventType: PH_MONITOR_NOTIFICATION_CMD_MISMATCH	1899
EventType: PH_MONITOR_NOTIFICATION_RETURN_FAILURE	1900
EventType: PH_MONITOR_PHOENIX_CONFIG_GLOBAL_MISSING	1900
EventType: PH_MONITOR_PHOENIX_CONFIG_INVALID	1900
EventType: PH_MONITOR_PROCESS_OWNER_NOT_ADMIN_ERROR	1900
EventType: PH_MONITOR_QUERY_LICENSE_FAILED	1901
EventType: PH_MONITOR_RECVD_CONFIG_CHANGE	1901
EventType: PH_MONITOR_RECVD_HEARTBEAT	1901
EventType: PH_MONITOR_REDIS_UPDATE_FAILED	1901
EventType: PH_MONITOR_REGISTER_MONITOR_GET_WORKER_FAILURE ..	1902
EventType: PH_MONITOR_REGISTER_NODE	1902
EventType: PH_MONITOR_REGISTER_SUPER_FOLLOWER	1902
EventType: PH_MONITOR_REGISTER_WORKER	1902
EventType: PH_MONITOR_REMOVE_NODE	1903
EventType: PH_MONITOR_REMOVE_SUPER_FOLLOWER	1903
EventType: PH_MONITOR_REMOVE_WORKER	1903
EventType: PH_MONITOR_REPORTSERVER_LICENSE_INVALID	1903
EventType: PH_MONITOR_REPORTSERVER_NOTIFICATION_CLIENT_	
CONTACT_FAILURE	1903
EventType: PH_MONITOR_REPORTSERVER_NOTIFICATION_CLIENT_INIT_	
FAILURE	1904
EventType: PH_MONITOR_REPORTSERVER_NOTIFICATION_SERVER_	
RETURN_FAILURE	1904
EventType: PH_MONITOR_RESET_DB_SERVER_NAME_FAILED	1904
EventType: PH_MONITOR_RESET_JDBC_CONN_FAILED	1905
EventType: PH_MONITOR_RESET_STORAGE_CONFIG_FAILED	1905
EventType: PH_MONITOR_RESTART_MODULES	1905
EventType: PH_MONITOR_REST_CACHE_REQUEST_EMPTY	1905
EventType: PH_MONITOR_REST_CACHE_REQUEST_FAILURE	1905
EventType: PH_MONITOR_REST_CACHE_REQUEST_FORMAT_ILLEGAL	1906
EventType: PH_MONITOR_REST_CACHE_SERVER_INIT_FAILURE	1906
EventType: PH_MONITOR_REST_CALL_FAILURE	1906
EventType: PH_MONITOR_ROLE_UNDEFINED	1907
EventType: PH_MONITOR_SAVE_DR_CONFIG_FAILED	1907
EventType: PH_MONITOR_SEND_CMD_TO_MODULE	1907
EventType: PH_MONITOR_SEND_VG_UPDATE_CMD_TO_MODULE	1907
EventType: PH_MONITOR_SETUID_FAILURE	1908
EventType: PH_MONITOR_START_MODULE	1908
EventType: PH_MONITOR_START_MODULES	1908
EventType: PH_MONITOR_STATFS_FAILURE	1909
EventType: PH_MONITOR_STATUS_PUSHER_SPAWN_FAILURE	1909
EventType: PH_MONITOR_STOP_MODULES	1909
EventType: PH_MONITOR_STOP_READER	1909
EventType: PH_MONITOR_STORAGE_ES_CUSTOMIZED_TEMPLATE_	
DEPLOYED	1910
EventType: PH_MONITOR_STORAGE_GET_WORKER_FAILURE	1910
EventType: PH_MONITOR_STORAGE_LOCAL_GET_FAILURE	1910
EventType: PH_MONITOR_STORAGE_NFS_GET_FAILURE	1910
EventType: PH_MONITOR_STORAGE_TYPE_GET_FAILURE	1910

EventType: PH_MONITOR_STORAGE_TYPE_UNKNOWN	1911
EventType: PH_MONITOR_STORAGE_UPDATE_WORKER_FAILURE	1911
EventType: PH_MONITOR_SVC_PASSWORD_DISTRIBUTION_ERROR	1911
EventType: PH_MONITOR_SYSINFO_FAILURE	1911
EventType: PH_MONITOR_SYSTEM_DB_LOGIN_ERROR	1912
EventType: PH_MONITOR_SYSTEM_HEALTH_CPU	1912
EventType: PH_MONITOR_SYSTEM_HEALTH_ISSUE	1912
EventType: PH_MONITOR_SYSTEM_HEALTH_MEM	1913
EventType: PH_MONITOR_SYSTEM_STATUS_SPAWN_FAILURE	1913
EventType: PH_MONITOR_THREAD_SPAWN_FAILED	1913
EventType: PH_MONITOR_TUNNEL_ERROR	1913
EventType: PH_MONITOR_UMOUNT_NFS_FAILURE	1914
EventType: PH_MONITOR_UNABLE_CONTACT_APPSVR	1914
EventType: PH_MONITOR_UPDATE_DATA_FAILED	1914
EventType: PH_MONITOR_UPDATE_DR_FAILED	1915
EventType: PH_MONITOR_UPDATE_WORKER_INFO_FAILED	1915
EventType: PH_MONITOR_UPLOAD_LOG_SPAWN_FAILURE	1915
EventType: PH_MONITOR_WINAGENT_DELETE_PWD_SPAWN_FAILURE	1915
EventType: PH_MONITOR_WINAGENT_UPDATE_PWD_ERROR	1915
EventType: PH_MONITOR_WIN_LINUX_AGENT_PWD_UPDATE_SUCCESS	1916
EventType: PH_MONITOR_WORKER_NODECONFIG_UPDATE_FAILED	1916
EventType: PH_MONITOR_WORKER_REDIS_ADDSLAVE_UPDATE_FAILED	1916
EventType: PH_MONITOR_WORKER_REDIS_CONF_UPDATE_FAILED	1916
EventType: PH_NETFLOW_BAD_FLOW	1916
EventType: PH_NETFLOW_BAD_FLOW_END	1917
EventType: PH_NETFLOW_BAD_HEADER_PROTOCOL	1917
EventType: PH_NETFLOW_BAD_PACKET	1917
EventType: PH_NETFLOW_BAD_RECORD	1917
EventType: PH_NETFLOW_BAD_TYPE	1917
EventType: PH_NETFLOW_BAD_VER	1918
EventType: PH_NETFLOW_EXCEPTION	1918
EventType: PH_NOTIFICATION_ACCEPT_FAILURE	1918
EventType: PH_NOTIFICATION_CALLBACK_ERROR	1918
EventType: PH_NOTIFICATION_CONN_FAILED	1918
EventType: PH_NOTIFICATION_INIT_FAILED	1919
EventType: PH_NOTIFICATION_NO_RESPONSE	1919
EventType: PH_NOTIFICATION_RETURN_FAILURE	1919
EventType: PH_NOTIFICATION_SEND_FAILURE	1919
EventType: PH_NOTIFICATION_SEND_FILE_FAILURE	1920
EventType: PH_NO_PARSER_FOR_EVENT	1920
EventType: PH_OBJECT_NOT_FOUND	1920
EventType: PH_PARSER_BIND_PORT_FAILURE	1921
EventType: PH_PARSER_DATA_SIZE_OVERFLOW	1921
EventType: PH_PARSER_DIR_OPEN_FAILURE	1921
EventType: PH_PARSER_EVENT_PARSER_ERROR	1921
EventType: PH_PARSER_EVENT_SERIALIZE_ERROR	1922
EventType: PH_PARSER_FILE_DELETE_FAILURE	1922
EventType: PH_PARSER_FILE_DELETE_FAILURE_RENAME	1922
EventType: PH_PARSER_FILE_INVALID_FORMAT	1923

EventType: PH_PARSER_FILE_INVALID_HEADER	1923
EventType: PH_PARSER_FILE_NOT_EXIST	1923
EventType: PH_PARSER_FILE_OPEN_FAILURE	1924
EventType: PH_PARSER_FILE_PARSE_FAILURE	1924
EventType: PH_PARSER_FILE_READ_FAILURE	1924
EventType: PH_PARSER_FILE_RENAME_FAILURE	1925
EventType: PH_PARSER_FILE_SIZE_MISMATCH	1925
EventType: PH_PARSER_FILE_STAT_FAILURE	1925
EventType: PH_PARSER_FILE_WRITE_FAILURE	1926
EventType: PH_PARSER_GEO_WRONG_ATTR_NUMBER	1926
EventType: PH_PARSER_GEO_WRONG_CACHE_NUMBER	1926
EventType: PH_PARSER_GET_PROCESS_ERROR	1926
EventType: PH_PARSER_GLOBAL_LICENSE_EXCEED	1926
EventType: PH_PARSER_HTTP_RESPONSE_ERROR	1927
EventType: PH_PARSER_HTTP_UPLOAD_FAILURE	1927
EventType: PH_PARSER_INIT_DEV_CRED_FAILED	1927
EventType: PH_PARSER_INIT_FAILURE	1928
EventType: PH_PARSER_INVALID_CSV	1928
EventType: PH_PARSER_INVALID_EXT_LOG_PROTO	1928
EventType: PH_PARSER_INVALID_ORG_NAME	1928
EventType: PH_PARSER_INVALID_PHOENIX_CONFIG	1929
EventType: PH_PARSER_IP_TYPE_INVALID	1929
EventType: PH_PARSER_JSON_PARSE_FAILURE	1929
EventType: PH_PARSER_MALLOC_FAILURE	1930
EventType: PH_PARSER_PACK_EVENT_ERROR	1930
EventType: PH_PARSER_RAWEVENT_TOO_LARGER	1930
EventType: PH_PARSER_REST_PARSE_ERROR	1930
EventType: PH_PARSER_RUN_PROCESS_ERROR	1931
EventType: PH_PARSER_SEND_EVENT_FAILURE	1931
EventType: PH_PARSER_SEND_TO_DISCOV_FAILURE	1931
EventType: PH_PARSER_SEND_TO_MONITOR_FAILURE	1931
EventType: PH_PARSER_SET_USER_ID_FAILURE	1931
EventType: PH_PARSER_SHARED_STORE_ERROR	1931
EventType: PH_PARSER_SNMPTRAP_INIT_FAILURE	1932
EventType: PH_PARSER_SOCKET_ERROR	1932
EventType: PH_PARSER_SOCKET_RECV_ERROR	1932
EventType: PH_PARSER_SOCKET_SELECT_ERROR	1933
EventType: PH_PARSER_SPAWN_THREAD_FAILURE	1933
EventType: PH_PARSER_SSL_ACCEPT_ERROR	1933
EventType: PH_PARSER_SSL_CERT_LOAD_ERROR	1934
EventType: PH_PARSER_TCP_SOCKET_ACCEPT_ERROR	1934
EventType: PH_PARSER_TEST_RULES_PARSE_ALL_EVENTS_BEGIN	1934
EventType: PH_PARSER_TEST_RULES_PARSE_ALL_EVENTS_END	1934
EventType: PH_PARSER_TEST_RULES_PARSE_ONE_EVENT_BEGIN	1935
EventType: PH_PARSER_TEST_RULES_PARSE_ONE_EVENT_END	1935
EventType: PH_PARSER_TOO_MANY_UNKNOWN_EVENTS	1935
EventType: PH_PARSER_UPDATE_FAILURE	1936
EventType: PH_PARSER_USE_ERROR_BEFORE_INIT	1936
EventType: PH_PARSER_WRONG_EVENT_SIZE	1937

EventType: PH_PARSER_WRONG_PARAMETER	1937
EventType: PH_PARSER_WTAP_ERR_BAD_FILE	1937
EventType: PH_PARSER_WTAP_ERR_CANT_OPEN	1937
EventType: PH_PARSER_WTAP_ERR_COMPRESSION_NOT_SUPPORTED	1938
EventType: PH_PARSER_WTAP_ERR_DECOMPRESS	1938
EventType: PH_PARSER_WTAP_ERR_ENCAP_PER_PACKET_	
UNSUPPORTED	1938
EventType: PH_PARSER_WTAP_ERR_FILE_UNKNOWN_FORMAT	1939
EventType: PH_PARSER_WTAP_ERR_NOT_REGULAR_FILE	1939
EventType: PH_PARSER_WTAP_ERR_RANDOM_OPEN_PIPE	1939
EventType: PH_PARSER_WTAP_ERR_SHORT_READ	1940
EventType: PH_PARSER_WTAP_ERR_SHORT_WRITE	1940
EventType: PH_PARSER_WTAP_ERR_UNSUPPORTED	1940
EventType: PH_PARSER_XML_PARSE_ERROR	1941
EventType: PH_PARSER_XML_PARSE_FAILURE	1941
EventType: PH_PARSE_CONFIG_CHANGE_FAILED	1941
EventType: PH_PDF_BUILDER_ERROR	1942
EventType: PH_PERFMON_COMMIT_FILE_FAILED	1942
EventType: PH_PERFMON_CONFIG_SEND_FAILED	1942
EventType: PH_PERFMON_CONFIG_VERSION_ERROR	1943
EventType: PH_PERFMON_CONFIG_VERSION_WARNING	1943
EventType: PH_PERFMON_CUST_JOB_ADD_FAILED	1943
EventType: PH_PERFMON_INIT_ERROR	1943
EventType: PH_PERFMON_INST_SW_MAP_EMPTY	1944
EventType: PH_PERFMON_INST_SW_NO_NAME	1944
EventType: PH_PERFMON_JOB_ADD_FAILED	1944
EventType: PH_PERFMON_MASS_PING_WARNING	1944
EventType: PH_PERFMON_MONITEE_BAD	1944
EventType: PH_PERFMON_MONITEE_NOT_FOUND	1944
EventType: PH_PERFMON_NO_DEV_TYPE	1945
EventType: PH_PERFMON_PERF_OBJ_PARSE_FAILURE	1945
EventType: PH_PERFMON_PING_RESULT_OPEN_FAILED	1945
EventType: PH_PERFMON_PROC_RUN_FAILED	1945
EventType: PH_PERFMON_REAL_TIME_JOB_RUN_FAILED	1945
EventType: PH_PERFMON_ROUTE_LOAD_ERROR	1946
EventType: PH_PERFMON_STATUS_REPORTER_INIT_FAILED	1946
EventType: PH_PERFMON_STATUS_REPORT_FAILED	1946
EventType: PH_PERFMON_SVN_CHECKOUT_FAILED	1946
EventType: PH_PERFMON_SVN_CONFIG_MISSING	1947
EventType: PH_PERFMON_SVN_DIR_CREATE_FAILED	1947
EventType: PH_PERFMON_SVN_DIR_UPDATE_FAILED	1947
EventType: PH_PERFMON_SVN_FILE_COPY_FAILED	1948
EventType: PH_PERFMON_SVN_FILE_EMPTY	1948
EventType: PH_PERFMON_SVN_FILE_MARK_FAILED	1948
EventType: PH_PERFMON_SVN_FILE_OPEN_FAILED	1949
EventType: PH_PERFMON_SVN_FILE_PARSE_FAILED	1949
EventType: PH_PERFMON_SVN_FILE_REMOVE_FAILED	1949
EventType: PH_PERFMON_SVN_FILE_RENAME_FAILED	1950
EventType: PH_PERFMON_SVN_FIM_FILE_MISSING	1950

EventType: PH_PERFMON_SVN_FIRSTFILELINES_EMPTY	1950
EventType: PH_PERFMON_SVN_FIRSTFILELINES_NOT_IN_FILE	1950
EventType: PH_PERFMON_SVN_GET_DEVICE_ID_FAILED	1951
EventType: PH_PERFMON_SVN_GET_DISCOV_TIME_FAILED	1951
EventType: PH_PERFMON_SVN_INFO_GET_FAILED	1951
EventType: PH_PERFMON_SVN_INST_SW_BAD	1952
EventType: PH_PERFMON_SVN_INVALID_FILE_FORMAT	1952
EventType: PH_PERFMON_SVN_INVALID_HEADER_IN_FILE	1952
EventType: PH_PERFMON_SVN_INVALID_SECONDFILENAME	1953
EventType: PH_PERFMON_SVN_LINE_MISMATCH	1953
EventType: PH_PERFMON_SVN_SECONDFILENAME_EMPTY	1953
EventType: PH_PERFMON_SVN_SOFTWARE_MISSING	1953
EventType: PH_PERFMON_TOPO_CONFIG_ERROR	1954
EventType: PH_PERFMON_TOPO_FILE_OPEN_FAILED	1954
EventType: PH_PERFMON_TOPO_LOAD_ERROR	1954
EventType: PH_PERFMON_TRACERT_FILE_OPEN_FAILED	1954
EventType: PH_PERFMON_UNKNOWN_CUST_PERF_JOB_ID	1955
EventType: PH_PERFMON_UNKNOWN_PERF_JOB_ID	1955
EventType: PH_PERFMON_UNKNOWN_PROBE_JOB_ID	1955
EventType: PH_PERFMON_UPDATE_CONFIG_ERROR	1955
EventType: PH_PERFMON_UPDATE_FILTERS_ERROR	1956
EventType: PH_PERFMON_UPDATE_ROUTE_DEPENDENCY_FAILED	1956
EventType: PH_PERFMON_USER_PWD_GET_FAILED	1956
EventType: PH_PERFORM_MONITOR_ERROR	1957
EventType: PH_PER_MON_CONFIG_ERROR	1957
EventType: PH_PER_MON_FETCH	1957
EventType: PH_PER_MON_FUNCTION	1958
EventType: PH_PER_MON_SNMP_DONE	1958
EventType: PH_PER_MON_WALK	1958
EventType: PH_PER_MON_WALK_ERROR	1959
EventType: PH_QUERYSRV_DUPLICATED_QUERYID	1959
EventType: PH_QUERYSRV_INVALID_QUERYXML	1959
EventType: PH_QUERY_AGGR_RESULTS_POST_PROCESS_FAILED	1959
EventType: PH_QUERY_ATTR_UNDEFINED	1960
EventType: PH_QUERY_BAD_RESULT_STATUS	1960
EventType: PH_QUERY_CACHE_GET_FAILED	1960
EventType: PH_QUERY_CACHE_RESULT_GET_FAILED	1960
EventType: PH_QUERY_CACHE_TRIGGER_EVENT_GET_FAILED	1961
EventType: PH_QUERY_CHAR_UNEXPECTED	1961
EventType: PH_QUERY_CH_PARSE_FAILED	1961
EventType: PH_QUERY_CH_POST_FAILED	1961
EventType: PH_QUERY_CLICKHOUSE_DATA_FAILED	1962
EventType: PH_QUERY_CLICKHOUSE_EXEC_FAILED	1962
EventType: PH_QUERY_CLICKHOUSE_STARTS	1962
EventType: PH_QUERY_CLICKHOUSE_STOP_FAILED	1963
EventType: PH_QUERY_CLICKHOUSE_WAITING_QUEUE_FULL	1963
EventType: PH_QUERY_COMMAND_BAD	1963
EventType: PH_QUERY_COMPLETION_NOTIFICATION_SEND_FAILED	1964
EventType: PH_QUERY_CONFIG_UNDEFINED	1964

EventType: PH_QUERY_CONVERT_FAILED	1964
EventType: PH_QUERY_DATA_ENUM_FAILED	1964
EventType: PH_QUERY_DATA_MANAGER_NODES_GET_FAILED	1965
EventType: PH_QUERY_DATA_SEND_FAILED	1965
EventType: PH_QUERY_DATA_SIZE_MISMATCH	1965
EventType: PH_QUERY_DATA_SIZE_UNEXPECTED	1965
EventType: PH_QUERY_DATA_TYPE_UNEXPECTED	1966
EventType: PH_QUERY_DB_SERVER_HOST_UNDEFINED	1966
EventType: PH_QUERY_DIR_CREATE_FAILED	1966
EventType: PH_QUERY_DIR_RENAME_FAILED	1966
EventType: PH_QUERY_DISTRIBUTION	1967
EventType: PH_QUERY_DURATION	1967
EventType: PH_QUERY_ES_PARSE_FAILED	1968
EventType: PH_QUERY_ES_POST_FAILED	1968
EventType: PH_QUERY_ES_SCROLL_FAILED	1968
EventType: PH_QUERY_EVENT_COLLECTOR_UNAVAILABLE	1968
EventType: PH_QUERY_EVENT_ID_GET_FAILED	1969
EventType: PH_QUERY_EVENT_PARSE_FAILED	1969
EventType: PH_QUERY_EVENT_PAYLOAD_READ_FAILED	1969
EventType: PH_QUERY_EXCEPTION_CAUGHT	1970
EventType: PH_QUERY_EXPORT_TASK_CREAT_FAILED	1970
EventType: PH_QUERY_EXPORT_TASK_INSERT_FAILED	1970
EventType: PH_QUERY_EXPR_INCOMPLETE	1971
EventType: PH_QUERY_FILE_CONTENT_BAD	1971
EventType: PH_QUERY_FILE_CONTENT_MISSING	1971
EventType: PH_QUERY_FILE_COPY_FAILED	1971
EventType: PH_QUERY_FILE_CORRUPT	1972
EventType: PH_QUERY_FILE_CREATE_FAILED	1972
EventType: PH_QUERY_FILE_EMPTY	1973
EventType: PH_QUERY_FILE_HEADER_GET_FAILED	1973
EventType: PH_QUERY_FILE_LINK_FAILED	1973
EventType: PH_QUERY_FILE_MAGIC_BAD	1973
EventType: PH_QUERY_FILE_MMAP_FAILED	1974
EventType: PH_QUERY_FILE_NAME_BAD	1974
EventType: PH_QUERY_FILE_OPEN_FAILED	1974
EventType: PH_QUERY_FILE_READ_FAILED	1975
EventType: PH_QUERY_FILE_REMOVE_FAILED	1975
EventType: PH_QUERY_FILE_SEEK_FAILED	1975
EventType: PH_QUERY_FILE_STAT_FAILED	1976
EventType: PH_QUERY_FORMAT_UNSUPPORTED	1976
EventType: PH_QUERY_FUNC_ERROR	1976
EventType: PH_QUERY_ID_DUPLICATE	1976
EventType: PH_QUERY_ID_INACTIVE	1977
EventType: PH_QUERY_ID_NOT_FOUND	1977
EventType: PH_QUERY_ID_REMOVE_FAILED	1977
EventType: PH_QUERY_ID_UNSUPPORTED	1978
EventType: PH_QUERY_INLINEREQUEST_BAD	1978
EventType: PH_QUERY_IPC_EVENT_SEND_FAILED	1978
EventType: PH_QUERY_IP_GET_FAILED	1979

EventType: PH_QUERY_IP_INVALID	1979
EventType: PH_QUERY_IP_TYPE_INVALID	1979
EventType: PH_QUERY_LOGINTEGRITYEXPORT_TASK_CREAT_FAILED	1979
EventType: PH_QUERY_LOGINTEGRITYEXPORT_TASK_INSERT_FAILED	1980
EventType: PH_QUERY_LOG_INTEGRITY_EXPORT_DIR_UNCONFIGURED	1980
EventType: PH_QUERY_LOG_INTEGRITY_EXPORT_FAILED	1980
EventType: PH_QUERY_LONG_RUNNING_STOPPED	1980
EventType: PH_QUERY_MEM_ALLOC_FAILED	1981
EventType: PH_QUERY_MESSAGE_SEND_FAILED	1981
EventType: PH_QUERY_MODULE_INIT_FAILED	1981
EventType: PH_QUERY_MODULE_UNCONFIGURED	1982
EventType: PH_QUERY_ONLINE_WORKER_CHANGED	1982
EventType: PH_QUERY_PARSED_EVENT_LOAD_FAILED	1982
EventType: PH_QUERY_PARTIAL_WORKER_FAILURE	1982
EventType: PH_QUERY_PCAP_FINALIZE_FAILED	1983
EventType: PH_QUERY_PCAP_LOAD_FAILED	1983
EventType: PH_QUERY_PCAP_RENAME_FAILED	1983
EventType: PH_QUERY_PCAP_TRANSFER_FAILED	1984
EventType: PH_QUERY_PGDB_EXEC_SQL_FAILED	1984
EventType: PH_QUERY_PGDB_RECONNECT_FAILED	1984
EventType: PH_QUERY_PGDB_SQL_GET_VAL_FAILED	1985
EventType: PH_QUERY_POST_FILTER_PARSE_FAILED	1985
EventType: PH_QUERY_PQ_ERROR	1985
EventType: PH_QUERY_PROCESS_GET_FAILED	1985
EventType: PH_QUERY_PROFILE_ATTR_UNSPECIFIED	1986
EventType: PH_QUERY_PROFILE_EVENT_TYPE_ERROR	1986
EventType: PH_QUERY_PROFILE_FUNCTION_ERROR	1986
EventType: PH_QUERY_PROFILE_NOT_MARKED_AS_BASELINE	1986
EventType: PH_QUERY_PROGRESS_REJECTED	1987

All Logs Page 5 **1988**

EventType: PH_QUERY_REPORTEXPORT_TASK_CREAT_FAILED	2001
EventType: PH_QUERY_REPORTEXPORT_TASK_INSERT_FAILED	2001
EventType: PH_QUERY_REPORT_RESULTS_LOAD_FAILED	2001
EventType: PH_QUERY_REPORT_RESULTS_POST_FILTER_FAILED	2002
EventType: PH_QUERY_REPORT_RESULT_FILE_NOT_EXIST	2002
EventType: PH_QUERY_REQUEST_BAD	2002
EventType: PH_QUERY_RESULT_FILES_MERGE_FAILED	2003
EventType: PH_QUERY_RESULT_GET_FAILED	2003
EventType: PH_QUERY_RESULT_NOT_READY	2003
EventType: PH_QUERY_RESULT_PARSE_FAILED	2003
EventType: PH_QUERY_RESULT_REJECTED	2004
EventType: PH_QUERY_RESULT_SAVE_FAILED	2004
EventType: PH_QUERY_RESULT_UPLOAD_FAILED	2004
EventType: PH_QUERY_RT_ERROR	2005
EventType: PH_QUERY_SORT_SPEC_GET_FAILED	2005
EventType: PH_QUERY_START_FAILED	2005
EventType: PH_QUERY_STATE_BAD	2005
EventType: PH_QUERY_STATUS_LOAD_FAILED	2006
EventType: PH_QUERY_STATUS_SAVE_FAILED	2006

EventType: PH_QUERY_SUMM_ATTR_BAD	2006
EventType: PH_QUERY_SUMM_ATTR_MISSING	2006
EventType: PH_QUERY_SUMM_ATTR_UPDATE_FAILED	2006
EventType: PH_QUERY_SUMM_COLUMN_UNSUPPORTED	2007
EventType: PH_QUERY_SUMM_EVENT_SKIPPED	2007
EventType: PH_QUERY_SUMM_PARSE_FAILED	2007
EventType: PH_QUERY_SUMM_PERF_ETINFO_UNSUPPORTED	2008
EventType: PH_QUERY_TASK_INVALID	2008
EventType: PH_QUERY_TASK_REROUTED	2008
EventType: PH_QUERY_TASK_REROUTE_FAILED	2009
EventType: PH_QUERY_VALUE_TYPE_UNSUPPORTED	2009
EventType: PH_QUERY_WORKERS_GET_FAILED	2009
EventType: PH_QUERY_WORKERS_SPLIT_AMONG_FAILED	2009
EventType: PH_QUERY_WORKER_CHANGED_TO_OFFLINE	2010
EventType: PH_QUERY_WORKER_CHANGED_TO_ONLINE	2010
EventType: PH_QUERY_XML_PARSE_FAILED	2010
EventType: PH_READER_BLOCK_WRITE	2011
EventType: PH_REPORT_ACTION_STATUS	2011
EventType: PH_REPORT_ACT_FAILED	2011
EventType: PH_REPORT_AGGR_FIELDS_EMPTY	2012
EventType: PH_REPORT_AGGR_FIELD_NOT_ADDED	2012
EventType: PH_REPORT_AGGR_FUNC_EMPTY	2012
EventType: PH_REPORT_AGGR_TYPE_ERROR	2012
EventType: PH_REPORT_AGGR_TYPE_UNDEFINED	2013
EventType: PH_REPORT_ATTR_ID_UNSUPPORTED	2013
EventType: PH_REPORT_ATTR_MISSING	2013
EventType: PH_REPORT_ATTR_UNDEFINED	2013
EventType: PH_REPORT_BUFFER_OVERFLOW	2013
EventType: PH_REPORT_CHECKSUM_MISMATCH	2014
EventType: PH_REPORT_CONFIG_UPDATE_NULL	2014
EventType: PH_REPORT_CONVERT_FAILED	2014
EventType: PH_REPORT_DATA_INIT_FAILED	2014
EventType: PH_REPORT_DATA_SIZE_MISMATCH	2014
EventType: PH_REPORT_DATA_SIZE_OVERFLOW	2015
EventType: PH_REPORT_DATA_SIZE_UNEXPECTED	2015
EventType: PH_REPORT_DATA_SIZE_UNKNOWN	2015
EventType: PH_REPORT_DATA_TYPE_UNEXPECTED	2015
EventType: PH_REPORT_DIR_CREATE_FAILED	2016
EventType: PH_REPORT_DIR_OPEN_FAILED	2016
EventType: PH_REPORT_DIR_REMOVE_FAILED	2016
EventType: PH_REPORT_ES_BUCKETS_EMPTY	2017
EventType: PH_REPORT_ES_POST_FAILED	2017
EventType: PH_REPORT_ES_PROFILE_EMPTY	2017
EventType: PH_REPORT_ES_PROFILE_TIMEOUT	2017
EventType: PH_REPORT_ES_PURGE_INDEX_FAILED	2018
EventType: PH_REPORT_ES_TIME_RANGE_INVALID	2018
EventType: PH_REPORT_EXPR_PARSE_FAILED	2018
EventType: PH_REPORT_FILE_CONTENT_MISSING	2018
EventType: PH_REPORT_FILE_COPY_FAILED	2019

EventType: PH_REPORT_FILE_HEADER_BAD	2019
EventType: PH_REPORT_FILE_INIT_FAILED	2019
EventType: PH_REPORT_FILE_LINK_FAILED	2020
EventType: PH_REPORT_FILE_MAGIC_BAD	2020
EventType: PH_REPORT_FILE_MMAP_FAILED	2020
EventType: PH_REPORT_FILE_NAME_BAD	2021
EventType: PH_REPORT_FILE_OPEN_FAILED	2021
EventType: PH_REPORT_FILE_PARSE_FAILED	2021
EventType: PH_REPORT_FILE_READ_FAILED	2022
EventType: PH_REPORT_FILE_REMOVE_FAILED	2022
EventType: PH_REPORT_FILE_RENAME_FAILED	2022
EventType: PH_REPORT_FILE_RSYNC_FAILED	2023
EventType: PH_REPORT_FILE_STAT_FAILED	2023
EventType: PH_REPORT_FILE_TYPE_UNKNOWN	2024
EventType: PH_REPORT_FILE_UNSPECIFIED	2024
EventType: PH_REPORT_FILE_WRITE_FAILED	2024
EventType: PH_REPORT_FUNC_OBJ_DEF_ERROR	2025
EventType: PH_REPORT_FUNC_OBJ_DEF_GET_FAILED	2025
EventType: PH_REPORT_FUNC_OBJ_DEF_UNKNOWN	2025
EventType: PH_REPORT_ID_LOC_DEVICE_EXCLUDED_INVALID	2025
EventType: PH_REPORT_ID_LOC_EVENT_SEND_FAILED	2025
EventType: PH_REPORT_ID_LOC_RESULT_UPLOAD_FAILED	2026
EventType: PH_REPORT_ID_LOC_SYNCH_DATA_UPLOAD_FAILED	2026
EventType: PH_REPORT_ID_LOC_USER_ALREADY_EXCLUDED	2026
EventType: PH_REPORT_ID_LOC_USER_EXCLUDE_FAILED	2027
EventType: PH_REPORT_INDEX_OVERFLOW	2027
EventType: PH_REPORT_IP_GET_FAILED	2027
EventType: PH_REPORT_IP_TYPE_INVALID	2028
EventType: PH_REPORT_KEY_LOAD_FAILED	2028
EventType: PH_REPORT_MODULE_INIT_FAILED	2028
EventType: PH_REPORT_MODULE_UNCONFIGURED	2028
EventType: PH_REPORT_OLD_REPORT_DATA	2029
EventType: PH_REPORT_OP_UNEXPECTED	2029
EventType: PH_REPORT_ORDER_BY_ATTR_EMPTY	2029
EventType: PH_REPORT_ORDER_BY_INVALID	2030
EventType: PH_REPORT_PACK_FAILED	2030
EventType: PH_REPORT_PACK_FAILED_COUNT	2030
EventType: PH_REPORT_PARSED_EVENT_LOAD_FAILED	2030
EventType: PH_REPORT_PGDB_CONNECT_FAILED	2031
EventType: PH_REPORT_PGDB_EXEC_FAILED	2031
EventType: PH_REPORT_PGDB_NOT_CONNECTED	2031
EventType: PH_REPORT_PGDB_NOT_INIT	2031
EventType: PH_REPORT_POINTER_NULL	2032
EventType: PH_REPORT_POINTER_NULL_WARNING	2032
EventType: PH_REPORT_POSITIVE_INTEGER_EXPECTED	2032
EventType: PH_REPORT_PQ_ERROR	2032
EventType: PH_REPORT_PROFILE_TYPE_BAD	2033
EventType: PH_REPORT_PROFILE_TYPE_WRONG_FORMAT	2033
EventType: PH_REPORT_PROFILE_UPDATE_FAILED	2033

EventType: PH_REPORT_ROW_LENGTH_ZERO	2034
EventType: PH_REPORT_RULE_ATTR_MISSING	2034
EventType: PH_REPORT_SCHEMA_INCOMPATIBLE	2034
EventType: PH_REPORT_SCHEMA_INVALID	2034
EventType: PH_REPORT_SCHEMA_LOAD_FAILED	2035
EventType: PH_REPORT_SQLITE3_BATCH_BEGIN_FAILED	2035
EventType: PH_REPORT_SQLITE3_BATCH_COMMIT_FAILED	2035
EventType: PH_REPORT_SQLITE3_BIND_VALUE_FAILED	2036
EventType: PH_REPORT_SQLITE3_BUSY	2036
EventType: PH_REPORT_SQLITE3_BUSY_TIMEOUT_ERROR	2036
EventType: PH_REPORT_SQLITE3_CHECKPOINT_FAILED	2037
EventType: PH_REPORT_SQLITE3_COMMIT_ERROR	2037
EventType: PH_REPORT_SQLITE3_CONFIG_FAILED	2037
EventType: PH_REPORT_SQLITE3_ENABLE_SHARED_CACHE_FAILED	2038
EventType: PH_REPORT_SQLITE3_EXEC_FAILED	2038
EventType: PH_REPORT_SQLITE3_EXTENDED_RESULT_CODES_ERROR	2039
EventType: PH_REPORT_SQLITE3_OPEN_FAILED	2039
EventType: PH_REPORT_SQLITE3_PREPARE_ERROR	2039
EventType: PH_REPORT_SQLITE3_PROFILE_ENTRY_DELETE_FAILED	2040
EventType: PH_REPORT_SQLITE3_PROFILE_NOT_FOUND	2040
EventType: PH_REPORT_SQLITE3_STEP_ERROR	2041
EventType: PH_REPORT_UNPACK_FAILED	2041
EventType: PH_REPORT_VALUE_TYPE_LOOKUP_BY_ID_FAILED	2041
EventType: PH_REPORT_VALUE_TYPE_LOOKUP_BY_NAME_FAILED	2041
EventType: PH_REPORT_VALUE_TYPE_OF_ID_UNEXPECTED	2042
EventType: PH_REPORT_VALUE_TYPE_OF_NAME_UNEXPECTED	2042
EventType: PH_REPORT_VALUE_TYPE_OF_STAT_UNEXPECTED	2042
EventType: PH_REPORT_VALUE_TYPE_UNSUPPORTED	2042
EventType: PH_REPORT_WORKER_UPLOAD_FAILED	2042
EventType: PH_REPORT_XML_ELEMENT_DUPLICATE	2043
EventType: PH_REPORT_XML_ELEMENT_MISSING	2043
EventType: PH_REPORT_XML_ELEMENT_PARSE_FAILED	2044
EventType: PH_REPORT_XML_PARSE_FAILED	2044
EventType: PH_REPORT_ZLIB_COMPRESSION_TYPE_UNKNOWN	2044
EventType: PH_REPORT_ZLIB_UNCOMPRESS_FAILED	2045
EventType: PH_RULEMASTER_TEST_RULES_CHECK_SYNTAX	2045
EventType: PH_RULEMASTER_TEST_RULES_FINALIZE_STATE	2045
EventType: PH_RULEMASTER_TEST_RULES_UPDATE_STATE	2045
EventType: PH_RULEMOD_AGGREGATOR_EMPTY	2046
EventType: PH_RULEMOD_ARITH_OP_ILLEGAL	2046
EventType: PH_RULEMOD_ATTR_ALREADY_ASSOCIATED	2046
EventType: PH_RULEMOD_ATTR_ID_LOOKUP_BY_NAME_FAILED	2047
EventType: PH_RULEMOD_ATTR_ID_UNDEFINED	2047
EventType: PH_RULEMOD_ATTR_MISSING	2047
EventType: PH_RULEMOD_ATTR_NAME_LOOKUP_BY_ID_FAILED	2047
EventType: PH_RULEMOD_ATTR_UNDEFINED	2048
EventType: PH_RULEMOD_BUFFER_EMPTY	2048
EventType: PH_RULEMOD_CLEAR_CONDITION_INVALID	2048
EventType: PH_RULEMOD_CLEAR_CONDITION_SET_FAILED	2048

EventType: PH_RULEMOD_CONFIG_UNDEFINED	2049
EventType: PH_RULEMOD_CONSTRUCTOR_ERROR	2049
EventType: PH_RULEMOD_CUST_ID_LIST_INVALID	2049
EventType: PH_RULEMOD_DATA_REQUEST_PARSE_FAILED	2050
EventType: PH_RULEMOD_DATA_SIZE_OVERFLOW	2050
EventType: PH_RULEMOD_DATA_UNSUPPORTED	2050
EventType: PH_RULEMOD_DB_SERVER_HOST_UNDEFINED	2050
EventType: PH_RULEMOD_DIR_OPEN_FAILED	2051
EventType: PH_RULEMOD_ENCODE_FAILED	2051
EventType: PH_RULEMOD_ENTITY_VERSION_MISSING	2051
EventType: PH_RULEMOD_EVENT_TYPE_GROUP_INVALID	2052
EventType: PH_RULEMOD_EVENT_TYPE_NOT_FOUND	2052
EventType: PH_RULEMOD_EXCEPTION_ELEMENT_INVALID	2052
EventType: PH_RULEMOD_EXPR_EVAL_UNKNOWN	2053
EventType: PH_RULEMOD_EXPR_PARSE_FAILED	2053
EventType: PH_RULEMOD_EXPR_UNSUPPORTED	2053
EventType: PH_RULEMOD_FILE_OPEN_FAILED	2054
EventType: PH_RULEMOD_FILE_UNSPECIFIED	2054
EventType: PH_RULEMOD_FORMAT_ERROR	2054
EventType: PH_RULEMOD_FUNC_NOT_FOUND	2054
EventType: PH_RULEMOD_FUNC_PARSE_FAILED	2055
EventType: PH_RULEMOD_GLOBAL_CONSTRAINT_INVALID	2055
EventType: PH_RULEMOD_GROUPBY_LIST_INVALID	2055
EventType: PH_RULEMOD_GROUPBY_LIST_NOT_FOUND	2056
EventType: PH_RULEMOD_GROUP_EVENT_CONSTRAINT_INVALID	2056
EventType: PH_RULEMOD_ID_LOOKUP_BY_INCIDENT_FAILED	2056
EventType: PH_RULEMOD_INCIDENT_ARG_INVALID	2057
EventType: PH_RULEMOD_INCIDENT_CACHE_NOT_FOUND	2057
EventType: PH_RULEMOD_INCIDENT_DEF_INVALID	2057
EventType: PH_RULEMOD_INCIDENT_NOT_FOUND	2058
EventType: PH_RULEMOD_INCIDENT_REPORT_SEND_FAILED	2058
EventType: PH_RULEMOD_INDEX_OVERFLOW	2058
EventType: PH_RULEMOD_INFO_GET_FAILED	2059
EventType: PH_RULEMOD_IP_GET_FAILED	2059
EventType: PH_RULEMOD_IP_INVALID	2059
EventType: PH_RULEMOD_IP_TYPE_INVALID	2060
EventType: PH_RULEMOD_LOAD_METHOD_UNDEFINED	2060
EventType: PH_RULEMOD_MEM_ALLOC_FAILED	2060
EventType: PH_RULEMOD_MODULE_INIT_FAILED	2060
EventType: PH_RULEMOD_MUTEX_ACQUIRE_FAILED	2061
EventType: PH_RULEMOD_NOTIF_CONNECTION_FAILED	2061
EventType: PH_RULEMOD_OBJ_GET_FROM_SUBPATTERN_FAILED	2061
EventType: PH_RULEMOD_OBJ_LOAD_FAILED	2061
EventType: PH_RULEMOD_OP_NOT_FUNC	2062
EventType: PH_RULEMOD_OP_UNKNOWN	2062
EventType: PH_RULEMOD_PARSED_EVENT_LOAD_FAILED	2062
EventType: PH_RULEMOD_PQ_ERROR	2062
EventType: PH_RULEMOD_PROFILE	2062
EventType: PH_RULEMOD_REM_BY_ZERO	2063

EventType: PH_RULEMOD_REM_BY_ZEROD	2063
EventType: PH_RULEMOD_SELECT_ATTR_PARSE_FAILED	2063
EventType: PH_RULEMOD_SELECT_SPEC_PARSE_FAILED	2063
EventType: PH_RULEMOD_SINGLE_EVENT_CONSTRAINT_INVALID	2064
EventType: PH_RULEMOD_SUBPATTERN_INVALID	2064
EventType: PH_RULEMOD_SUBPATTERN_MISSING	2064
EventType: PH_RULEMOD_SUBPATTERN_MORE_THAN_ONE	2064
EventType: PH_RULEMOD_SUBPATTERN_UNDEFINED	2065
EventType: PH_RULEMOD_SUMMARY_UPLOAD_FAILED	2065
EventType: PH_RULEMOD_THREAD_SPAWN_FAILED	2066
EventType: PH_RULEMOD_TOKEN_UNDEFINED	2066
EventType: PH_RULEMOD_TOKEN_UNEXPECTED	2066
EventType: PH_RULEMOD_UNPACK_FAILED	2067
EventType: PH_RULEMOD_VALUE_TYPE_UNEXPECTED	2067
EventType: PH_RULEMOD_XML_ELEMENT_EMPTY	2067
EventType: PH_RULEMOD_XML_ELEMENT_MISSING	2067
EventType: PH_RULEMOD_XML_ELEMENT_PARSE_FAILED	2068
EventType: PH_RULEMOD_XML_ELEMENT_UNEXPECTED	2068
EventType: PH_RULEMOD_XML_ELEMENT_UNKNOWN	2068
EventType: PH_RULEMOD_XML_LOAD_FAILED	2068
EventType: PH_RULEMOD_XML_PARSE_FAILED	2069
EventType: PH_RULEMOD_XML_POINTER_NULL	2069
EventType: PH_RULEWORKER_TEST_RULES_CHECK_SYNTAX	2069
EventType: PH_RULEWORKER_TEST_RULES_EVENT_MATCH_STATUS	2070
EventType: PH_Rule_AbuseCH_Botnetc2_MalwareIP_Inbound	2070
EventType: PH_Rule_AbuseCH_Botnetc2_MalwareIP_Outbound	2070
EventType: PH_Rule_Blocklist_MalwareIP_Inbound	2070
EventType: PH_Rule_Blocklist_MalwareIP_Outbound	2070
EventType: PH_Rule_C2_Tracker_MalwareIP_Inbound	2071
EventType: PH_Rule_C2_Tracker_MalwareIP_Outbound	2071
EventType: PH_Rule_CINSScore_MalwareIP_Inbound	2071
EventType: PH_Rule_CINSScore_MalwareIP_Outbound	2071
EventType: PH_Rule_CertPL_MalwareDomain_Inbound	2071
EventType: PH_Rule_CertPL_MalwareDomain_Outbound	2072
EventType: PH_Rule_Cisco_Talos_MalwareIP_Inbound	2072
EventType: PH_Rule_Cisco_Talos_MalwareIP_Outbound	2072
EventType: PH_Rule_Cluster_DBLeader_Changed	2072
EventType: PH_Rule_Cluster_REPL_Leader_Changed	2072
EventType: PH_Rule_DigitalSide_MalwareDomain_Inbound	2072
EventType: PH_Rule_DigitalSide_MalwareDomain_Outbound	2073
EventType: PH_Rule_DigitalSide_MalwareIP_Inbound	2073
EventType: PH_Rule_DigitalSide_MalwareIP_Outbound	2073
EventType: PH_Rule_DigitalSide_MalwareURL_Outbound	2073
EventType: PH_Rule_FML_Antispam_Malicious_File	2073
EventType: PH_Rule_FML_Antispam_Malicious_Url	2074
EventType: PH_Rule_FireHol_MalwareIP_Inbound	2074
EventType: PH_Rule_FireHol_MalwareIP_Outbound	2074
EventType: PH_Rule_FortiRecon_MalwareDomain_Inbound	2074
EventType: PH_Rule_FortiRecon_MalwareDomain_Outbound	2074

EventType: PH_Rule_FortiRecon_MalwareIP_Inbound	2074
EventType: PH_Rule_FortiRecon_MalwareIP_Outbound	2075
EventType: PH_Rule_FortiRecon_MalwareURL_Outbound	2075
EventType: PH_Rule_FortiSOAR_MalwareDomain_Inbound	2075
EventType: PH_Rule_FortiSOAR_MalwareDomain_Outbound	2075
EventType: PH_Rule_FortiSOAR_MalwareIP_Inbound	2075
EventType: PH_Rule_FortiSOAR_MalwareIP_Outbound	2076
EventType: PH_Rule_FortiSOAR_MalwareURL_Outbound	2076
EventType: PH_Rule_Greensnow_MalwareIP_Inbound	2076
EventType: PH_Rule_Greensnow_MalwareIP_Outbound	2076
EventType: PH_Rule_IPSum_MalwareIP_Inbound	2076
EventType: PH_Rule_IPSum_MalwareIP_Outbound	2076
EventType: PH_Rule_MISP_MalwareDomain_Inbound	2077
EventType: PH_Rule_MISP_MalwareDomain_Outbound	2077
EventType: PH_Rule_MISP_MalwareIP_Inbound	2077
EventType: PH_Rule_MISP_MalwareIP_Outbound	2077
EventType: PH_Rule_MISP_MalwareURL_Outbound	2077
EventType: PH_Rule_Mandiant_MalwareDomain_Inbound	2078
EventType: PH_Rule_Mandiant_MalwareDomain_Outbound	2078
EventType: PH_Rule_Mandiant_MalwareIP_Inbound	2078
EventType: PH_Rule_Mandiant_MalwareIP_Outbound	2078
EventType: PH_Rule_Mandiant_MalwareURL_Outbound	2078
EventType: PH_Rule_OPENCTI_MalDomain_Inbound	2078
EventType: PH_Rule_OPENCTI_MalDomain_Outbound	2079
EventType: PH_Rule_OPENCTI_MalwareIP_Inbound	2079
EventType: PH_Rule_OPENCTI_MalwareIP_Outbound	2079
EventType: PH_Rule_OPENCTI_MalwareURL_Outbound	2079
EventType: PH_Rule_OpenPhish_MalwareURL_Outbound	2079
EventType: PH_Rule_Proofpoint_MalwareIP_Inbound	2080
EventType: PH_Rule_Proofpoint_MalwareIP_Outbound	2080
EventType: PH_Rule_Snort_MalwareIP_Inbound	2080
EventType: PH_Rule_Snort_MalwareIP_Outbound	2080
EventType: PH_Rule_ThreatFox_MalwareURL_Outbound	2080
EventType: PH_Rule_TweetFeed_MalwareDomain_Inbound	2080
EventType: PH_Rule_TweetFeed_MalwareDomain_Outbound	2081
EventType: PH_Rule_TweetFeed_MalwareURL_Outbound	2081
EventType: PH_Rule_Tweetfeed_MalwareIP_Inbound	2081
EventType: PH_Rule_Tweetfeed_MalwareIP_Outbound	2081
EventType: PH_SAAS_OP_COLLECTOR_DOWN	2081
EventType: PH_SAAS_OP_COLLECTOR_UP	2082
EventType: PH_SCHEDULED_RULE_QUERY_FAILED	2082
EventType: PH_SER_MON_SERVICE_DOWN	2082
EventType: PH_SHAREDSTORE_ACQUIRE_ERROR	2082
EventType: PH_SHAREDSTORE_WRITER_POS_UNEXPECTED_ALTERED	2083
EventType: PH_SHAREDSTORE_WRITE_ERROR	2083
EventType: PH_SSL_SHUTDOWN_ERROR	2083
EventType: PH_STM_ACCOUNT_UNMATCHED	2083
EventType: PH_STM_AUTH_TYPE_UNKNOWN	2083
EventType: PH_STM_BAD_ELEM	2084

EventType: PH_STM_BAD_ELEM_VALUE	2084
EventType: PH_STM_BAD_PORT	2084
EventType: PH_STM_BAD_RTT_LINE	2084
EventType: PH_STM_BAD_SSL	2084
EventType: PH_STM_BAD_TAG	2084
EventType: PH_STM_CMD_EXEC_FAILED	2085
EventType: PH_STM_CRED_INVALID	2085
EventType: PH_STM_CURL_ESCAPE_FAILED	2085
EventType: PH_STM_CURL_INIT_FAILED	2085
EventType: PH_STM_DNS_TYPE_UNSUPPORT	2086
EventType: PH_STM_DUPLICATED	2086
EventType: PH_STM_ELEM_EMPTY	2086
EventType: PH_STM_ELEM_MISSING	2086
EventType: PH_STM_ELEM_NEGATIVE	2086
EventType: PH_STM_ERROR	2086
EventType: PH_STM_FILE_OPEN_FAILED	2087
EventType: PH_STM_GET_HOST_FAILED	2087
EventType: PH_STM_GUESS_TYPE_FAILED	2088
EventType: PH_STM_HTTP_RESP_FAILED	2088
EventType: PH_STM_METHOD_UNKNOWN	2088
EventType: PH_STM_MONITOR_MISSING_ACTION	2088
EventType: PH_STM_MONITOR_RESULT_UPLOAD_FAILED	2088
EventType: PH_STM_NO_ORACLE_NAME	2089
EventType: PH_STM_PORT_UNKNOWN	2089
EventType: PH_STM_PROCESS_INVOKE_FAILED	2089
EventType: PH_STM_PROTO_UNKNOWN	2089
EventType: PH_STM_PROTO_UNSUPPORT	2089
EventType: PH_STM_SERVER_ADDR_INVALID	2090
EventType: PH_STM_SPECIAL_LINE_NOT_FOUND	2090
EventType: PH_STM_STM_GET_PROCESS_FAILED	2090
EventType: PH_STM_STM_GET_PROCESS_NAME_FAILED	2090
EventType: PH_STM_TAG_MISSING	2090
EventType: PH_STM_TAG_NOT_FOUND	2090
EventType: PH_STM_TAG_UNKNOWN	2091
EventType: PH_STM_TRACEROUTE_FAILED	2091
EventType: PH_STM_XML_PARSE_FAILED	2091
EventType: PH_SYSTEM_ARCHIVE_LOW	2091
EventType: PH_SYSTEM_ARCHIVE_PURGED_LOW_SPACE	2091
EventType: PH_SYSTEM_ARCHIVE_PURGED_POLICY	2092
EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_FAILED	2092
EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_FINISHED	2092
EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_STARTED	2092
EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_SUCCESS	2092
EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_FAILED	2093
EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_FINISHED	2093
EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_STARTED	2093
EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_SUCCESS	2093
EventType: PH_SYSTEM_ARCHIVE_RETENTION_POLICY_VIOLATED	2093
EventType: PH_SYSTEM_ARCHIVE_USAGE	2094

EventType: PH_SYSTEM_DATAMGR_ARCHIVE_SKIP	2094
EventType: PH_SYSTEM_DEVAPP_EVENTS_PER_SEC	2094
EventType: PH_SYSTEM_DEVAPP_NO_EVENTS	2095
EventType: PH_SYSTEM_DEVICE_NO_EVENTS	2095
EventType: PH_SYSTEM_DISK_ARCHIVING_FAILED	2096
EventType: PH_SYSTEM_DISK_ARCHIVING_FINISHED	2096
EventType: PH_SYSTEM_DISK_ARCHIVING_STARTED	2096
EventType: PH_SYSTEM_DISK_ARCHIVING_SUCCESS	2096
EventType: PH_SYSTEM_DISK_PURGED	2096
EventType: PH_SYSTEM_DISK_PURGING_FAILED	2097
EventType: PH_SYSTEM_DISK_PURGING_FINISHED	2097
EventType: PH_SYSTEM_DISK_PURGING_STARTED	2097
EventType: PH_SYSTEM_DISK_PURGING_SUCCESS	2097
EventType: PH_SYSTEM_DISK_USAGE	2097
EventType: PH_SYSTEM_DISK_USAGE_EXCEED_LICENSE	2098
EventType: PH_SYSTEM_DISK_USAGE_WARNING	2098
EventType: PH_SYSTEM_DROP_UNKNOWN_ORG	2098
EventType: PH_SYSTEM_EPS_GLOBAL	2098
EventType: PH_SYSTEM_EPS_NODE	2099
EventType: PH_SYSTEM_EPS_ORG	2100
EventType: PH_SYSTEM_EVENTS_FWD_STAT	2101
EventType: PH_SYSTEM_EVENTS_PER_SEC	2102
EventType: PH_SYSTEM_EVENTS_VIA_ZMQ_EPS	2102
EventType: PH_SYSTEM_EVENT_RATE_EXCEED_LICENSE	2103
EventType: PH_SYSTEM_INTERNAL_EVENTS_PER_SEC	2103
EventType: PH_SYSTEM_IP_EVENTS_PER_SEC	2103
EventType: PH_SYSTEM_ONLINE_RETENTION_POLICY_VIOLATED	2104
EventType: PH_SYSTEM_PERF_EVENTS_PER_SEC	2104
EventType: PH_SYSTEM_RAW_EVENT_SIZE	2104
EventType: PH_SYSTEM_RETENTION_POLICY_EXEC_TIME	2105
EventType: PH_SYSTEM_RETENTION_POLICY_FAILED	2105
EventType: PH_SYSTEM_RETENTION_POLICY_FINISHED	2106
EventType: PH_SYSTEM_RETENTION_POLICY_STARTED	2106
EventType: PH_SYSTEM_RETENTION_POLICY_STATS	2106
EventType: PH_SYSTEM_RETENTION_POLICY_SUCCESS	2106
EventType: PH_SYSTEM_STORAGE_LOW	2106
EventType: PH_SYSTEM_STORED_EVENTS_PER_SEC	2107
EventType: PH_SYSTEM_SUMM_EVENTS_STORED_EPS	2107
EventType: PH_SYS_ERROR_XML_SEND_ERROR	2108
EventType: PH_SYS_ERROR_XML_SENT	2108
EventType: PH_TASK_DATA_EMPTY	2108
EventType: PH_TASK_DATA_IS_WRONG	2108
EventType: PH_TASK_FAILED	2108
EventType: PH_TASK_NOT_CONTAIN_LIC	2109
EventType: PH_TASK_NO_LICENSE	2109
EventType: PH_TASK_RUN_COMMAND_FAILED	2109
EventType: PH_TASK_SEND_FAILED	2109
EventType: PH_TASK_UNSUPPORT	2110
EventType: PH_TEST_CONN_COMPLETE	2110

EventType: PH_TEST_CONN_CONTACT_APP_SERVER	2110
EventType: PH_TEST_CONN_FAILED	2111
EventType: PH_TEST_CONN_FAILED_INVALID_REQUEST	2111
EventType: PH_TEST_CONN_FAILED_INVALID_REQUEST_XML	2111
EventType: PH_TEST_CONN_RECVD_VALID_REQUEST	2111
EventType: PH_TEST_CONN_RESULT_SENT	2112
EventType: PH_TEST_CONN_STARTED	2112
EventType: PH_TEST_RULES_PARSE_STATUS	2112
EventType: PH_THREAD_EXITING	2112
EventType: PH_THREAD_RECVD_EXIT	2113
EventType: PH_THREAD_STARTING	2113
EventType: PH_UNABLE_ACCESS_DIR	2113
EventType: PH_UNABLE_ALLOC_MEMORY	2114
EventType: PH_UNABLE_CREATE_DIR	2114
EventType: PH_UNABLE_CREATE_FILE	2114
EventType: PH_UNABLE_CREATE_TIMER	2114
EventType: PH_UNABLE_OPEN_DIR	2115
EventType: PH_UNABLE_OPEN_FILE	2115
EventType: PH_UNABLE_PARSE_XML	2115
EventType: PH_UNABLE_RENAME_FILE	2116
EventType: PH_UNRESOLVABLE_HOSTNAME	2116
EventType: PH_UNRESOLVABLE_IP	2116
EventType: PH_UPDATE_RULE_SUCCEED	2117
EventType: PH_USER_MON_SUDDEN_LOC_CHANGE	2117
EventType: PH_USER_MON_SUDDEN_LOGIN_DISTRIBUTION_CHANGE	2118
EventType: PH_USER_MON_SUDDEN_LOGIN_VOLUME_CHANGE	2119
EventType: PH_UTIL_BIZ_CHANGE_UPDATE_SPAWN_FAILURE	2119
EventType: PH_UTIL_BIZ_HTTP_REQUEST_FAILURE	2119
EventType: PH_UTIL_CMD_FAILURE	2120
EventType: PH_UTIL_CONFIG_IP_MISSING	2120
EventType: PH_UTIL_CONFIG_LOAD_FAILURE	2120
EventType: PH_UTIL_CONFIG_LOAD_FILE_ACESS_FAILURE	2120
EventType: PH_UTIL_CONFIG_PARSE_FAILURE	2121
EventType: PH_UTIL_CONFIG_UNKNOWN_SERVER_TYPE	2121
EventType: PH_UTIL_CONNECTION_ERROR	2121
EventType: PH_UTIL_CSV_LINE_ILLEGAL	2122
EventType: PH_UTIL_CSV_READ_FAILURE	2122
EventType: PH_UTIL_CUSTOMER_COLLECTOR_MISSING	2122
EventType: PH_UTIL_CUSTOMER_COLLECTOR_PARSE_FAILURE	2123
EventType: PH_UTIL_CUSTOMER_DOMAIN_MISSING	2123
EventType: PH_UTIL_CUSTOMER_INFO_PARSE_FAILURE	2123
EventType: PH_UTIL_CUSTOMER_PARSE_FAILURE	2123
EventType: PH_UTIL_DASHBOARD_DUPLICATE_IP	2123
EventType: PH_UTIL_DASHBOARD_DUPLICATE_ITEM	2124
EventType: PH_UTIL_DASHBOARD_PARSE_FAILURE	2124
EventType: PH_UTIL_DEVICE_MAP_PROP_ERROR	2124
EventType: PH_UTIL_DEVICE_PROP_ERROR	2125
EventType: PH_UTIL_DEVICE_SIMPLE_PROP_PARSE_FAILURE	2125
EventType: PH_UTIL_DGA_FREQ_FILE_OPEN_FAILURE	2125

EventType: PH_UTIL_DGA_WHITELIST_FILE_OPEN_FAILURE	2126
EventType: PH_UTIL_DIR_CREATE_FAILURE	2126
EventType: PH_UTIL_DIR_CREATE_RETRIED	2126
EventType: PH_UTIL_DIR_OPEN_FAILURE	2127
EventType: PH_UTIL_DIR_PARENT_NOT_EXIST	2127
EventType: PH_UTIL_DIR_REMOVE_FAILURE	2127
EventType: PH_UTIL_DISK_USAGE_INFO_GET_FAILURE	2128
EventType: PH_UTIL_DISPATH_CMD_XML_ILLEGAL	2128
EventType: PH_UTIL_DISPATH_CMD_XML_PARSE_FAILURE	2128
EventType: PH_UTIL_EMAIL_SEND_FAILURE	2129
EventType: PH_UTIL_ETCD_COMPAGN_FAILED	2129
EventType: PH_UTIL_ETCD_GET_LEADER_FAILED	2129
EventType: PH_UTIL_ETCD_LEASE_FAILED	2130
EventType: PH_UTIL_ETCD_SET_FAILED	2130
EventType: PH_UTIL_EVENT_FILE_ERROR	2130
EventType: PH_UTIL_EVENT_GROUP_ERROR	2131
EventType: PH_UTIL_EVENT_STATUS_REPORTER_SPAWN_FAILURE	2131
EventType: PH_UTIL_EVENT_STATUS_UPLOAD_FAILURE	2131
EventType: PH_UTIL_EVENT_TYPE_ERROR	2131
EventType: PH_UTIL_FILE_NOT_EXIST	2132
EventType: PH_UTIL_FILE_OPEN_FAILURE	2132
EventType: PH_UTIL_FILE_READ_FAILURE	2132
EventType: PH_UTIL_FILE_SIZE_MISMATCH	2133
EventType: PH_UTIL_FILE_SIZE_TOO_SMALL	2133
EventType: PH_UTIL_FILE_STATFS_FAILURE	2133
EventType: PH_UTIL_FILE_STAT_FAILURE	2134
EventType: PH_UTIL_FILE_WRITE_FAILURE	2134
EventType: PH_UTIL_FORK_FAILURE	2134
EventType: PH_UTIL_GET_ADDR_FAILURE	2135
EventType: PH_UTIL_GET_ATTR_NAME_FAILED	2135
EventType: PH_UTIL_GET_JOB_STATUS_FAILURE	2135
EventType: PH_UTIL_HOSTNAME_GET_FAILURE	2136
EventType: PH_UTIL_INET_PTON_FAILURE	2136
EventType: PH_UTIL_INODE_INFO_GET_FAILURE	2136
EventType: PH_UTIL_INVALID_PARAM	2137
EventType: PH_UTIL_IOCTL_FAILURE	2137
EventType: PH_UTIL_IOCTL_SIOCGIFADDR_FAILURE	2137
EventType: PH_UTIL_IP_TYPE_INVALID	2137
EventType: PH_UTIL_IP_TYPE_MISMATCH	2138
EventType: PH_UTIL_JOB_STATUS_REPORTER_SPAWN_FAILURE	2138
EventType: PH_UTIL_JOB_STATUS_UPLOAD_FAILURE	2138
EventType: PH_UTIL_JSON_GET_NODE_FAILURE	2138
EventType: PH_UTIL_JSON_GET_TOTAL_COUNT_FAILURE	2139
EventType: PH_UTIL_JSON_OBJ_EMPTY	2139
EventType: PH_UTIL_JSON_PARSE_FAILURE	2139
EventType: PH_UTIL_KILLPG_FAILURE	2139
EventType: PH_UTIL_LOAD_EXT_FUNC_FILE_OPEN_FAILUE	2140
EventType: PH_UTIL_LOAD_EXT_FUNC_FORMAT_INVALID	2140
EventType: PH_UTIL_LOAD_EXT_FUNC_GET_NAME_FAILUE	2140

EventType: PH_UTIL_LOCAL_IP_MISSING	2141
EventType: PH_UTIL_LOOKUP_TABLES_DUPLICATE	2141
EventType: PH_UTIL_LOOKUP_TABLES_DUPLICATE_COLUMN	2141
EventType: PH_UTIL_LOOKUP_TABLES_DUPLICATE_KEY	2142
EventType: PH_UTIL_MAIL_CMD_RUN_FAILURE	2142
EventType: PH_UTIL_MAIL_SMTP_INIT_FAILURE	2142
EventType: PH_UTIL_MD5_ERROR	2142
EventType: PH_UTIL_MEM_ALLOC_FAILURE	2143
EventType: PH_UTIL_MKDTEMP_FAILURE	2143
EventType: PH_UTIL_MKSTEMP_FAILURE	2143
EventType: PH_UTIL_MMAP_FAILURE	2144
EventType: PH_UTIL_MOVE_FILE_FAILURE	2144
EventType: PH_UTIL_NOTIFICATION_SENDER_SPAWN_FAILURE	2144
EventType: PH_UTIL_NOTIFICATION_SERVER_INIT_FAILURE	2144
EventType: PH_UTIL_NOTIFICATION_UPLOAD_FAILURE	2145
EventType: PH_UTIL_PCRE_COMPILE_FAILED	2145
EventType: PH_UTIL_PHOENIX_CONFIG_ITEM_MISSING	2145
EventType: PH_UTIL_PIPE_FAILURE	2146
EventType: PH_UTIL_PROP_DEF_SET_PARSE_FAILURE	2146
EventType: PH_UTIL_REDIS_CONNECTION_ERROR	2146
EventType: PH_UTIL_REGEX_PATTERN_EMPTY	2147
EventType: PH_UTIL_REGEX_PATTERN_TOO_LONG	2147
EventType: PH_UTIL_SEND_DATA_FAILED	2147
EventType: PH_UTIL_SEND_TO_UDP_PORT_FAILURE	2147
EventType: PH_UTIL_SETPGRP_FAILURE	2148
EventType: PH_UTIL_SET_JOB_STATUS_FAILURE	2148
EventType: PH_UTIL_SOCKET_FAILURE	2148
EventType: PH_UTIL_STR_TO_IP_FAILURE	2149
EventType: PH_UTIL_SVN_DIFF_FAILURE	2149
EventType: PH_UTIL_SYS_ERROR_REPORTER_INIT_FAILURE	2149
EventType: PH_UTIL_TIME_RANGE_INVALID	2150
EventType: PH_UTIL_TIME_STR_FORMAT_INVALID	2150
EventType: PH_UTIL_TLS_SERVER_RECV_FAILED	2150
EventType: PH_UTIL_UNKNOWN_PHOENIX_ERROR_NUMBER	2150
EventType: PH_UTIL_VALUE_GROUP_ERROR	2151
EventType: PH_UTIL_WAITPID_FAILURE	2151
EventType: PH_UTIL_WAITPID_LAST_TRY_FAILUE	2151
EventType: PH_UTIL_WINDOWS_BID_LOAD_FAILURE	2152
EventType: PH_UTIL_WRITE_BIN_FILE_OPEN_FAILURE	2152
EventType: PH_UTIL_WRITE_FILE_OPEN_FAILURE	2152
EventType: PH_UTIL_XML_HANDLING_ERROR	2153
EventType: PH_UTIL_ZIP_DECOMPRESS_FAILED	2153
EventType: PH_VA_EVENTS_PER_SEC	2153
EventType: PH_VA_LICENSE_UPDATE	2154
EventType: PH_VULN_LOAD_ERROR	2154
EventType: PH_VULN_UPDATE_ERROR	2154
EventType: PH_WORKER_DOWN	2154
EventType: PH_WORKER_PROVISION_FAILED	2155
EventType: PH_WORKER_UP	2155

EventType: PH_WS_COMM_ERROR	2155
EventType: WEBSense_MAIL_JDBC_PULL_STAT	2155
EventType: WEBSense_WEB_JDBC_PULL_STAT	2155

Change Log

Date	Change Description
12/16/2024	Initial version of the 7.3.0 Log Reference Guide.

Important Logs By Use case

This section identifies important logs for several failure use cases.

- Collector clock skew detected
- Collector failing to forward events to External System
- Collector failing to send events to Worker on time
- Collector failing to send events to Workers
- Collector/Worker to Supervisor communication issue
- Devices not sending logs
- EPS License Exceeded
- EPS Reporting
- Event Archiving Error (Elasticsearch to EventDB/NFS)
- Event Archiving Error (EventDB to EventDB/NFS)
- FortiSIEM Process is Down
- FortiSIEM process to Supervisor communication issue
- GUI Change Audit
- GUI User Login
- Incident External Integration issue
- Incident email notification issue
- Linux Agent operational errors
- Malware IOC handling Errors
- Query Errors
- Query Performance
- Rule Performance
- Rule trigger issues
- Scheduled Report issue
- Test Connectivity/Discovery Errors
- Windows/Linux Agent operational errors
- Worker failing to store events in ClickHouse
- Worker failing to store events in Elasticsearch
- Worker failing to store events in EventDB
- Worker falling behind in storing configuration files to SVN-lite
- Worker falling behind in storing events to Event Database

Use Case: Collector clock skew detected

- PH_COLLECTOR_CLOCK_SKEW

EventType: PH_COLLECTOR_CLOCK_SKEW

Description: Clock skew between Collector and Super

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
collectorId	Collector ID	uint32	This field captures the ID of a FortiSIEM Collector
collectorIp	Collector IP	IP	This field captures the IP address of a FortiSIEM Collector
superTime	Supervisor Time	Date	This field represents SupervisorTime used to determine Clock Skew between Collector and Supervisor. A Clock Skew may develop if NTP is not configured correctly in both Collector and Supervisor.
collectorTime	Collector Time	Date	This field represents Collector Time used to determine Clock Skew between Collector and Supervisor. A Clock Skew may develop if NTP is not configured correctly in both Collector and Supervisor.
timeSkewSec	Time skew	uint32	Time skew between Collector and Supervisor. If there is significant time skew then rules may not trigger, since rules need to be evaluated based on a time window.

Use Case: Collector failing to forward events to External System

- [PH_AGENTMGR_KAFKA_PRODUCER_ERROR](#)
- [PH_EVENT_FWD_SOCKET_CONNECT_FAILED](#)
- [PH_EVENT_FWD_SOCKET_WRITE_FAILED](#)

EventType: PH_AGENTMGR_KAFKA_PRODUCER_ERROR

Description: Event Forwarder failed to write events into Kafka

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_EVENT_FWD_SOCKET_CONNECT_FAILED

Description: Event Forwarder failed to connect the destination for TCP based forwarding

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_EVENT_FWD_SOCKET_WRITE_FAILED

Description: Event Forwarder failed to write to socket for sending events

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

Use Case: Collector failing to send events to Worker on time

- [PH_COLLECTOR_EVENT_STORE_DELAYED](#)

EventType: PH_COLLECTOR_EVENT_STORE_DELAYED

Description: Collector event file delayed

Severity: 9 (High)

Event Category: 3 (System Logs)

Use Case: Collector failing to send events to Workers

- [PH_EVENT_PKG_FILE_UPLOAD_FAILED](#)
- [PH_EVENT_PKG_HTTP_FAILED](#)
- [PH_EVENT_PKG_HTTP_INIT_FAILED](#)
- [PH_EVT_PACKAGER_FILE_UPLOAD_FAILURE](#)

EventType: PH_EVENT_PKG_FILE_UPLOAD_FAILED

Description: Event Packager failed to upload event file to Worker or Super; will retry

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
serverIpAddr	Server IP	IP	

EventType: PH_EVENT_PKG_HTTP_FAILED

Description: Event Packager encountered HTTPS error response code

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_EVENT_PKG_HTTP_INIT_FAILED

Description: Event Packager HTTP client initialization failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_EVT_PACKAGER_FILE_UPLOAD_FAILURE

Description: FortiSIEM Event Packager file upload failure

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

Use Case: Collector/Worker to Supervisor communication issue

- [PH_COLLECTOR_DOWN](#)
- [PH_WORKER_DOWN](#)

EventType: PH_COLLECTOR_DOWN

Description: Collector down

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_WORKER_DOWN

Description: Worker down

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Use Case: Devices not sending logs

- [PH_DEV_MON_LOG_DEVICE_DELAY_HIGH](#)
- [PH_DEV_MON_LOG_DEVICE_DELAY_LOW](#)

EventType: PH_DEV_MON_LOG_DEVICE_DELAY_HIGH

Description: Log receipt delay for a single device crossed high water mark

Notes: This event is generated by FortiSIEM Supervisor node when no events are received from a single source IP (Reporting IP) within a (high threshold) time window. The time period can be set in two ways:

- Global Setting: Set the EventRecvTimeGapHigh attribute in Admin > Device Support > Custom Properties. By default it is set to 10 minutes
- Per device Setting: Set the "Event Receive Time Gap High Threshold minutes" attribute in CMDB > Choose a Device > Edit > Device Properties

An event is generated for each jobType, e.g. Syslog, Windows Agent Log Collection, Linux Agent Log Collection, Cloud Service Log Collection etc.

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_LOG_DEVICE_DELAY_LOW

Description: Log receipt delay for a single device fell below water mark

Notes: This event is generated by FortiSIEM Supervisor node when no events are received from a single source IP (Reporting IP) within a (low threshold) time window. The time period can be set in two ways:

- Global Setting: Set the EventRecvTimeGapLow attribute in Admin > Device Support > Custom Properties. By default it is set to 5 minutes
- Per device Setting: Set the "Event Receive Time Gap Low Threshold minutes" attribute in CMDB > Choose a Device > Edit > Device Properties

An event is generated for each jobType, e.g. Syslog, Windows Agent Log Collection, Linux Agent Log Collection, Cloud Service Log Collection etc.

Severity: 1 (Low)

Event Category: 3 (System Logs)

Use Case: EPS License Exceeded

- [PH_PARSER_GLOBAL_LICENSE_EXCEED](#)

EventType: PH_PARSER_GLOBAL_LICENSE_EXCEED

Description: Global EPS license exceeded and events will be dropped

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
licenseEventsPerSec	License EPS	uint64	

Use Case: EPS Reporting

- PH_SYSTEM_EPS_GLOBAL
- PH_SYSTEM_EPS_NODE
- PH_SYSTEM_EPS_ORG

EventType: PH_SYSTEM_EPS_GLOBAL

Description: FortiSIEM Global event handling statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
licenseEventsPerSec	License EPS	uint64	
incomingEventsPerSec	Incoming Event Rate	double	This is a FortiSIEM event ingestion rate calculated every 3 minutes, divided by 180 to generate a rolling EPS (Events Per Second) interval.
peakIncomingEventsPerSec	Peak Incoming Event Rate	double	This is the spike or max event ingestion rate seen during a 3 minute interval averaged overall data points.
dropLicenseEventsPerSec	License Dropped Event Rate	double	The number of events dropped due to exceeding license in past 3 minutes.
peakDropLicenseEventsPerSec	Peak License Dropped Event Rate	double	The max value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.
unusedEvents	Unused Event Count	uint64	The difference between licenseEventsPerSec and incomingEventsPerSec accumulated.

EventType: PH_SYSTEM_EPS_NODE

Description: FortiSIEM per Node event handling statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
role	Role	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
guaranteedEventsPerSec	Guaranteed EPS	uint64	
incomingEventsPerSec	Incoming Event Rate	double	This is a FortiSIEM event ingestion rate calculated every 3 minutes, divided by 180 to generate a rolling EPS (Events Per Second) interval.
peakIncomingEventsPerSec	Peak Incoming Event Rate	double	This is the spike or max event ingestion rate seen during a 3 minute interval averaged overall data points.
ingestedEventsPerSec	Ingested Event Rate	double	
dropPolicyEvents	Policy Dropped Events	uint64	The number of events dropped by Event Dropping Rules in the last 3 minutes.
dropPolicyEventsPerSec	Policy Droppped Event Rate	double	This is the per second count of events dropped by policy, which is calculated as dropPolicyEvents (3min interval) / 180 seconds.
peakDropPolicyEventsPerSec	Peak Policy Dropped Event Rate	double	The max value of dropPolicyEventsPerSec, over all 3-minute periods, since phParser started.
dropLicenseEvents	License Dropped Events	uint64	This is the total count of events dropped due to exceeding license over all 3 minute intervals since phParser started.
dropLicenseEventsPerSec	License Dropped Event Rate	double	The number of events dropped due to exceeding license in past 3 minutes.
peakDropLicenseEventsPerSec	Peak License Dropped Event Rate	double	The max value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.
dropLicenseEventRatio	License Dropped Event Ratio	uint16	Ratio of dropped events due to license to total incoming events in last 3 minutes.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_SYSTEM_EPS_ORG

Description: FortiSIEM per Organization event handling statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
incomingEventsPerSec	Incoming Event Rate	double	This is a FortiSIEM event ingestion rate calculated every 3 minutes, divided by 180 to generate a rolling EPS (Events Per Second) interval.
peakIncomingEventsPerSec	Peak Incoming Event Rate	double	This is the spike or max event ingestion rate seen during a 3 minute interval averaged overall data points.
dropLicenseEventsPerSec	License Dropped Event Rate	double	The number of events dropped due to exceeding license in past 3 minutes.
peakDropLicenseEventsPerSec	Peak License Dropped Event Rate	double	The max value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.

Use Case: Event Archiving Error (Elasticsearch to EventDB/NFS)

- [PH_ES_COLD_STORAGE_ARCHIVING_FAILED](#)
- [PH_ES_HOT_STORAGE_ARCHIVING_FAILED](#)
- [PH_ES_WARM_STORAGE_ARCHIVING_FAILED](#)

EventType: PH_ES_COLD_STORAGE_ARCHIVING_FAILED

Description: Failed to archive indices from cold nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_HOT_STORAGE_ARCHIVING_FAILED

Description: Failed archive indices from hot nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_WARM_STORAGE_ARCHIVING_FAILED

Description: Failed to archive indices from warm nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

Use Case: Event Archiving Error (EventDB to EventDB/NFS)

- PH_SYSTEM_ARCHIVE_PURGING_POLICY_FAILED
- PH_SYSTEM_DISK_ARCHIVING_FAILED

EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_FAILED

Description: Failed to purge Archive FortiSIEM EventDB - purge caused by policy

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_ARCHIVING_FAILED

Description: Online FortiSIEM EventDB Archiving encountered errors

Severity: 10 (High)

Event Category: 3 (System Logs)

Use Case: FortiSIEM Process is Down

- PH_APPSERVER_FRAMEWORK_SECURITY_INIT_SYSTEM_ERROR
- PH_MODULE_ABORT

- [PH_MODULE_ABORT_FOUND](#)
- [PH_MODULE_EXITING](#)
- [PH_MODULE_INIT_FAILURE](#)

EventType: PH_APPSERVER_FRAMEWORK_SECURITY_INIT_SYSTEM_ERROR

Description: App Server Phoenix Caching system initialization failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MODULE_ABORT

Description: Module exited abnormally

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
coreDumpFile	Coredump File Name	string	

EventType: PH_MODULE_ABORT_FOUND

Description: Module found aborted

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	
eventTime	Event Occur Time	Date	

EventType: PH_MODULE_EXITING**Description:** Module exiting**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**EventType: PH_MODULE_INIT_FAILURE****Description:** Module initialization failure**Severity:** 6 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
module	Module Name	string	

Use Case: FortiSIEM process to Supervisor communication issue

- [PH_DATAMANAGER_HTTP_UPLOAD_ERROR](#)
- [PH_DISCOV_DISCOV_REQ_GET_FAILED](#)
- [PH_DISCOV_TEST_CONN_GET_REQ_FAILED](#)
- [PH_EVT_PACKAGER_HTTP_RESPONSE_ERROR](#)
- [PH_IDENTITYMASTER_HTTP_UPLOAD_ERROR](#)
- [PH_MONITOR_UNABLE_CONTACT_APPSVR](#)
- [PH_PARSER_HTTP_RESPONSE_ERROR](#)
- [PH_PARSER_HTTP_UPLOAD_FAILURE](#)

EventType: PH_DATAMANAGER_HTTP_UPLOAD_ERROR**Description:** Data Manager module failed to upload event database statistics to App server**Severity:** 9 (High)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_EVT_PACKAGER_HTTP_RESPONSE_ERROR

Description: FortiSIEM Event Packager http response error from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_IDENTITYMASTER_HTTP_UPLOAD_ERROR

Description: Identity Master failed to upload identity location information to App server

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_UNABLE_CONTACT_APPSVR

Description: phMonitor uable to contact App Server - see respnse code

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
httpStatusCode	HTTP Status	string	

EventType: PH_PARSER_HTTP_RESPONSE_ERROR

Description: Parser module failed to get response from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_PARSER_HTTP_UPLOAD_FAILURE

Description: Parser module failed to upload information to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Use Case: GUI Change Audit

- PH_AUDIT_CASE_CLOSED
- PH_AUDIT_CASE_CREATED
- PH_AUDIT_CASE_UPDATED
- PH_AUDIT_CMDB_DISK_PRUNE_FAILED
- PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS
- PH_AUDIT_DASHBOARD_SHARED
- PH_AUDIT_DEVICE_ADDED
- PH_AUDIT_DEVICE_DELETED
- PH_AUDIT_DEVICE_DISCOVERY_ITEM_CHANGED
- PH_AUDIT_DEVICE_MERGED_BY_IP_WITH_DIFF_NAME
- PH_AUDIT_DEVICE_STATUS_CHANGED
- PH_AUDIT_GROUP_CREATED
- PH_AUDIT_GROUP_DELETED

- PH_AUDIT_INCIDENT_SYS_CLEAR
- PH_AUDIT_INCIDENT_USER_CLEAR
- PH_AUDIT_MALWARE_DATA_DELETED
- PH_AUDIT_MALWARE_DATA_UPDATED
- PH_AUDIT_OBJECT_CREATED
- PH_AUDIT_OBJECT_DELETED
- PH_AUDIT_OBJECT_UPDATED
- PH_AUDIT_PASSWORD_CHANGED
- PH_AUDIT_REPORT_SCHEDULED
- PH_AUDIT_RULE_ACTIVATED
- PH_AUDIT_RULE_DEACTIVATED
- PH_AUDIT_USER_ADDED
- PH_AUDIT_USER_DEFAULT_ROLE_CHANGED
- PH_AUDIT_USER_DELETED
- PH_AUDIT_USER_ORGANIZATION_ROLE_CHANGED
- PH_AUDIT_USER_ORGANIZATION_ROLE_ENABLED
- PH_AUDIT_USER_ORGANIZATION_ROLE_REMOVED

EventType: PH_AUDIT_CASE_CLOSED

Description: FortiSIEM Case Closed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
comment	Comment	string	

EventType: PH_AUDIT_CASE_CREATED

Description: FortiSIEM Case Created

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

EventType: PH_AUDIT_CASE_UPDATED

Description: FortiSIEM Case Updated

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_CMDB_DISK_PRUNE_FAILED

Description: CMDB Disk Prune Failed

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
freeDiskMB	Free Disk MB	uint32	

EventType: PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS

Description: CMDB Disk Prune Success

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
freeDiskMB	Free Disk MB	uint32	

EventType: PH_AUDIT_DASHBOARD_SHARED

Description: FortiSIEM dashboard folder shared

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	
targetUserGrp	Target User Group	string	

EventType: PH_AUDIT_DEVICE_ADDED

Description: System CMDB device added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_AUDIT_DEVICE_DELETED

Description: System CMDB device deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_AUDIT_DEVICE_DISCOVERY_ITEM_CHANGED

Description: System CMDB device changed by discovery

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
objType	Object Type	string	
addedItem	Added Item	string	

EventType: PH_AUDIT_DEVICE_MERGED_BY_IP_WITH_DIFF_NAME

Description: Two devices with different hostname merged because of overlapping IP addresses

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
targetHostName	Target Host Name	string	
overlapIp	Overlapping IP	string	This field represents the list of IP addresses of a just discovered device that overlaps with an existing device in CMDB.

EventType: PH_AUDIT_DEVICE_STATUS_CHANGED

Description: CMDB Device audit status changed

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
origStatus	Original Status	string	
newStatus	New Status	string	
eventSource	Event Source	string	

EventType: PH_AUDIT_GROUP_CREATED

Description: FortiSIEM GUI Group Created

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
osObjName	Object Name	string	
osObjType	OS Object Type	string	

EventType: PH_AUDIT_GROUP_DELETED

Description: FortiSIEM GUI Group Deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
osObjName	Object Name	string	
osObjType	OS Object Type	string	

EventType: PH_AUDIT_INCIDENT_SYS_CLEAR

Description: FortiSIEM Incident System Auto-Cleared

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	
osObjHandleID	Object Handle	string	

EventType: PH_AUDIT_INCIDENT_USER_CLEAR

Description: FortiSIEM Incident User Cleared

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	
osObjHandleID	Object Handle	string	

EventType: PH_AUDIT_MALWARE_DATA_DELETED

Description: Malware data deleted by scheduled update

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
updateTime	Update Time	Date	

Id	Display name	Type	Description
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.
folder	Folder	string	

EventType: PH_AUDIT_MALWARE_DATA_UPDATED

Description: Malware data updated by scheduled update

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
updateTime	Update Time	Date	
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.
folder	Folder	string	

EventType: PH_AUDIT_OBJECT_CREATED

Description: System data object created

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjType	OS Object Type	string	
osObjName	Object Name	string	

EventType: PH_AUDIT_OBJECT_DELETED

Description: System data object deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	

EventType: PH_AUDIT_OBJECT_UPDATED

Description: System data object updated

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjType	OS Object Type	string	
objType	Object Type	string	
osObjName	Object Name	string	
osObjAction	Object Action	string	
targetCustomer	Target Organization Name	string	
oldSettingsValue	Old Settings Value	string	
newSettingsValue	New Settings Value	string	

EventType: PH_AUDIT_PASSWORD_CHANGED

Description: System user password changed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
user	User	string	
domain	Domain	string	

EventType: PH_AUDIT_REPORT_SCHEDULED

Description: FortiSIEM Report Scheduled

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_RULE_ACTIVATED

Description: FortiSIEM Rule activated

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	

EventType: PH_AUDIT_RULE_DEACTIVATED

Description: FortiSIEM Rule de-activated

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	

EventType: PH_AUDIT_USER_ADDED

Description: System user added

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
user	User	string	
domain	Domain	string	

EventType: PH_AUDIT_USER_DEFAULT_ROLE_CHANGED

Description: FortiSIEM Admin User Default Role Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
targetCustomer	Target Organization Name	string	
role	Role	string	

EventType: PH_AUDIT_USER_DELETED

Description: System user deleted

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
user	User	string	
targetUser	Target User	string	
details	Details	string	

EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_CHANGED

Description: FortiSIEM Admin User Organization Role changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
targetCustomer	Target Organization Name	string	
role	Role	string	

EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_ENABLED

Description: FortiSIEM Admin User Organization Role enabled

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_REMOVED

Description: FortiSIEM Admin User Organization Role disabled

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	

Id	Display name	Type	Description
targetCustomer	Target Organization Name	string	
role	Role	string	

Use Case: GUI User Login

- PH_AUDIT_ACCOUNT_LOCKED
- PH_AUDIT_USER_LOGIN_FAILURE
- PH_AUDIT_USER_LOGIN_SUCCESS
- PH_AUDIT_USER_LOGOFF

EventType: PH_AUDIT_ACCOUNT_LOCKED

Description: System user account locked due to excessive login failures

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
reason	Reason	string	
targetUser	Target User	string	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.

EventType: PH_AUDIT_USER_LOGIN_FAILURE

Description: System user failed to login

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
domain	Domain	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_AUDIT_USER_LOGIN_SUCCESS

Description: System user login success

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
userFullName	User Full Name	string	

EventType: PH_AUDIT_USER_LOGOFF

Description: System user logoff

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
userFullName	User Full Name	string	

Use Case: Incident External Integration issue

- [PH_APPSERVER_IN_INTEGRATION_ERROR](#)
- [PH_APPSERVER_OUT_INTEGRATION_ERROR](#)

EventType: PH_APPSERVER_IN_INTEGRATION_ERROR

Description: Inbound external ticketing system integration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_OUT_INTEGRATION_ERROR

Description: Outbound external ticketing system integration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Use Case: Incident email notification issue

- [PH_APPSERVER_NOTIFIER_ERROR](#)
- [PH_INCIDENT_ACTION_STATUS](#)

EventType: PH_APPSERVER_NOTIFIER_ERROR

Description: App Server Notifier error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_INCIDENT_ACTION_STATUS

Description: Record action result for incident notification

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
scriptOutput	Script Output	string	

Use Case: Linux Agent operational errors

- PH_FAILED_TO_EXEC
- PH_LINUX_AGENT_BIND_PORT_FAILED
- PH_LINUX_AGENT_CONFIG_ATTR_NOT_FOUND
- PH_LINUX_AGENT_CREATE_SOCKET_FAILED
- PH_LINUX_AGENT_HOST_IP_GOT_FAILED
- PH_LINUX_AGENT_OPEN_FILE_FAILED
- PH_LINUX_AGENT_OPEN_PORT_FAILED
- PH_LINUX_AGENT_RECV_ERROR
- PH_LINUX_AGENT_VERIFIER_ERROR

EventType: PH_FAILED_TO_EXEC

Description: Failed to execute specified command

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_BIND_PORT_FAILED

Description: Socket failed to bind port

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_LINUX_AGENT_CONFIG_ATTR_NOT_FOUND

Description: Cannot find attribute in config file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_LINUX_AGENT_CREATE_SOCKET_FAILED

Description: Failed to create socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LINUX_AGENT_HOST_IP_GOT_FAILED

Description: Failed to get host ip

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_OPEN_FILE_FAILED

Description: Linux agent open file failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LINUX_AGENT_OPEN_PORT_FAILED

Description: Failed to open port

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ipPort	IP Port	uint16	IP port number

EventType: PH_LINUX_AGENT_RECV_ERROR

Description: Linux agent received error from socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.

EventType: PH_LINUX_AGENT_VERIFIER_ERROR

Description: Linux agent verifier error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
size	Size	uint32	

Use Case: Malware IOC handling Errors

- [PH_APPSERVER_EXT_THREAT_INTEL_UPDATE_ERROR](#)
- [PH_APPSERVER_FORTIGUARD_IOC_INTEGRATION_ERROR](#)
- [PH_APPSERVER_IOC_TASK_CREATE_FAILED_ERROR](#)

EventType: PH_APPSERVER_EXT_THREAT_INTEL_UPDATE_ERROR

Description: External Threat Intelligence update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FORTIGUARD_IOC_INTEGRATION_ERROR

Description: FortiGuard IOC data download/parse error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_IOC_TASK_CREATE_FAILED_ERROR

Description: App Server failed to create External Threat Intelligence Update task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Use Case: Query Errors

- PH_APPSERVER_QUERY_EXPORT_ERROR
- PH_APPSERVER_QUERY_RESULT_RETRIEVE_ERROR
- PH_APPSERVER_QUERY_RUN_ERROR
- PH_APPSERVER_QUERY_STOP_ERROR
- PH_APPSERVER_REPORT_BUNDLE_PRINT_ERROR

EventType: PH_APPSERVER_QUERY_EXPORT_ERROR

Description: App Server failed to export historical query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_RESULT_RETRIEVE_ERROR

Description: App Server failed to retrieve historical query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_RUN_ERROR

Description: App Server failed to run historical query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_STOP_ERROR

Description: App Server failed to stop historical query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_BUNDLE_PRINT_ERROR

Description: Print report bundle error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Use Case: Query Performance

- [PH_AUDIT_QUERY_COMPLETED](#)

EventType: PH_AUDIT_QUERY_COMPLETED

Description: Audit query completed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
osObjName	Object Name	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
durationMSec	Duration	uint32	Duration of a connection (in msec)
queryFilter	Query Filter	string	
queryDisplay	Query Display	string	
queryId	Query Id	string	
usageType	Usage Type	string	

Use Case: Rule Performance

- [PH_RULEMOD_PROFILE](#)

EventType: PH_RULEMOD_PROFILE

Description: FortiSIEM Rule resource usage profile

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleName	Rule Name	string	FortiSIEM rule name.
usedMemKB	Used Memory	uint32	
updateQueueSize	Update Queue Size	uint32	

Use Case: Rule trigger issues

- [PH_DROP_EVENT_FROM_SHARED_BUFFER](#)
- [PH_DROP_INCIDENT](#)
- [PH_REPORT_PACK_FAILED](#)
- [PH_RULEMOD_SUMMARY_UPLOAD_FAILED](#)
- [PH_UTIL_NOTIFICATION_UPLOAD_FAILURE](#)

EventType: PH_DROP_EVENT_FROM_SHARED_BUFFER

Description: Event dropped from shared buffer

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
collectorId	Collector ID	uint32	This field captures the ID of a FortiSIEM Collector

Id	Display name	Type	Description
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_DROP_INCIDENT

Description: Incident dropped

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.
incidentId	Incident ID	uint64	Unique ID of a FortiSIEM Incident
details	Details	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_REPORT_PACK_FAILED

Description: Failed to pack data

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_SUMMARY_UPLOAD_FAILED

Description: Rule Worker failed to upload rule summary to Rule Master, causing potential incident loss.

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_UTIL_NOTIFICATION_UPLOAD_FAILURE

Description: Failed to Send Notification

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

Use Case: Scheduled Report issue

- [PH_REPORT_ACTION_STATUS](#)

EventType: PH_REPORT_ACTION_STATUS

Description: Record action result for report notification

Severity: 1 (Low)

Event Category: 3 (System Logs)

Use Case: Test Connectivity/Discovery Errors

- PH_DISCOV_DISCOV_REQ_GET_FAILED
- PH_DISCOV_RESULT_SEND_FAILED
- PH_DISCOV_TEST_CONN_GET_REQ_FAILED
- PH_DISCOV_TEST_CONN_RESULT_SEND_ERROR

EventType: PH_DISCOV_DISCOV_REQ_GET_FAILED

Description: Discovery module failed to get discovery request from App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_RESULT_SEND_FAILED

Description: Discovery module failed to send discovery result to App server after many retries; discovery will fail

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_TEST_CONN_GET_REQ_FAILED

Description: Discovery module failed to get test connectivity request from App server

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TEST_CONN_RESULT_SEND_ERROR

Description: Discovery module encountered error in sending Test Connectivity result to app server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovFailCode	PH Discovery Failure Code	string	

Use Case: Windows/Linux Agent operational errors

- [PH_AUDIT_AGENT_DISABLED](#)
- [PH_AUDIT_AGENT_NOTRESPONDING](#)
- [PH_AUDIT_AGENT_UNINSTALLED](#)

EventType: PH_AUDIT_AGENT_DISABLED

Description: FortiSIEM Windows/Linux Agent disabled

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_NOTRESPONDING

Description: FortiSIEM Windows/Linux Agent not responding

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_UNINSTALLED

Description: FortiSIEM Windows/Linux Agent uninstalled

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

Use Case: Worker failing to store events in ClickHouse

- [PH_CLICKHOUSE_INSERTION_DROP_EVENTS](#)
- [PH_DATAMANAGER_CLICKHOUSE_HTTP_UPLOAD_ERROR](#)

EventType: PH_CLICKHOUSE_INSERTION_DROP_EVENTS

Description: FortiSIEM dropped events while failing to insert them to ClickHouse after retries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_DATAMANAGER_CLICKHOUSE_HTTP_UPLOAD_ERROR

Description: Failed to upload events to ClickHouse

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
serverName	Server Name	string	

Use Case: Worker failing to store events in Elasticsearch

- [PH_DATAMANAGER_EVTLOADER_ERROR](#)
- [PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FAIL](#)

EventType: PH_DATAMANAGER_EVTLOADER_ERROR

Description: Data Manager failed to load events from shared buffer

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
dirName	Directory Name	string	

EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FAIL

Description: Elasticsearch indexing failed at the last time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
size	Size	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

Use Case: Worker failing to store events in EventDB

- [PH_DATAMANAGER_EVTLOADER_ERROR](#)
- [PH_DATAMANAGER_SUMMARYWRITER_ERROR](#)
- [PH_UNABLE_ACCESS_DIR](#)
- [PH_UNABLE_CREATE_DIR](#)
- [PH_UNABLE_OPEN_DIR](#)

EventType: PH_DATAMANAGER_SUMMARYWRITER_ERROR

Description: Data Manager failed to write inline report results

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_UNABLE_ACCESS_DIR**Description:** Unable to access archive directory**Severity:** 10 (High)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_UNABLE_CREATE_DIR**Description:** Unable to create dir**Severity:** 6 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
dirName	Directory Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_UNABLE_OPEN_DIR**Description:** Unable to open dir**Severity:** 6 (Medium)**Event Category:** 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

Use Case: Worker falling behind in storing configuration files to SVN-lite

- [PH_EVT_HANDLER_SVN_QUEUE_WARNING](#)

EventType: PH_EVT_HANDLER_SVN_QUEUE_WARNING

Description: Worker Input Event Queue large

Severity: 10 (High)

Event Category: 3 (System Logs)

Use Case: Worker falling behind in storing events to Event Database

- [PH_EVT_HANDLER_EVT_QUEUE_LARGE](#)
- [PH_EVT_HANDLER_EVT_QUEUE_WARNING](#)

EventType: PH_EVT_HANDLER_EVT_QUEUE_LARGE

Description: Uploaded event files on Worker has a size of more than 100MB

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_EVT_QUEUE_WARNING

Description: Worker Input Event Queue large

Severity: 10 (High)

Event Category: 3 (System Logs)

AppServer Logs

This section provides logs generated by the App Server module

- PH_APPSERVER_ADMIN_AGENT_GET_UPDATE_FAILED_ERROR
- PH_APPSERVER_ADMIN_AGENT_UNKOWN_TASK_ID_ERROR
- PH_APPSERVER_ADMIN_CUST_GENERATE_KEY_ERROR
- PH_APPSERVER_ADMIN_GET_RESOURCE_FAILED
- PH_APPSERVER_ADMIN_LOCATE_KEY_FAILED
- PH_APPSERVER_ADMIN_RESET_FIELD_FAILED_ERROR
- PH_APPSERVER_AUDIT_REPORT_EXPORT_ERROR
- PH_APPSERVER_BEACON_LIB_ERROR
- PH_APPSERVER_BEACON_REGISTER_ERROR
- PH_APPSERVER_BEACON_SERVER_ERROR
- PH_APPSERVER_BEACON_WEB_SERVER_ERROR
- PH_APPSERVER_BEAN_REF_CHECK_WARN
- PH_APPSERVER_BEAN_SYNC_PROPERTIES_ERROR
- PH_APPSERVER_BEAN_TO_VALUE_ERROR
- PH_APPSERVER_BEAN_TO_XML_ERROR
- PH_APPSERVER_BEAN_VALUE_TO_BEAN_ERROR
- PH_APPSERVER_CMDB_REPORT_DATA_ERROR
- PH_APPSERVER_CMDB_REPORT_EXPORT_ERROR
- PH_APPSERVER_CMDB_REPORT_IMPORT_ERROR
- PH_APPSERVER_CMDB_REPORT_QUERY_ERROR
- PH_APPSERVER_CMDB_REPORT_TYPE_ERROR
- PH_APPSERVER_COLLECTOR_INFO_ERROR
- PH_APPSERVER_COLLECTOR_LICENSE_ERROR
- PH_APPSERVER_COLLECTOR_STATUS_ERROR
- PH_APPSERVER_COMMONPWD_EXPORT_ERROR
- PH_APPSERVER_DASHBOARD_DATA_ERROR
- PH_APPSERVER_DASHBOARD_HTML_BUILD_XML_ERROR
- PH_APPSERVER_DASHBOARD_WIDGET_ERROR
- PH_APPSERVER_DATA_IMPORT_ERROR
- PH_APPSERVER_DATA_ROBUST_INFO_ERROR
- PH_APPSERVER_DB_CONNECTION_CLOSE_ERROR
- PH_APPSERVER_DB_DATA_ERROR
- PH_APPSERVER_DB_DELETE_ERROR
- PH_APPSERVER_DB_QUERY_ERROR
- PH_APPSERVER_DB_UPDATE_ERROR
- PH_APPSERVER_DISCOVERY_CREDENTIAL_DECRYPT_PASSWORD_WARN
- PH_APPSERVER_DISCOVERY_RESULT_ENCRYPT_XML_ELEMENT_ERROR

- PH_APPSERVER_DISCOVERY_RESULT_ERROR
- PH_APPSERVER_DISCOVERY_RESULT_UNKOWN_TASK_ID_ERROR
- PH_APPSERVER_EAMIL_GENERATE_EVENT_ERROR
- PH_APPSERVER_ELASTIC_UPDATE_ERROR
- PH_APPSERVER_EMAIL_PREPARE_DATA_ERROR
- PH_APPSERVER_EVENTDB_EXPORT_ERROR
- PH_APPSERVER_EVENT_ATTRIBUTE_BUILD_XML_ERROR
- PH_APPSERVER_EXPORT_ERROR
- PH_APPSERVER_EXT_THREAT_INTEL_DOWNLOAD_ERROR
- PH_APPSERVER_EXT_THREAT_INTEL_PARSE_ERROR
- PH_APPSERVER_EXT_THREAT_INTEL_UPDATE_ERROR
- PH_APPSERVER_FILE_NOT_FOUND
- PH_APPSERVER_FILE_READ_ERROR
- PH_APPSERVER_FILE_SYSTEM_ERROR
- PH_APPSERVER_FILE_WRITE_ERROR
- PH_APPSERVER_FLEX_INTERCEPTOR_NO_LOGIN_EXCEPTION_ERROR
- PH_APPSERVER_FORTIGUARD_IOC_INTEGRATION_ERROR
- PH_APPSERVER_FRAMEWORK_REGISTER_ERROR
- PH_APPSERVER_FRAMEWORK_RUN_THREAD_ERROR
- PH_APPSERVER_FRAMEWORK_SECURITY_CHECK_LICENSE_WARN
- PH_APPSERVER_FRAMEWORK_SECURITY_GET_ENTITY_MANAGER_ERROR
- PH_APPSERVER_FRAMEWORK_SECURITY_GET_RS_EXPIRATION_ERROR
- PH_APPSERVER_FRAMEWORK_SECURITY_INIT_SYSTEM_ERROR
- PH_APPSERVER_FRAMEWORK_SERVICE_MISSED_WARN
- PH_APPSERVER_FRAMEWORK_SHUTDOWN_SERVICE_STARTER_WARN
- PH_APPSERVER_GENERIC_ERROR
- PH_APPSERVER_GENERIC_INFO
- PH_APPSERVER_GENERIC_WARN
- PH_APPSERVER_GET_MAX_CONFIG_ITEM_COUNT_ERROR
- PH_APPSERVER_GROUP_DATA_ERROR
- PH_APPSERVER_IDENTITYLOCATION_EXPORT_ERROR
- PH_APPSERVER_INCIDENT_NOTIFY_ERROR
- PH_APPSERVER_INCIDENT_UPDATE_ERROR
- PH_APPSERVER_INTEGRATION_ERROR
- PH_APPSERVER_INTEGRATION_UPDATE_POLICY_ERROR
- PH_APPSERVER_INTEGRATION_UPDATE_POLICY_WARN
- PH_APPSERVER_INTEGRATION_WARN
- PH_APPSERVER_IN_INTEGRATION_ERROR
- PH_APPSERVER_IOC_LICENSE_CHECK_FAILED_WARN
- PH_APPSERVER_IOC_TASK_CREATE_FAILED_ERROR
- PH_APPSERVER_JOB_DISTRIBUTE_ERROR
- PH_APPSERVER_LICENSE_EXPIRY_ERROR
- PH_APPSERVER_LICENSE_VALIDATION_ERROR

- PH_APPSERVER_LOGIN_ERROR
- PH_APPSERVER_LOG_INTEGRITY_ERROR
- PH_APPSERVER_MONITOR_AUDIT_PERF_ERROR
- PH_APPSERVER_MONITOR_HEALTH_CONFIG_SET_ERROR
- PH_APPSERVER_NETSEGMENT_EXPORT_ERROR
- PH_APPSERVER_NOTIFICATION_EMAIL_GET_RESOURCE_FAILED
- PH_APPSERVER_NOTIFICATION_ERROR
- PH_APPSERVER_NOTIFICATION_JMS_CONNECTION_ERROR
- PH_APPSERVER_NOTIFICATION_UPDATE_ERROR
- PH_APPSERVER_NOTIFIER_ERROR
- PH_APPSERVER_NO_WATCHLIST_SELECTED_WARN
- PH_APPSERVER_OPENPROXY_EXPORT_ERROR
- PH_APPSERVER_OUT_INTEGRATION_ERROR
- PH_APPSERVER_PARSER_IMPORT_ERROR
- PH_APPSERVER_PARSER_UPDATE_ERROR
- PH_APPSERVER_PARSING_CONSTRAINT_ERROR
- PH_APPSERVER_PDF_BUILDER_ERROR
- PH_APPSERVER_PERFMON_TASK_ERROR
- PH_APPSERVER_QUERY_CHECK_POLICY_ACTION_WARN
- PH_APPSERVER_QUERY_EXPORT_ERROR
- PH_APPSERVER_QUERY_RESULT_PARSER_ERROR
- PH_APPSERVER_QUERY_RESULT_RETRIEVE_ERROR
- PH_APPSERVER_QUERY_RUN_ERROR
- PH_APPSERVER_QUERY_STOP_ERROR
- PH_APPSERVER_QUERY_STRING_ESCAPE_ERROR
- PH_APPSERVER_RBAC_ERROR
- PH_APPSERVER_RBAC_NO_PERMISSION_WARN
- PH_APPSERVER_REALTIME_QUERY_ERROR
- PH_APPSERVER_REMEDY_ERROR
- PH_APPSERVER_REPORT_BUNDLE_PRINT_ERROR
- PH_APPSERVER_REPORT_COMPILE_ERROR
- PH_APPSERVER_REPORT_DEVICE_COMPONENT_SN_ERROR
- PH_APPSERVER_REPORT_DEVICE_DETAIL_ERROR
- PH_APPSERVER_REPORT_DEVICE_SN_ERROR
- PH_APPSERVER_REPORT_DEVICE_SUMMARY_ERROR
- PH_APPSERVER_REPORT_EXPORT_ERROR
- PH_APPSERVER_REPORT_FAILED_BLOCK_SUMMARY_ERROR
- PH_APPSERVER_REPORT_FIRE_TRIGGER_EVENT_ERROR
- PH_APPSERVER_REPORT_GET_PH_CONFIG_ERROR
- PH_APPSERVER_REPORT_IDENTITY_AND_LOCATION_ERROR
- PH_APPSERVER_REPORT_LOG_FILE_SUMMARY_ERROR
- PH_APPSERVER_REPORT_TEMPLATE_GENERATE_PDF_ERROR
- PH_APPSERVER_REPORT_TEMPLATE_INIT_IMAGE_ERROR

- PH_APPSERVER_REPORT_TEMPLATE_INIT_PARM_ERROR
- PH_APPSERVER_REPORT_TEMPLATE_PDF_SUMMARY_ERROR
- PH_APPSERVER_REPORT_TICKET_SUMMARY_ERROR
- PH_APPSERVER_REPORT_UPDATE_ERROR
- PH_APPSERVER_REPORT_USER_SUMMARY_ERROR
- PH_APPSERVER_REST_ERROR
- PH_APPSERVER_REST_H5_ERROR
- PH_APPSERVER_RISKSCORE_CALCULATE_ERROR
- PH_APPSERVER_RULE_ACTIVE_ERROR
- PH_APPSERVER_RULE_CLONE_ERROR
- PH_APPSERVER_RULE_DEBUG_INVALID_EVENT_DB_ID_ERROR
- PH_APPSERVER_RULE_DEBUG_WORKERS_SETTING_ERROR
- PH_APPSERVER_RULE_TEST_ERROR
- PH_APPSERVER_RULE_UPDATE_ERROR
- PH_APPSERVER_SCHEDULE_ERROR
- PH_APPSERVER_SCHEDULE_UPDATE_ERROR
- PH_APPSERVER_SECURITY_ERROR
- PH_APPSERVER_SERVLET_ERROR
- PH_APPSERVER_SERVLET_NO_ACCESS_TO_URI_WARN
- PH_APPSERVER_SOCKET_COMM_ERROR
- PH_APPSERVER_SVN_ERROR
- PH_APPSERVER_SYNC_UPDATE_CONFIG_ERROR
- PH_APPSERVER_SYSCONFIG_GET_ERROR
- PH_APPSERVER_SYSTEM_WINAGENT_REGISTER_WARN
- PH_APPSERVER_SYS_APPLICATION_ERROR
- PH_APPSERVER_SYS_DATA_UPDATE_ERROR
- PH_APPSERVER_TASK_CREATE_ERROR
- PH_APPSERVER_TASK_FLEX_RESULT_BUILD_XML_ERROR
- PH_APPSERVER_TASK_GET_ERROR
- PH_APPSERVER_TASK_UPDATE_ERROR
- PH_APPSERVER_TICKET_EXPORT_ERROR
- PH_APPSERVER_UPDATER_FIND_EXIST_USER_BY_NOTHING_ERROR
- PH_APPSERVER_USERAGENT_EXPORT_ERROR
- PH_APPSERVER_VULNERABILITY_IGNORE_WARN
- PH_APPSERVER_WATCHLIST_ADD_TO_DISTIRBUTED_QUEUE
- PH_APPSERVER_WATCHLIST_EXPORT_ERROR
- PH_APPSERVER_WATCHLIST_IMPORT_ERROR
- PH_APPSERVER_WATCHLIST_IMPORT_WARN
- PH_APPSERVER_WATCHLIST_UPDATE_ERROR
- PH_APPSERVER_WEBSERVICE_UPDATE_TASK_ERROR
- PH_APPSERVER_WORKER_PROVISION_FAILED
- PH_APPSERVER_WS_COMM_ERROR
- PH_APPSERVER_XML_PARSE_ERROR

- PH_AUDIT_ACCOUNT_LOCKED
- PH_AUDIT_AGENT_DISABLED
- PH_AUDIT_AGENT_INSTALLED
- PH_AUDIT_AGENT_NOTRESPONDING
- PH_AUDIT_AGENT_RUNNING
- PH_AUDIT_AGENT_STARTED
- PH_AUDIT_AGENT_STOPPED
- PH_AUDIT_AGENT_UNINSTALLED
- PH_AUDIT_CASE_ASSIGNED
- PH_AUDIT_CASE_CLOSED
- PH_AUDIT_CASE_CREATED
- PH_AUDIT_CASE_EVIDENCE_ADDED
- PH_AUDIT_CASE_EVIDENCE_DELETED
- PH_AUDIT_CASE_INCIDENT_ADDED
- PH_AUDIT_CASE_MERGED
- PH_AUDIT_CASE_NOTE_ADDED
- PH_AUDIT_CASE_NOTE_DELETED
- PH_AUDIT_CASE_NOTE_MODIFIED
- PH_AUDIT_CASE_PRIORITY_CHANGED
- PH_AUDIT_CASE_REASSIGNED
- PH_AUDIT_CASE_STAGE_CHANGED
- PH_AUDIT_CASE_STAT
- PH_AUDIT_CASE_STATUS_CHANGED
- PH_AUDIT_CASE_SUMMARY_CHANGED
- PH_AUDIT_CASE_UPDATED
- PH_AUDIT_CI_QUOTE_EXCEEDED
- PH_AUDIT_CMDB_DISK_PRUNE_FAILED
- PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS
- PH_AUDIT_DASHBOARD_SHARED
- PH_AUDIT_DATA_PURGE
- PH_AUDIT_DB_LEADER_CHANGE
- PH_AUDIT_DEFAULT_PWD_MATCH
- PH_AUDIT_DEVICE_ADDED
- PH_AUDIT_DEVICE_DELETED
- PH_AUDIT_DEVICE_DISCOVERY_ITEM_CHANGED
- PH_AUDIT_DEVICE_MAINTENANCE_ENDED
- PH_AUDIT_DEVICE_MAINTENANCE_STARTED
- PH_AUDIT_DEVICE_MERGED_BY_IP_WITH_DIFF_NAME
- PH_AUDIT_DEVICE_STATUS_CHANGED
- PH_AUDIT_DEVICE_UNMANAGED
- PH_AUDIT_DEV_MON_JOB_NOT_STARTED
- PH_AUDIT_DEV_MON_JOB_STATUS_CHANGE
- PH_AUDIT_DISCOVERY

- PH_AUDIT_EXPORT_REPORT_END
- PH_AUDIT_GENAI_USER_QUERY
- PH_AUDIT_GENERIC
- PH_AUDIT_GROUP_CREATED
- PH_AUDIT_GROUP_DELETED
- PH_AUDIT_INACTIVE_USER_LOGIN
- PH_AUDIT_INCIDENT_SYS_CLEAR
- PH_AUDIT_INCIDENT_USER_CLEAR
- PH_AUDIT_INTEGRATION_POLICY_EXECUTED
- PH_AUDIT_MALWARE_DATA_DELETED
- PH_AUDIT_MALWARE_DATA_UPDATED
- PH_AUDIT_ML_GENERIC_ERROR
- PH_AUDIT_ML_GENERIC_INFO
- PH_AUDIT_ML_INFERENCE_COMPLETED
- PH_AUDIT_ML_INFERENCE_RESULT
- PH_AUDIT_ML_INFERENCE_STARTED
- PH_AUDIT_ML_TRAINING_COMPLETED
- PH_AUDIT_ML_TRAINING_STARTED
- PH_AUDIT_NOTIF_POLICY_EXECUTED
- PH_AUDIT_OBJECT_CREATED
- PH_AUDIT_OBJECT_DELETED
- PH_AUDIT_OBJECT_UPDATED
- PH_AUDIT_ONDEMAND_REMEDIATION_EXECUTED
- PH_AUDIT_PASSWORD_CHANGED
- PH_AUDIT_QUERY_COMPLETED
- PH_AUDIT_QUERY_SCHEDULED
- PH_AUDIT_QUERY_START
- PH_AUDIT_QUERY_STOP
- PH_AUDIT_REPL_LEADER_CHANGE
- PH_AUDIT_REPORT_SCHEDULED
- PH_AUDIT_REPORT_SCHEDULE_APPROVE
- PH_AUDIT_REPORT_SCHEDULE_REQUEST
- PH_AUDIT_REPORT_SERVER_LICENSE_EXPIRED
- PH_AUDIT_REPORT_SERVER_LICENSE_REMOVED
- PH_AUDIT_REPORT_SERVER_LICENSE_TO_EXPIRE
- PH_AUDIT_RISK_DECREASE_LOW
- PH_AUDIT_RISK_DECREASE_MED
- PH_AUDIT_RISK_INCREASE_HIGH
- PH_AUDIT_RISK_INCREASE_MED
- PH_AUDIT_RULE_ACTIVATED
- PH_AUDIT_RULE_ACTIVATION_APPROVE
- PH_AUDIT_RULE_ACTIVATION_REQUEST
- PH_AUDIT_RULE_DEACTIVATED

- PH_AUDIT_RULE_DEACTIVATION_APPROVE
- PH_AUDIT_RULE_DEACTIVATION_REQUEST
- PH_AUDIT_SVC_LOGIN_FAILURE
- PH_AUDIT_SVC_LOGIN_SUCCESS
- PH_AUDIT_SVC_LOGOFF
- PH_AUDIT_SVC_SESSION_TIMEOUT
- PH_AUDIT_TUNNEL_CLOSE
- PH_AUDIT_TUNNEL_OPEN
- PH_AUDIT_USER_ADDED
- PH_AUDIT_USER_CHANGE_ORG_SCOPE
- PH_AUDIT_USER_DEFAULT_ROLE_CHANGED
- PH_AUDIT_USER_DELETED
- PH_AUDIT_USER_LOGIN_FAILURE
- PH_AUDIT_USER_LOGIN_SUCCESS
- PH_AUDIT_USER_LOGOFF
- PH_AUDIT_USER_ORGANIZATION_ROLE_CHANGED
- PH_AUDIT_USER_ORGANIZATION_ROLE_ENABLED
- PH_AUDIT_USER_ORGANIZATION_ROLE_REMOVED
- PH_AUDIT_USER_SESSION_TIMEOUT
- PH_AUDIT_WS_COMM

EventType: PH_APPSERVER_ADMIN_AGENT_GET_UPDATE_FAILED_ERROR

Description: App Server failed to get update

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_ADMIN_AGENT_UNKOWN_TASK_ID_ERROR

Description: App Server detects unkown Admin Agent task ID

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_ADMIN_CUST_GENERATE_KEY_ERROR

Description: App Server failed to generate organization key

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_ADMIN_GET_RESOURCE_FAILED

Description: App Server failed to get resource for admin tab

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_ADMIN_LOCATE_KEY_FAILED

Description: App Server failed to locate resource for admin tab

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_ADMIN_RESET_FIELD_FAILED_ERROR

Description: App Server failed to reset resource for admin tab

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_AUDIT_REPORT_EXPORT_ERROR

Description: Audit Data Export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEACON_LIB_ERROR

Description: App Server Beaconsing library error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEACON_REGISTER_ERROR

Description: App Server Beaconsing Register error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEACON_SERVER_ERROR

Description: App Server Beaconsing Server error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEACON_WEB_SERVER_ERROR

Description: App Server Beaconsing Web Server error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEAN_REF_CHECK_WARN

Description: App Server check entity bean reference warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEAN_SYNC_PROPERTIES_ERROR

Description: App Server entity bean sync properties error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEAN_TO_VALUE_ERROR

Description: App Server entity bean to property value map error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEAN_TO_XML_ERROR

Description: App Server entity to XML generation error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEAN_VALUE_TO_BEAN_ERROR

Description: App Server set value for Entity bean error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_CMDB_REPORT_DATA_ERROR

Description: CMDB Report Data error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_CMDB_REPORT_EXPORT_ERROR

Description: CMDB Report export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_CMDB_REPORT_IMPORT_ERROR

Description: CMDB Report import error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_CMDB_REPORT_QUERY_ERROR

Description: CMDB Report query error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_CMDB_REPORT_TYPE_ERROR

Description: CMDB Report Type error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_COLLECTOR_INFO_ERROR

Description: Collector information error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_COLLECTOR_LICENSE_ERROR

Description: Collector license error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_COLLECTOR_STATUS_ERROR

Description: Collector status error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_COMMONPWD_EXPORT_ERROR

Description: Common password data export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DASHBOARD_DATA_ERROR

Description: Dashbaord Data error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DASHBOARD_HTML_BUILD_XML_ERROR

Description: App Server failed to build dashboard XML content

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DASHBOARD_WIDGET_ERROR

Description: Dashbaord Widget error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DATA_IMPORT_ERROR

Description: App Server failed to import data during initialization

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DATA_ROBUST_INFO_ERROR

Description: Data Robust Info error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DB_CONNECTION_CLOSE_ERROR

Description: PostgreSQL database connection close error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DB_DATA_ERROR

Description: PostgreSQL database data error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DB_DELETE_ERROR

Description: PostgreSQL database data delete error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DB_QUERY_ERROR

Description: PostgreSQL database query error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DB_UPDATE_ERROR

Description: PostgreSQL database data update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DISCOVERY_CREDENTIAL_DECRYPT_PASSWORD_WARN

Description: App Server discovery result credential decrypt error

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DISCOVERY_RESULT_ENCRYPT_XML_ELEMENT_ERROR

Description: App Server discovery result credential encrypt error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DISCOVERY_RESULT_ERROR

Description: App Server failed to process discovery result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DISCOVERY_RESULT_UNKOWN_TASK_ID_ERROR

Description: App Server detects unknown Discovery Result task ID

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EAMIL_GENERATE_EVENT_ERROR

Description: App Server failed to generate raw event for email notification

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_ELASTIC_UPDATE_ERROR

Description: App Server failed to update Elasticsearch configuration

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EMAIL_PREPARE_DATA_ERROR

Description: App Server failed to prepare email body for email notification

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EVENTDB_EXPORT_ERROR

Description: Event DB data export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EVENT_ATTRIBUTE_BUILD_XML_ERROR

Description: App Server failed to build Event Attribute XML content

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EXPORT_ERROR

Description: App Server Generic Export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EXT_THREAT_INTEL_DOWNLOAD_ERROR

Description: External Threat Intelligence download error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EXT_THREAT_INTEL_PARSE_ERROR

Description: External Threat Intelligence parse error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EXT_THREAT_INTEL_UPDATE_ERROR

Description: External Threat Intelligence update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FILE_NOT_FOUND

Description: App Server cannot find specified file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FILE_READ_ERROR

Description: App Server cannot read from specified file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FILE_SYSTEM_ERROR

Description: App Server encountered file system error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FILE_WRITE_ERROR

Description: App Server cannot write to specified file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FLEX_INTERCEPTOR_NO_LOGIN_EXCEPTION_ERROR

Description: App Server encountered Flex API exception

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FORTIGUARD_IOC_INTEGRATION_ERROR

Description: FortiGuard IOC data download/parse error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_REGISTER_ERROR

Description: App Server Registration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_RUN_THREAD_ERROR

Description: App Server run thread error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_SECURITY_CHECK_LICENSE_WARN

Description: App Server Check license warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_SECURITY_GET_ENTITY_MANAGER_ERROR

Description: App Server cannot get EntityManager

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_SECURITY_GET_RS_EXPIRATION_ERROR

Description: App Server Get Report Server expiration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_SECURITY_INIT_SYSTEM_ERROR

Description: App Server Phoenix Caching system initialization failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_SERVICE_MISSED_WARN

Description: App Server can not find service

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_SHUTDOWN_SERVICE_STARTER_WARN

Description: App Server cannot shutdown service starter

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_GENERIC_ERROR

Description: Unknown Application Server error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_GENERIC_INFO

Description: Generic Application Server Informational log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_GENERIC_WARN

Description: Generic Application Server Warn

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_GET_MAX_CONFIG_ITEM_COUNT_ERROR

Description: App Server encountered error while getting max system configuration item count

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_GROUP_DATA_ERROR

Description: Group Data error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_IDENTITYLOCATION_EXPORT_ERROR

Description: Identity location export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_INCIDENT_NOTIFY_ERROR

Description: App Server failed to notify Incident via email or other methods

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_INCIDENT_UPDATE_ERROR

Description: App Server failed to update Incident in PostgreSQL database

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_INTEGRATION_ERROR

Description: External ticketing system integration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_INTEGRATION_UPDATE_POLICY_ERROR

Description: App Server encountered error while updating Ticketing system integration policy

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_INTEGRATION_UPDATE_POLICY_WARN

Description: App Server encountered warning while updating Ticketing system integration policy

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_INTEGRATION_WARN

Description: External ticketing system integration warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_IN_INTEGRATION_ERROR

Description: Inbound external ticketing system integration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_IOC_LICENSE_CHECK_FAILED_WARN

Description: App Server failed to check External Threat Intelligence License

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_IOC_TASK_CREATE_FAILED_ERROR

Description: App Server failed to create External Threat Intelligence Update task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_JOB_DISTRIBUTE_ERROR

Description: Application Server monitoring job distribution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_LICENSE_EXPIRY_ERROR

Description: License Expiration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_LICENSE_VALIDATION_ERROR

Description: License Validation error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_LOGIN_ERROR

Description: App Server Login exception

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_LOG_INTEGRITY_ERROR

Description: App Server failed to update log integrity hashes

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_MONITOR_AUDIT_PERF_ERROR

Description: App Server encountered exception while updating performance monitor job status

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_MONITOR_HEALTH_CONFIG_SET_ERROR

Description: App Server failed to update CMDB Device Monitor Health

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NETSEGMENT_EXPORT_ERROR

Description: Network Segment Export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NOTIFICATION_EMAIL_GET_RESOURCE_FAILED

Description: App Server failed to get resource for email notification

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NOTIFICATION_ERROR

Description: App Server notification error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NOTIFICATION_JMS_CONNECTION_ERROR

Description: App Server create JMS connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NOTIFICATION_UPDATE_ERROR

Description: App Server notification Update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NOTIFIER_ERROR

Description: App Server Notifier error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NO_WATCHLIST_SELECTED_WARN

Description: No watch list selected for entry warn

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_OPENPROXY_EXPORT_ERROR

Description: Open proxy data export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_OUT_INTEGRATION_ERROR

Description: Outbound external ticketing system integration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_PARSER_IMPORT_ERROR

Description: Custom parser import error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_PARSER_UPDATE_ERROR

Description: Custom parser update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_PARSING_CONSTRAINT_ERROR

Description: Rule/Report constraint parsing error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_PDF_BUILDER_ERROR

Description: App Server failed to build PDF during report export

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_PERFMON_TASK_ERROR

Description: App Server failed to create Performance Monitoring Task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_CHECK_POLICY_ACTION_WARN

Description: App Server failed to validate Incident notification policy action

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_EXPORT_ERROR

Description: App Server failed to export historical query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_RESULT_PARSER_ERROR

Description: App Server failed to parse historical query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_RESULT_RETRIEVE_ERROR

Description: App Server failed to retrieve historical query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_RUN_ERROR

Description: App Server failed to run historical query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_STOP_ERROR

Description: App Server failed to stop historical query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_STRING_ESCAPE_ERROR

Description: App Server can't find close escape string

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RBAC_ERROR

Description: App Server encountered error while setting RBAC policies

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RBAC_NO_PERMISSION_WARN

Description: App Server enforced user RBAC

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REALTIME_QUERY_ERROR

Description: App Server failed to start real time query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REMEDY_ERROR

Description: App Server failed to create tickets in Remedy

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_BUNDLE_PRINT_ERROR

Description: Print report bundle error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_COMPILE_ERROR

Description: Compile report to file error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_DEVICE_COMPONENT_SN_ERROR

Description: CMDB device serial number report error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_DEVICE_DETAIL_ERROR

Description: CMDB detail report error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_DEVICE_SN_ERROR

Description: CMDB server serial number report error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_DEVICE_SUMMARY_ERROR

Description: CMDB summary report error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_EXPORT_ERROR

Description: Report Export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_FAILED_BLOCK_SUMMARY_ERROR

Description: Get failed blocks error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_FIRE_TRIGGER_EVENT_ERROR

Description: App Server incident trigger events report error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_GET_PH_CONFIG_ERROR

Description: App Server get phoenix configuration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_IDENTITY_AND_LOCATION_ERROR

Description: Identity and location report error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_LOG_FILE_SUMMARY_ERROR

Description: App Server get log files error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_TEMPLATE_GENERATE_PDF_ERROR

Description: App Server Report template generate PDF error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_TEMPLATE_INIT_IMAGE_ERROR

Description: App Server Report template init image error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_TEMPLATE_INIT_PARM_ERROR

Description: App Server Report template init parameter error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_TEMPLATE_PDF_SUMMARY_ERROR

Description: App Server Report template create PDF summary error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_TICKET_SUMMARY_ERROR

Description: App Server get tickets error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_UPDATE_ERROR

Description: User defined report update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_USER_SUMMARY_ERROR

Description: App Server get users error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REST_ERROR

Description: App Server REST error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REST_H5_ERROR

Description: App Server HTML5 REST error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RISKSCORE_CALCULATE_ERROR

Description: Risk score calculation error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RULE_ACTIVE_ERROR

Description: App Server failed to activate rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RULE_CLONE_ERROR

Description: App Server failed to clone rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RULE_DEBUG_INVALID_EVENT_DB_ID_ERROR

Description: App Server found invalid event id during rule testing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RULE_DEBUG_WORKERS_SETTING_ERROR

Description: App Server detected Worker Settings error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RULE_TEST_ERROR

Description: App Server encountered error while testing rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RULE_UPDATE_ERROR

Description: App Server failed to update rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SCHEDULE_ERROR

Description: App Server job schedule error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SCHEDULE_UPDATE_ERROR

Description: App Server job schedule Update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SECURITY_ERROR

Description: Application Server System Security Data error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SERVLET_ERROR

Description: App Server Servlet error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SERVLET_NO_ACCESS_TO_URI_WARN

Description: App Server Servlet has no access to URI

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SOCKET_COMM_ERROR

Description: App Server Socket communication error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SVN_ERROR

Description: App Server SVN Repository error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SYNC_UPDATE_CONFIG_ERROR

Description: App Server encountered error on syncing update config for performance monitoring jobs

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SYSCONFIG_GET_ERROR

Description: App Server failed to get system configuration from PostGreSQL database

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SYSTEM_WINAGENT_REGISTER_WARN

Description: Windows Agent Manager not found or not registered

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SYS_APPLICATION_ERROR

Description: Application Server System error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SYS_DATA_UPDATE_ERROR

Description: Application Server Data Update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_TASK_CREATE_ERROR

Description: App Server create task error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_TASK_FLEX_RESULT_BUILD_XML_ERROR

Description: App Server failed to build Flex XML content

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_TASK_GET_ERROR

Description: App Server get task error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_TASK_UPDATE_ERROR

Description: App Server update task error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_TICKET_EXPORT_ERROR

Description: Incident ticket export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_UPDATER_FIND_EXIST_USER_BY_NOthing_ERROR

Description: App Server failed to locate existing user in CMDB

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_USERAGENT_EXPORT_ERROR

Description: User agent export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_VULNERABILITY_IGNORE_WARN

Description: App Server ignored host Vulnerability result

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WATCHLIST_ADD_TO_DISTIRBUTED_QUEUE

Description: App Server failed to add incident attribute to watch list

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WATCHLIST_EXPORT_ERROR

Description: Watch List export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WATCHLIST_IMPORT_ERROR

Description: Watch List import error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WATCHLIST_IMPORT_WARN

Description: Watch List import warnings

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WATCHLIST_UPDATE_ERROR

Description: Watch List update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WEBSERVICE_UPDATE_TASK_ERROR

Description: App Server encountered error while updating task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WORKER_PROVISION_FAILED

Description: App Server failed to provision Worker

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WS_COMM_ERROR

Description: App Server Web service communication error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_XML_PARSE_ERROR

Description: App Server failed to parse XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ACCOUNT_LOCKED

Description: System user account locked due to excessive login failures

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
reason	Reason	string	
targetUser	Target User	string	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.

EventType: PH_AUDIT_AGENT_DISABLED

Description: FortiSIEM Windows/Linux Agent disabled

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_INSTALLED

Description: FortiSIEM Windows/Linux Agent installed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_NOTRESPONDING

Description: FortiSIEM Windows/Linux Agent not responding

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_RUNNING

Description: FortiSIEM Windows/Linux Agent is running and sending events

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_STARTED

Description: FortiSIEM Windows/Linux Agent started

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_STOPPED

Description: FortiSIEM Windows/Linux Agent stopped

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_UNINSTALLED

Description: FortiSIEM Windows/Linux Agent uninstalled

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_CASE_ASSIGNED

Description: FortiSIEM Case Assigned to a User

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
targetUser	Target User	string	

EventType: PH_AUDIT_CASE_CLOSED

Description: FortiSIEM Case Closed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
comment	Comment	string	

EventType: PH_AUDIT_CASE_CREATED

Description: FortiSIEM Case Created

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	

Id	Display name	Type	Description
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

EventType: PH_AUDIT_CASE_EVIDENCE_ADDED

Description: FortiSIEM Case Evidence Added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
type	Type	string	
fileName	File Name	string	

EventType: PH_AUDIT_CASE_EVIDENCE_DELETED

Description: FortiSIEM Case Evidence Deleted

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

Id	Display name	Type	Description
type	Type	string	
fileName	File Name	string	

EventType: PH_AUDIT_CASE_INCIDENT_ADDED

Description: FortiSIEM Incident added to a Case

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

EventType: PH_AUDIT_CASE_MERGED

Description: FortiSIEM Case Merged

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case

EventType: PH_AUDIT_CASE_NOTE_ADDED

Description: FortiSIEM Case Note Added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
comment	Comment	string	

EventType: PH_AUDIT_CASE_NOTE_DELETED

Description: FortiSIEM Case Note Deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

EventType: PH_AUDIT_CASE_NOTE_MODIFIED

Description: FortiSIEM Case Note Modified

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
comment	Comment	string	

EventType: PH_AUDIT_CASE_PRIORITY_CHANGED

Description: FortiSIEM Case Priority Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
oldSeverity	Old Severity	string	
newSeverity	New Severity	string	

EventType: PH_AUDIT_CASE_REASSIGNED

Description: FortiSIEM Case Reassigned

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

Id	Display name	Type	Description
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
targetUser	Target User	string	

EventType: PH_AUDIT_CASE_STAGE_CHANGED

Description: FortiSIEM Case Stage Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

EventType: PH_AUDIT_CASE_STAT

Description: FortiSIEM Case Closed Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
user	User	string	

Id	Display name	Type	Description
newDuration	New Duration	uint64	Duration of a case in the new status
assignedDuration	Assigned Duration	uint64	Duration of a case in the assigned status
inProgressDuration	In-Progress Duration	uint64	Duration of a case in the in-progress status
pendCustFeedbackDuration	Pending Customer Feedback Duration	uint64	Duration of a case in the pending feedback status
recvCustFeedbackDuration	Received Customer Feedback Duration	uint64	Duration of a case in the received feedback status
timeToClose	Time to Close	uint64	Total duration that a case was open

EventType: PH_AUDIT_CASE_STATUS_CHANGED

Description: FortiSIEM Case Status Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

EventType: PH_AUDIT_CASE_SUMMARY_CHANGED

Description: FortiSIEM Case Summary Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
oldTitle	Old Title	string	

EventType: PH_AUDIT_CASE_UPDATED

Description: FortiSIEM Case Updated

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_CI_QUOTE_EXCEEDED

Description: System CI Quote Exceeded

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_CMDB_DISK_PRUNE_FAILED

Description: CMDB Disk Prune Failed

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
freeDiskMB	Free Disk MB	uint32	

EventType: PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS

Description: CMDB Disk Prune Success

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
freeDiskMB	Free Disk MB	uint32	

EventType: PH_AUDIT_DASHBOARD_SHARED

Description: FortiSIEM dashboard folder shared

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	
targetUserGrp	Target User Group	string	

EventType: PH_AUDIT_DATA_PURGE

Description: System data has been purged

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_DB_LEADER_CHANGE

Description: DB Leader Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phEventCategory	System Event Category	uint16	This is the category of log event. (Values: 0 - External, 1 - Incidents, 2 - Audit, 3 - System, 4 - Traffic Flow, 5- Health, 6 - Performance). When you query events in FortiSIEM, only Category 0 events show up in search results by default. To include other events, you need to explicitly include Categories in the Search condition; for example to search for Incidents, use System Event Category = 1.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_AUDIT_DEFAULT_PWD_MATCH

Description: Default password match

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
reptVendor	Reporting Vendor	string	This field captures the vendor of the reported event
reptModel	Reporting Model	string	This field captures the model of the reported event
appTransportProto	Application Protocol	string	
user	User	string	

EventType: PH_AUDIT_DEVICE_ADDED

Description: System CMDB device added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_AUDIT_DEVICE_DELETED

Description: System CMDB device deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_AUDIT_DEVICE_DISCOVERY_ITEM_CHANGED

Description: System CMDB device changed by discovery

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
objType	Object Type	string	
addedItem	Added Item	string	

EventType: PH_AUDIT_DEVICE_MAINTENANCE_ENDED

Description: System device maintenance ended

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
maintScheduleName	Maintenance Schedule Name	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
endTime	End Time	Date	This is the end time of a given item or task, stored in epoch milliseconds.

EventType: PH_AUDIT_DEVICE_MAINTENANCE_STARTED

Description: System device maintenance started

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
maintScheduleName	Maintenance Schedule Name	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
startTime	Start Time	Date	This is the start time of a given item or task, and is stored in epoch milliseconds

EventType: PH_AUDIT_DEVICE_MERGED_BY_IP_WITH_DIFF_NAME

Description: Two devices with different hostname merged because of overlapping IP addresses

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
targetHostName	Target Host Name	string	
overlapIp	Overlapping IP	string	This field represents the list of IP addresses of a just discovered device that overlaps with an existing device in CMDB.

EventType: PH_AUDIT_DEVICE_STATUS_CHANGED

Description: CMDB Device audit status changed

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
origStatus	Original Status	string	
newStatus	New Status	string	
eventSource	Event Source	string	

EventType: PH_AUDIT_DEVICE_UNMANAGED

Description: license exceeded - newly discovered device set to Unmanaged

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
status	Status	string	
eventSource	Event Source	string	
details	Details	string	

EventType: PH_AUDIT_DEV_MON_JOB_NOT_STARTED

Description: Performance monitoring Job is not picked up for execution for a long time

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_DEV_MON_JOB_STATUS_CHANGE

Description: Performance monitoring job status changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_DISCOVERY

Description: Audit discovery

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
startTime	Start Time	Date	This is the start time of a given item or task, and is stored in epoch milliseconds
type	Type	string	
task	Task	string	
osObjName	Object Name	string	

EventType: PH_AUDIT_EXPORT_REPORT_END

Description: User exported FortiSIEM Report result via GUI or Scheduled Report

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_GENAI_USER_QUERY

Description: FortiSIEM sent Generative AI Query to ChatGPT

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_GENERIC

Description: System generic audit message

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_GROUP_CREATED

Description: FortiSIEM GUI Group Created

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
osObjName	Object Name	string	
osObjType	OS Object Type	string	

EventType: PH_AUDIT_GROUP_DELETED

Description: FortiSIEM GUI Group Deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
osObjName	Object Name	string	
osObjType	OS Object Type	string	

EventType: PH_AUDIT_INACTIVE_USER_LOGIN

Description: A system inactive user tried to login

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_INCIDENT_SYS_CLEAR

Description: FortiSIEM Incident System Auto-Cleared

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	
osObjHandleID	Object Handle	string	

EventType: PH_AUDIT_INCIDENT_USER_CLEAR

Description: FortiSIEM Incident User Cleared

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	
osObjHandleID	Object Handle	string	

EventType: PH_AUDIT_INTEGRATION_POLICY_EXECUTED

Description: FortiSIEM Integration Policy Executed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	

EventType: PH_AUDIT_MALWARE_DATA_DELETED

Description: Malware data deleted by scheduled update

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
updateTime	Update Time	Date	
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.
folder	Folder	string	

EventType: PH_AUDIT_MALWARE_DATA_UPDATED

Description: Malware data updated by scheduled update

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
updateTime	Update Time	Date	
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.
folder	Folder	string	

EventType: PH_AUDIT_ML_GENERIC_ERROR

Description: Machine Learning generic error log

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ML_GENERIC_INFO

Description: Machine Learning generic info log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ML_INFERENCE_COMPLETED

Description: Machine Learning audit inference completed log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ML_INFERENCE_RESULT

Description: Machine Learning audit inference result log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ML_INFERENCE_STARTED

Description: Machine Learning audit inference started log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ML_TRAINING_COMPLETED

Description: Machine Learning audit training completed log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ML_TRAINING_STARTED

Description: Machine Learning audit training started log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_NOTIF_POLICY_EXECUTED

Description: FortiSIEM Incident Notification Policy Executed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	

Id	Display name	Type	Description
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
osObjHandleID	Object Handle	string	

EventType: PH_AUDIT_OBJECT_CREATED

Description: System data object created

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjType	OS Object Type	string	
osObjName	Object Name	string	

EventType: PH_AUDIT_OBJECT_DELETED

Description: System data object deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	

EventType: PH_AUDIT_OBJECT_UPDATED

Description: System data object updated

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjType	OS Object Type	string	
objType	Object Type	string	
osObjName	Object Name	string	
osObjAction	Object Action	string	
targetCustomer	Target Organization Name	string	
oldSettingsValue	Old Settings Value	string	
newSettingsValue	New Settings Value	string	

EventType: PH_AUDIT_ONDEMAND_REMEDIATION_EXECUTED

Description: FortiSIEM Ondemand Remediation Executed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	

EventType: PH_AUDIT_PASSWORD_CHANGED

Description: System user password changed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	

Id	Display name	Type	Description
user	User	string	
domain	Domain	string	

EventType: PH_AUDIT_QUERY_COMPLETED

Description: Audit query completed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
osObjName	Object Name	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
durationMSec	Duration	uint32	Duration of a connection (in msec)
queryFilter	Query Filter	string	
queryDisplay	Query Display	string	
queryId	Query Id	string	
usageType	Usage Type	string	

EventType: PH_AUDIT_QUERY_SCHEDULED

Description: System scheduled a query

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.

EventType: PH_AUDIT_QUERY_START

Description: System started a query

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
osObjName	Object Name	string	

EventType: PH_AUDIT_QUERY_STOP

Description: System stopped a query

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
osObjName	Object Name	string	
durationMSec	Duration	uint32	Duration of a connection (in msec)
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_AUDIT_REPL_LEADER_CHANGE

Description: Replication Leader Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phEventCategory	System Event Category	uint16	This is the category of log event. (Values: 0 - External, 1 - Incidents, 2 - Audit, 3 - System, 4 - Traffic Flow, 5- Health, 6 - Performance). When you query events in FortiSIEM, only Category 0 events show up in search results by default. To include other events, you need to explicitly include Categories in the Search condition; for example to search for Incidents, use System Event Category = 1.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_AUDIT_REPORT_SCHEDULED

Description: FortiSIEM Report Scheduled

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_REPORT_SCHEDULE_APPROVE

Description: FortiSIEM Report schedule approval

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
objId	DB Object Id	string	
status	Status	string	
targetUser	Target User	string	

Id	Display name	Type	Description
reportId	Report ID	uint32	
reportName	Report Name	string	FortiSIEM report name.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AUDIT_REPORT_SCHEDULE_REQUEST

Description: FortiSIEM Report schedule request

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
objId	DB Object Id	string	
status	Status	string	
targetUser	Target User	string	
reportId	Report ID	uint32	
reportName	Report Name	string	FortiSIEM report name.

EventType: PH_AUDIT_REPORT_SERVER_LICENSE_EXPIRED

Description: FortiSIEM Report Server license expired

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_REPORT_SERVER_LICENSE_REMOVED

Description: FortiSIEM Report Server Removed After License Expiry

Severity: 8 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_REPORT_SERVER_LICENSE_TO_EXPIRE

Description: FortiSIEM Report Server license about to expire

Severity: 8 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_RISK_DECREASE_LOW

Description: Device Risk Score decreased to LOW level

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_RISK_DECREASE_MED

Description: Device Risk Score decreased to MEDIUM level

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_RISK_INCREASE_HIGH

Description: Device Risk Score increased to HIGH level

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_RISK_INCREASE_MED

Description: Device Risk Score increased to MEDIUM level

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_RULE_ACTIVATED

Description: FortiSIEM Rule activated

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	

EventType: PH_AUDIT_RULE_ACTIVATION_APPROVE

Description: FortiSIEM Rule activation approval

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
objId	DB Object Id	string	
status	Status	string	
targetUser	Target User	string	
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AUDIT_RULE_ACTIVATION_REQUEST

Description: FortiSIEM Rule activation request

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
objId	DB Object Id	string	

Id	Display name	Type	Description
status	Status	string	
targetUser	Target User	string	
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_AUDIT_RULE_DEACTIVATED

Description: FortiSIEM Rule de-activated

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	

EventType: PH_AUDIT_RULE_DEACTIVATION_APPROVE

Description: FortiSIEM Rule de-activation approval

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
objId	DB Object Id	string	
status	Status	string	
targetUser	Target User	string	
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AUDIT_RULE_DEACTIVATION_REQUEST

Description: FortiSIEM Rule de-activation request

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
objId	DB Object Id	string	
status	Status	string	
targetUser	Target User	string	
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_AUDIT_SVC_LOGIN_FAILURE

Description: System service user failed to login

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_SVC_LOGIN_SUCCESS

Description: System service user login success

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_SVC_LOGOFF

Description: System Service user logoff

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_SVC_SESSION_TIMEOUT

Description: System service user session timeout

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_TUNNEL_CLOSE

Description: Collector to Super Reverse SSH Tunnel closed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
appTransportProto	Application Protocol	string	
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
collectorIp	Collector IP	IP	This field captures the IP address of a FortiSIEM Collector
tunnelUpTime	Tunnel Uptime	uint64	
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.

EventType: PH_AUDIT_TUNNEL_OPEN

Description: Collector to Super Reverse SSH Tunnel opened

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
appTransportProto	Application Protocol	string	
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
collectorIp	Collector IP	IP	This field captures the IP address of a FortiSIEM Collector
tunnelUpTime	Tunnel Uptime	uint64	
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.

EventType: PH_AUDIT_USER_ADDED

Description: System user added

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
user	User	string	
domain	Domain	string	

EventType: PH_AUDIT_USER_CHANGE_ORG_SCOPE

Description: FortiSIEM user changed organization scope

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
userFullName	User Full Name	string	
targetCustomer	Target Organization Name	string	

EventType: PH_AUDIT_USER_DEFAULT_ROLE_CHANGED

Description: FortiSIEM Admin User Default Role Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
targetCustomer	Target Organization Name	string	
role	Role	string	

EventType: PH_AUDIT_USER_DELETED

Description: System user deleted

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
user	User	string	
targetUser	Target User	string	
details	Details	string	

EventType: PH_AUDIT_USER_LOGIN_FAILURE

Description: System user failed to login

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
domain	Domain	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_AUDIT_USER_LOGIN_SUCCESS

Description: System user login success

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
userFullName	User Full Name	string	

EventType: PH_AUDIT_USER_LOGOFF

Description: System user logoff

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
userFullName	User Full Name	string	

EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_CHANGED

Description: FortiSIEM Admin User Organization Role changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
targetCustomer	Target Organization Name	string	
role	Role	string	

EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_ENABLED

Description: FortiSIEM Admin User Organization Role enabled

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_REMOVED

Description: FortiSIEM Admin User Organization Role disabled

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
targetCustomer	Target Organization Name	string	
role	Role	string	

EventType: PH_AUDIT_USER_SESSION_TIMEOUT

Description: System user session timeout

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
userFullName	User Full Name	string	

EventType: PH_AUDIT_WS_COMM

Description: System web service communication

Severity: 1 (Low)

Event Category: 3 (System Logs)

Data Manager Logs

This section provides logs related to (a)inserting events in database, (b)moving events within various database tiers e.g. Hot, Warm, Cold, Archive, (c)generating log integrity, and (d)purging events. Supported event databases include EventDB, ClickHouse and Elasticsearch.

- PH_CLICKHOUSE_CHECKIN_QUERY_THREADS_FAILED
- PH_CLICKHOUSE_CHECKOUT_QUERY_THREADS_FAILED
- PH_CLICKHOUSE_DISK_UTILS_PER_STORAGE_TIER
- PH_CLICKHOUSE_DROP_PARTITION_FAILED
- PH_CLICKHOUSE_DROP_PARTITION_STARTED
- PH_CLICKHOUSE_DROP_PARTITION_SUCCEEDED
- PH_CLICKHOUSE_GET_ONLINE_NODE_FAILED
- PH_CLICKHOUSE_GET_PARTITIONS_FAILED
- PH_CLICKHOUSE_GET_SHARDS_FAILED
- PH_CLICKHOUSE_GET_STORAGE_STATS_FAILED
- PH_CLICKHOUSE_GET_STORAGE_TIER_FAILED
- PH_CLICKHOUSE_INSERTION_DROP_EVENTS
- PH_CLICKHOUSE_INSERTION_EPS
- PH_CLICKHOUSE_JSON_ENCODER_EPS
- PH_CLICKHOUSE_JSON_ENCODER_EPS_PER_THREAD
- PH_CLICKHOUSE_LOG_INTEGRITY_ACTIVE_CONSOLIDATION
- PH_CLICKHOUSE_LOG_INTEGRITY_CALCULATE_REQUEST_PARSE_FAILED
- PH_CLICKHOUSE_LOG_INTEGRITY_CALCULATE_REQUEST_STARTED
- PH_CLICKHOUSE_LOG_INTEGRITY_CANDIDATE_PARTITIONS
- PH_CLICKHOUSE_LOG_INTEGRITY_CONSOLIDATION_DATE
- PH_CLICKHOUSE_LOG_INTEGRITY_CONSOLIDATION_STATUS_CHANGE
- PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_DONE
- PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_STARTED
- PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_STOPPED
- PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_TIMER
- PH_CLICKHOUSE_LOG_INTEGRITY_DB_QUERY_FAILED
- PH_CLICKHOUSE_LOG_INTEGRITY_EMPTY_PARTITION_CHECKSUM
- PH_CLICKHOUSE_LOG_INTEGRITY_EXEC_FAILED
- PH_CLICKHOUSE_LOG_INTEGRITY_MIN_MAX_QUERY_FAILED
- PH_CLICKHOUSE_LOG_INTEGRITY_OPTIMIZE_COMMAND_FAILED
- PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_CONSOLIDATION_DONE
- PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_CONSOLIDATION_STARTED
- PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_UPDATED_AFTER_CHECKSUM
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_MISMATCH
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_MISMATCH_REPLICAS
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_PARTITION_INFO_EMPTY

- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_REQUEST_PARSE_FAILED
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_EMPTY
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_ERROR
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_PARSE_FAILED
- PH_CLICKHOUSE_MOVE_PARTITION_FAILED
- PH_CLICKHOUSE_MOVE_PARTITION_STARTED
- PH_CLICKHOUSE_MOVE_PARTITION_SUCCEEDED
- PH_CLICKHOUSE_NOT_REACHABLE
- PH_CLICKHOUSE_QUERY_REDIS_CONN_FAILURE
- PH_CLICKHOUSE_QUERY_REDIS_GET_FAILURE
- PH_CLICKHOUSE_QUERY_UNCOMPRESS_FAILURE
- PH_CLICKHOUSE_QUERY_ZLIB_INIT_FAILURE
- PH_CLICKHOUSE_RESOURCE_TRACKER_QUERY_CHECKIN
- PH_CLICKHOUSE_RESOURCE_TRACKER_QUERY_CHECKOUT
- PH_CLICKHOUSE_RESOURCE_TRACKER_THREADS_CHECKIN
- PH_CLICKHOUSE_RESOURCE_TRACKER_THREADS_CHECKOUT
- PH_CLICKHOUSE_ROUND_ROBIN_INSERTION
- PH_CLICKHOUSE_ROUND_ROBIN_QUERY
- PH_CLICKHOUSE_STORAGE_FREE_SPACE_CRITICAL
- PH_CLICKHOUSE_STORAGE_FREE_SPACE_LOW
- PH_CLICKHOUSE_STORAGE_UTILS_PER_ORG_PER_DAY
- PH_CLICKHOUSE_WRITE_FAILED
- PH_CLUSTER_COLLECT_ALL_IP_FAILED
- PH_CLUSTER_COLLECT_CONFIG_DATA_FAILED
- PH_CLUSTER_CONFIG_SSH_KEY_FAILED
- PH_CLUSTER_GET_FW_IP_FAILED
- PH_CLUSTER_GET_TASK_FAILED
- PH_CLUSTER_NOT_SUPPORT_TASK
- PH_CLUSTER_NOT_VALID_FELLOWER
- PH_CLUSTER_RELOAD_CONFIG_FAILED
- PH_CLUSTER_RM_DB_FAILED
- PH_CLUSTER_RUN_COMMAND_FAILED
- PH_CLUSTER_SCIRPT_FAILED
- PH_CLUSTER_SEND_TASK_FAILED
- PH_CLUSTER_SSH_KEY_IS_WRONG
- PH_CLUSTER_TASK_DATA_EMPTY
- PH_CLUSTER_TASK_INFO_IS_WRONG
- PH_CLUSTER_TASK_NOT_CONTAIN_LIC
- PH_CLUSTER_UPDATE_CONFIG_ERROR
- PH_DATAINTEGRITY_PASSPHRASE_LOAD_ERROR
- PH_DATAINTEGRITY_SIGNER_ERROR
- PH_DATAINTEGRITY_UTILS_ERROR
- PH_DATAINTEGRITY_VERIFIER_ERROR

- PH_DATAMANAGER_CLICKHOUSE_HTTP_UPLOAD_ERROR
- PH_DATAMANAGER_CLUSTER_ENCODE_ERROR
- PH_DATAMANAGER_CLUSTER_INIT_ERROR
- PH_DATAMANAGER_CLUSTER_WAIT_ERROR
- PH_DATAMANAGER_CLUSTER_WRITER_ERROR
- PH_DATAMANAGER_DASHBOARD_RESPONSE_ERROR
- PH_DATAMANAGER_ELASTICWRITER_ERROR
- PH_DATAMANAGER_EVTATTR_ERROR
- PH_DATAMANAGER_EVTCACHE_DUPLICATE_ERROR
- PH_DATAMANAGER_EVTCACHE_GET_ERROR
- PH_DATAMANAGER_EVTCACHE_PARSE_ERROR
- PH_DATAMANAGER_EVTDBNOTIFIER_ERROR
- PH_DATAMANAGER_EVTIDX_CORRUPT_ERROR
- PH_DATAMANAGER_EVTIDX_MERGE_ERROR
- PH_DATAMANAGER_EVTIDX_QUERY_ERROR
- PH_DATAMANAGER_EVTIDX_READ_BLOCK_ERROR
- PH_DATAMANAGER_EVTIDX_READ_KEY_ERROR
- PH_DATAMANAGER_EVTIDX_READ_POST_ERROR
- PH_DATAMANAGER_EVTIDX_WRITE_ERROR
- PH_DATAMANAGER_EVTIDX_WRITE_KEY_ERROR
- PH_DATAMANAGER_EVTIDX_WRITE_POST_ERROR
- PH_DATAMANAGER_EVTLOADER_ERROR
- PH_DATAMANAGER_EVTWRITER_ERROR
- PH_DATAMANAGER_EXPORT_ERROR
- PH_DATAMANAGER_FILE_READ_FAILURE
- PH_DATAMANAGER_FILE_RENAME_FAILURE
- PH_DATAMANAGER_FILE_SIGN_ERROR
- PH_DATAMANAGER_FILE_WRITE_FAILURE
- PH_DATAMANAGER_GET_SIGN_ERROR
- PH_DATAMANAGER_GLOBAL_CACHE_MISSING
- PH_DATAMANAGER_HDFSWRITER_ERROR
- PH_DATAMANAGER_HTTP_UPLOAD_ERROR
- PH_DATAMANAGER_INIT_ERROR
- PH_DATAMANAGER_INTEGRITY_CHECK_ERROR
- PH_DATAMANAGER_INTEGRITY_RESPONSE_ERROR
- PH_DATAMANAGER_INVALID_LOG_FILE
- PH_DATAMANAGER_IP_TYPE_INVALID
- PH_DATAMANAGER_KAFKAWRITER_CONFIG_ERROR
- PH_DATAMANAGER_KAFKAWRITER_ERROR
- PH_DATAMANAGER_LOG_BUFFER_PAUSED_LOW_SPACE
- PH_DATAMANAGER_LOG_BUFFER_PAUSED_STATFS_FAILURE
- PH_DATAMANAGER_LOG_BUFFER_RESUMED
- PH_DATAMANAGER_PUT_SIGN_ERROR

- PH_DATAMANAGER_QUERY_EXPR_ERROR
- PH_DATAMANAGER_QUERY_RESPONSE_ERROR
- PH_DATAMANAGER_REDIS_KEY_NOT_EXIST
- PH_DATAMANAGER_SUMMARYWRITER_ERROR
- PH_DATAMGR_BAD_EVTBLKIDX_FILE
- PH_DATAMGR_BAD_SEGMENT
- PH_DATAMGR_INDEX_MERGE_FAILED
- PH_DATAMGR_INDEX_MERGE_FAILED_INDEX
- PH_DATAMGR_INDEX_MERGE_FAILED_INDEX_GROUP
- PH_DATAMGR_SEGMENT_MERGE_ERROR
- PH_DATAMGR_SEGMENT_MERGE_FAILED
- PH_DATAMGR_UNABLE_FLUSH_INDEX
- PH_DATAMGR_UNABLE_OPEN_EVTBLK_FILE
- PH_DATAPURGER_ARCHIVE_TASK_ERROR
- PH_DATAPURGER_CMD_FAILURE
- PH_DATAPURGER_DR_ES_RESTORE_FAILED
- PH_DATAPURGER_DR_ES_ROLE_UNKNOWN
- PH_DATAPURGER_DR_ES_SNAPSHOTS_GET_FAILED
- PH_DATAPURGER_DR_ES_SNAPSHOT_DELETION_FAILED
- PH_DATAPURGER_DR_ES_SNAPSHOT_FAILED
- PH_DATAPURGER_DUCHECKER_ERROR
- PH_DATAPURGER_ENFORCE_ERROR
- PH_DATAPURGER_EVAL_ERROR
- PH_DATAPURGER_HTTP_UPLOAD_ERROR
- PH_DATAPURGER_INIT_ERROR
- PH_DATAPURGER_OPEN_FILE_ERROR
- PH_DATAPURGER_PARSE_XML_ERROR
- PH_DATAPURGER_POLICY_ERROR
- PH_DATAPURGER_RESPONSE_ERROR
- PH_DATAPURGER_STORAGE_POLICY_CLICKHOUSE_NODES_EMPTY
- PH_DATA_CLUSTER_ALL_COORDINATOR_DOWN
- PH_DATA_CLUSTER_BUSY
- PH_DATA_CLUSTER_CLICKHOUSE_CONFIG_NO_PORT
- PH_DATA_CLUSTER_COORDINATOR_DOWN
- PH_DATA_CLUSTER_COORDINATOR_UP
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_HTTPPORT
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_IP
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_JAVAPORT
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NAME
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NUMREPLICAS
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NUMSHARD
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NULL
- PH_DATA_CLUSTER_ELASTIC_CONFIG_WRONG_FORMAT

- PH_DATA_CLUSTER_ELASTIC_EVENTID_NOT_FOUND
- PH_DATA_CLUSTER_ELASTIC_HTTP_CLIENT_FAIL
- PH_DATA_CLUSTER_ELASTIC_HTTP_CMD_FAIL
- PH_DATA_CLUSTER_ELASTIC_INDEX_FAIL
- PH_DATA_CLUSTER_ELASTIC_INDEX_RESEND_FAIL
- PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FAIL
- PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FIRST_FAIL
- PH_DATA_CLUSTER_ELASTIC_INDEX_UPLOAD_FAIL
- PH_DATA_CLUSTER_ELASTIC_WRONG_JSON_FORMAT
- PH_DATA_CLUSTER_GET_HOSTNAME_FAIL
- PH_DATA_CLUSTER_HDFS_CONFIG_NO_PORT
- PH_DATA_CLUSTER_HDFS_CONFIG_NO_SERVER
- PH_DATA_CLUSTER_HDFS_CONFIG_NO_YARN_PORT
- PH_DATA_CLUSTER_HDFS_CONFIG_NO_YARN_SERVER
- PH_DATA_CLUSTER_HDFS_CONFIG_NULL
- PH_DATA_CLUSTER_HDFS_HTTP_CMD_FAIL
- PH_DATA_CLUSTER_HDFS_LISTSTATUS_FAIL
- PH_DATA_CLUSTER_HDFS_SEND_FAIL
- PH_DATA_CLUSTER_HDFS_UPLOAD_FAIL
- PH_DATA_CLUSTER_JSON_GET_ATTRIBUTE_NAME_FAIL
- PH_ES_ARCHIVE_STORAGE_CHECK_ERROR
- PH_ES_ARCHIVE_STORAGE_LOW
- PH_ES_ARCHIVE_STORAGE_PURGING_FAILED
- PH_ES_ARCHIVE_STORAGE_PURGING_FINISHED
- PH_ES_ARCHIVE_STORAGE_PURGING_STARTED
- PH_ES_ARCHIVE_STORAGE_PURGING_SUCCESS
- PH_ES_ARCHIVE_STORAGE_USAGE
- PH_ES_CCR_DELAY
- PH_ES_COLD_STORAGE_ARCHIVING_FAILED
- PH_ES_COLD_STORAGE_ARCHIVING_FINISHED
- PH_ES_COLD_STORAGE_ARCHIVING_STARTED
- PH_ES_COLD_STORAGE_ARCHIVING_SUCCESS
- PH_ES_COLD_STORAGE_CHECK_ERROR
- PH_ES_COLD_STORAGE_LOW
- PH_ES_COLD_STORAGE_PURGING_FAILED
- PH_ES_COLD_STORAGE_PURGING_FINISHED
- PH_ES_COLD_STORAGE_PURGING_STARTED
- PH_ES_COLD_STORAGE_PURGING_SUCCESS
- PH_ES_COLD_STORAGE_USAGE
- PH_ES_HOTCOLD_STORAGE_MOVING_FAILED
- PH_ES_HOTCOLD_STORAGE_MOVING_FINISHED
- PH_ES_HOTCOLD_STORAGE_MOVING_STARTED
- PH_ES_HOTCOLD_STORAGE_MOVING_SUCCESS

- PH_ES_HOT_STORAGE_ARCHIVING_FAILED
- PH_ES_HOT_STORAGE_ARCHIVING_FINISHED
- PH_ES_HOT_STORAGE_ARCHIVING_STARTED
- PH_ES_HOT_STORAGE_ARCHIVING_SUCCESS
- PH_ES_HOT_STORAGE_CHECK_ERROR
- PH_ES_HOT_STORAGE_LOW
- PH_ES_HOT_STORAGE_MOVING_FAILED
- PH_ES_HOT_STORAGE_MOVING_FINISHED
- PH_ES_HOT_STORAGE_MOVING_STARTED
- PH_ES_HOT_STORAGE_MOVING_SUCCESS
- PH_ES_HOT_STORAGE_PURGING_FAILED
- PH_ES_HOT_STORAGE_PURGING_FINISHED
- PH_ES_HOT_STORAGE_PURGING_STARTED
- PH_ES_HOT_STORAGE_PURGING_SUCCESS
- PH_ES_HOT_STORAGE_USAGE
- PH_ES_INDEX_SEGMENT_MERGE_FAILED
- PH_ES_REST_FAILED
- PH_ES_SM_ADD_INDEX_FAILED
- PH_ES_SM_HOURLCHECK_FAILED
- PH_ES_SM_INIT_FAILED
- PH_ES_SM_INIT_INDEX_FAILED
- PH_ES_SNAPSHOT_FAILED
- PH_ES_TO_NFS_ARCHIVE_FAILED_ADD_INDEX
- PH_ES_WARM_STORAGE_ARCHIVING_FAILED
- PH_ES_WARM_STORAGE_ARCHIVING_FINISHED
- PH_ES_WARM_STORAGE_ARCHIVING_STARTED
- PH_ES_WARM_STORAGE_ARCHIVING_SUCCESS
- PH_ES_WARM_STORAGE_CHECK_ERROR
- PH_ES_WARM_STORAGE_LOW
- PH_ES_WARM_STORAGE_MOVING_FAILED
- PH_ES_WARM_STORAGE_MOVING_FINISHED
- PH_ES_WARM_STORAGE_MOVING_STARTED
- PH_ES_WARM_STORAGE_MOVING_SUCCESS
- PH_ES_WARM_STORAGE_PURGING_FAILED
- PH_ES_WARM_STORAGE_PURGING_FINISHED
- PH_ES_WARM_STORAGE_PURGING_STARTED
- PH_ES_WARM_STORAGE_PURGING_SUCCESS
- PH_ES_WARM_STORAGE_USAGE
- PH_HDFS_ARCHIVE_STORAGE_LOW
- PH_HDFS_ARCHIVE_STORAGE_USAGE
- PH_HDFS_PURGING_FAILED
- PH_HDFS_PURGING_FINISHED
- PH_HDFS_PURGING_STARTED

- PH_HDFS_PURGING_SUCCESS
- PH_SYSTEM_ARCHIVE_LOW
- PH_SYSTEM_ARCHIVE_PURGED_LOW_SPACE
- PH_SYSTEM_ARCHIVE_PURGED_POLICY
- PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_FAILED
- PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_FINISHED
- PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_STARTED
- PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_SUCCESS
- PH_SYSTEM_ARCHIVE_PURGING_POLICY_FAILED
- PH_SYSTEM_ARCHIVE_PURGING_POLICY_FINISHED
- PH_SYSTEM_ARCHIVE_PURGING_POLICY_STARTED
- PH_SYSTEM_ARCHIVE_PURGING_POLICY_SUCCESS
- PH_SYSTEM_ARCHIVE_RETENTION_POLICY_VIOLATED
- PH_SYSTEM_ARCHIVE_USAGE
- PH_SYSTEM_DATAMGR_ARCHIVE_SKIP
- PH_SYSTEM_DISK_ARCHIVING_FAILED
- PH_SYSTEM_DISK_ARCHIVING_FINISHED
- PH_SYSTEM_DISK_ARCHIVING_STARTED
- PH_SYSTEM_DISK_ARCHIVING_SUCCESS
- PH_SYSTEM_DISK_PURGED
- PH_SYSTEM_DISK_PURGING_FAILED
- PH_SYSTEM_DISK_PURGING_FINISHED
- PH_SYSTEM_DISK_PURGING_STARTED
- PH_SYSTEM_DISK_PURGING_SUCCESS
- PH_SYSTEM_DISK_USAGE
- PH_SYSTEM_DISK_USAGE_WARNING
- PH_SYSTEM_ONLINE_RETENTION_POLICY_VIOLATED
- PH_SYSTEM_RETENTION_POLICY_EXEC_TIME
- PH_SYSTEM_RETENTION_POLICY_FAILED
- PH_SYSTEM_RETENTION_POLICY_FINISHED
- PH_SYSTEM_RETENTION_POLICY_STARTED
- PH_SYSTEM_RETENTION_POLICY_STATS
- PH_SYSTEM_RETENTION_POLICY_SUCCESS

EventType: PH_CLICKHOUSE_CHECKIN_QUERY_THREADS_FAILED

Description: Failed to checkin query threads

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_CHECKOUT_QUERY_THREADS_FAILED

Description: Failed to checkout query threads

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_DISK_UTILS_PER_STORAGE_TIER

Description: ClickHouse disk utils per storage tier

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
diskType	Disk Type	string	
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_CLICKHOUSE_DROP_PARTITION_FAILED

Description: Failed to drop ClickHouse partitions

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
dbPartition	DB Partition	string	
errReason	Reason for Error	string	This is the reason for an error if given.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_DROP_PARTITION_STARTED

Description: Drop ClickHouse partition started

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
dbPartition	DB Partition	string	
command	Command	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_DROP_PARTITION_SUCCEEDED

Description: Drop ClickHouse partition successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
dbPartition	DB Partition	string	
command	Command	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_GET_ONLINE_NODE_FAILED

Description: ClickHouse getting online node failed

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_GET_PARTITIONS_FAILED

Description: Failed to get ClickHouse partitions

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_GET_SHARDS_FAILED

Description: Failed to get ClickHouse shards

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_GET_STORAGE_STATS_FAILED

Description: Failed to get ClickHouse storage stats

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_GET_STORAGE_TIER_FAILED

Description: Failed to get ClickHouse storage tier

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_INSERTION_DROP_EVENTS

Description: FortiSIEM dropped events while failing to insert them to ClickHouse after retries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_INSERTION_EPS

Description: ClickHouse Insertion EPS

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_CLICKHOUSE_JSON_ENCODER_EPS

Description: ClickHouse JSON Encoding EPS

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_CLICKHOUSE_JSON_ENCODER_EPS_PER_THREAD

Description: ClickHouse JSON Encoding EPS per thread

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_ACTIVE_CONSOLIDATION

Description: ClickHouse log integrity active consolidation

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CALCULATE_REQUEST_PARSE_FAILED

Description: Failed to parse log integrity calculate request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CALCULATE_REQUEST_STARTED

Description: ClickHouse partition consolidation request started

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CANDIDATE_PARTITIONS

Description: Clickhouse log integrity candidate partitions

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CONSOLIDATION_DATE

Description: ClickHouse log integrity consolidation target date

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CONSOLIDATION_STATUS_CHANGE

Description: ClickHouse partition consolidation status change

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_DONE

Description: ClickHouse daily consolidation done

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_STARTED

Description: ClickHouse daily consolidation started

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_STOPPED

Description: ClickHouse daily consolidation stopped

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_TIMER

Description: ClickHouse log integrity daily consolidation timer pops

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DB_QUERY_FAILED

Description: ClickHouse log integrity failed to execute query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_EMPTY_PARTITION_CHECKSUM

Description: ClickHouse log integrity empty partition checksum

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_EXEC_FAILED

Description: ClickHouse log integrity system command failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	
errorCode	Error Code	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_MIN_MAX_QUERY_FAILED

Description: ClickHouse log integrity failed min max block query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_OPTIMIZE_COMMAND_FAILED

Description: ClickHouse log integrity optimize command failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_CONSOLIDATION_DONE

Description: ClickHouse partition consolidation done

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	
hashSHA256	SHA256 Hash	string	

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_CONSOLIDATION_STARTED

Description: ClickHouse partition consolidation started

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_UPDATED_AFTER_CHECKSUM

Description: ClickHouse log integrity partition data updated after checksum calculation

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	
hashSHA256	SHA256 Hash	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_MISMATCH

Description: ClickHouse log integrity SHA256 response mismatch

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	
hashSHA256	SHA256 Hash	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_MISMATCH_REPLICAS

Description: ClickHouse log integrity MD5 response mismatch between replicas

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	
hashSHA256	SHA256 Hash	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_PARTITION_INFO_EMPTY

Description: ClickHouse log integrity sha256 target partition info empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
shard	Shard	string	
dbPartition	DB Partition	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_REQUEST_PARSE_FAILED

Description: Failed to parse log integrity sha256 validation request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_EMPTY

Description: Received error for log integrity sha256 response empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_ERROR

Description: Received error for log integrity sha256 validation response error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_PARSE_FAILED

Description: Failed to parse log integrity sha256 validation request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_MOVE_PARTITION_FAILED

Description: Failed to move ClickHouse partitions

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
dbPartition	DB Partition	string	
errReason	Reason for Error	string	This is the reason for an error if given.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_MOVE_PARTITION_STARTED

Description: Move ClickHouse partition started

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
dbPartition	DB Partition	string	
command	Command	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_MOVE_PARTITION_SUCCEEDED

Description: Move ClickHouse partition successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
dbPartition	DB Partition	string	
command	Command	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_NOT_REACHABLE

Description: Failed to reach ClickHouse

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_QUERY_REDIS_CONN_FAILURE

Description: Failed to contact with redis on super

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_QUERY_REDIS_GET_FAILURE

Description: Fail to get values from redis

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_CLICKHOUSE_QUERY_UNCOMPRESS_FAILURE

Description: Failed to uncompress data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_QUERY_ZLIB_INIT_FAILURE

Description: Failed to initialize zlib library

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_QUERY_CHECKIN

Description: ClickHouse query checkin

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_QUERY_CHECKOUT

Description: ClickHouse query checkout

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_THREADS_CHECKIN

Description: ClickHouse query threads checkin

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
replica	Replica	string	
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_THREADS_CHECKOUT

Description: ClickHouse query threads checkout

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
replica	Replica	string	
serverIpAddr	Server IP	IP	
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_CLICKHOUSE_ROUND_ROBIN_INSERTION

Description: Insert events to ClickHouse in roundrobin fashion

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_CLICKHOUSE_ROUND_ROBIN_QUERY

Description: Query from ClickHouse in roundrobin fashion

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_CLICKHOUSE_STORAGE_FREE_SPACE_CRITICAL

Description: ClickHouse lowest storage tier free space critical

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_CLICKHOUSE_STORAGE_FREE_SPACE_LOW

Description: ClickHouse lowest storage tier free space low

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_CLICKHOUSE_STORAGE_UTILS_PER_ORG_PER_DAY

Description: ClickHouse disk utils per organization per day

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_WRITE_FAILED

Description: ClickHouse Insertion failed

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_CLUSTER_COLLECT_ALL_IP_FAILED

Description: 670-Cluster: Failed to collect all ips of one node

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_COLLECT_CONFIG_DATA_FAILED

Description: 670-Cluster: Failed to collect config data of one node

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_CONFIG_SSH_KEY_FAILED

Description: 670-Cluster: Failed to configure SSH key

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_CLUSTER_GET_FW_IP_FAILED

Description: 670-Cluster: Failed to get followerIps

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_GET_TASK_FAILED

Description: 670-Cluster: Failed to get task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_CLUSTER_NOT_SUPPORT_TASK

Description: 670-Cluster: This type device doesn't support this task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_NOT_VALID_FELLOWER

Description: 670-Cluster: The node is invalid

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_RELOAD_CONFIG_FAILED

Description: 670-Cluster: Failed to re-load configuration from app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_RM_DB_FAILED

Description: 670-Cluster: Failed to remove DB

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_RUN_COMMAND_FAILED

Description: 670-Cluster: Failed to run command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_CLUSTER_SCIRPT_FAILED

Description: 670-Cluste: Failed to execute script

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_SEND_TASK_FAILED

Description: 670-Cluster: Failed to send task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_CLUSTER_SSH_KEY_IS_WRONG

Description: 670-Cluster: The SSH key is wrong

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_TASK_DATA_EMPTY

Description: 670-Cluster: Task data is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_TASK_INFO_IS_WRONG

Description: 670-Cluster: Task info is not right

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_TASK_NOT_CONTAIN_LIC

Description: 670-Cluster: There is no license in task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_UPDATE_CONFIG_ERROR

Description: Failed to update config

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propName	Property Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAINTEGRITY_PASSPHRASE_LOAD_ERROR

Description: Data integrity module failed to load passphrase from App Server. Passphrase is needed for signing events

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAINTEGRITY_SIGNER_ERROR

Description: Data integrity module failed to sign event data for message integrity

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAINTEGRITY_UTILS_ERROR

Description: Generic data integrity utilities error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAINTEGRITY_VERIFIER_ERROR

Description: Data integrity module failed to verify event data for message integrity

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAMANAGER_CLICKHOUSE_HTTP_UPLOAD_ERROR

Description: Failed to upload events to ClickHouse

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
serverName	Server Name	string	

EventType: PH_DATAMANAGER_CLUSTER_ENCODE_ERROR

Description: Elasticsearch event encode error while writing events

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_CLUSTER_INIT_ERROR

Description: Elasticsearch client initialization failed

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_CLUSTER_WAIT_ERROR

Description: Elasticsearch client failed tp get event block from sharedstore

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_CLUSTER_WRITER_ERROR

Description: Elasticsearch cluster writer error

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_DASHBOARD_RESPONSE_ERROR

Description: Data Manager failed to respond to Query Master for summary dashboard query requests

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_ELASTICWRITER_ERROR

Description: Elasticsearch client failed to write events to Elasticsearch

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTATTR_ERROR

Description: Data Manager found unknown event attribute while writing to database

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_EVTCACHE_DUPLICATE_ERROR

Description: Data Manager found duplicate event id in event cache for trigger event query

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_EVTCACHE_GET_ERROR

Description: Data Manager failed to get event from event cache for trigger event query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTCACHE_PARSE_ERROR

Description: Data Manager failed to parse trigger event query XML from Query Master

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTDBNOTIFIER_ERROR

Description: Data Manager failed to upload event-file-signature related details to App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTIDX_CORRUPT_ERROR

Description: Data Manager detected event index corruption

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAMANAGER_EVTIDX_MERGE_ERROR

Description: Data Manager failed to merge event index

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.
dirName	Directory Name	string	

EventType: PH_DATAMANAGER_EVTIDX_QUERY_ERROR

Description: Data Manager failed to read event index during query

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTIDX_READ_BLOCK_ERROR

Description: Data Manager failed to read event file block during query or index merge

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTIDX_READ_KEY_ERROR

Description: Data Manager failed to read event file index during query or index merge

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTIDX_READ_POST_ERROR

Description: Data Manager failed to read event index posting file during query or index merge

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTIDX_WRITE_ERROR

Description: Data Manager failed to write event index

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAMANAGER_EVTIDX_WRITE_KEY_ERROR

Description: Data Manager failed to write event index file key

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAMANAGER_EVTIDX_WRITE_POST_ERROR

Description: Data Manager failed to write event index posting file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTLOADER_ERROR

Description: Data Manager failed to load events from shared buffer

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
dirName	Directory Name	string	

EventType: PH_DATAMANAGER_EVTWRITER_ERROR

Description: Data Manager failed to store events to event database

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_DATAMANAGER_EXPORT_ERROR

Description: Data Manager failed to export events from event database

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_FILE_READ_FAILURE

Description: FortiSIEM DataManager failed to read file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_DATAMANAGER_FILE_RENAME_FAILURE

Description: FortiSIEM DataManager failed to rename file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_DATAMANAGER_FILE_SIGN_ERROR

Description: Data Manager failed to sign event files for message integrity

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_DATAMANAGER_FILE_WRITE_FAILURE

Description: FortiSIEM DataManager failed to write file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_DATAMANAGER_GET_SIGN_ERROR

Description: Data Manager failed to read event message integrity signatures

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_DATAMANAGER_GLOBAL_CACHE_MISSING

Description: FortiSIEM DataManager missing global cache

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_HDFSWRITER_ERROR

Description: Data Manager module failed to write to HDFS

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
infoURL	Informational URL	string	This field captures an URL if present in an event
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATAMANAGER_HTTP_UPLOAD_ERROR

Description: Data Manager module failed to upload event database statistics to App server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_DATAMANAGER_INIT_ERROR

Description: Data Manager module initialization error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_INTEGRITY_CHECK_ERROR

Description: Data Manager failed to do integrity check for certain event files

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAMANAGER_INTEGRITY_RESPONSE_ERROR

Description: Data Manager failed to respond to App Server for log integrity check requests

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_INVALID_LOG_FILE

Description: FortiSIEM DataManager invalid log file

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_KAFKAWRITER_CONFIG_ERROR

Description: Data Manager failed to load Kafka configuration from App server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_KAFKAWRITER_ERROR

Description: Data Manager failed to write events to Kafka message bus

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorString	Error String	string	This is the error message, synonymous to attribute errReason
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_DATAMANAGER_LOG_BUFFER_PAUSED_LOW_SPACE

Description: PerCust event buffer is paused because of low free space

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_LOG_BUFFER_PAUSED_STATFS_FAILURE

Description: PerCust event buffer is paused because of statfs failure

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_LOG_BUFFER_RESUMED

Description: PerCust event buffer is resumed

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_PUT_SIGN_ERROR

Description: Data Manager failed to store event file integrity signatures

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_DATAMANAGER_QUERY_EXPR_ERROR

Description: Data Manager failed to parse trigger event query expression

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_QUERY_RESPONSE_ERROR

Description: Data Manager failed to respond to Query Master for incident trigger event query requests

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_REDIS_KEY_NOT_EXIST

Description: redis key not exist

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_SUMMARYWRITER_ERROR

Description: Data Manager failed to write inline report results

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_DATAMGR_BAD_EVTBLKIDX_FILE

Description: Bad event block index file

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_BAD_SEGMENT

Description: Bad data segment

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_INDEX_MERGE_FAILED

Description: Failed to merge indices

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_INDEX_MERGE_FAILED_INDEX

Description: Index that failed to merge

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_INDEX_MERGE_FAILED_INDEX_GROUP

Description: Index group that failed to merge

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_SEGMENT_MERGE_ERROR

Description: Datamgr segment merge error

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_SEGMENT_MERGE_FAILED

Description: Failed to merge segments

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_UNABLE_FLUSH_INDEX

Description: Failed to flush index

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_UNABLE_OPEN_EVTBLK_FILE

Description: Unable to open event block file

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAPURGER_ARCHIVE_TASK_ERROR

Description: Data Purger failed to archive events but they are purged

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_CMD_FAILURE

Description: Data Purger failed to run command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
errorNoInt	Error Number Int	int32	

EventType: PH_DATAPURGER_DR_ES_RESTORE_FAILED

Description: Data Purger failed to do restore for Disaster Recovery

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_DR_ES_ROLE_UNKNOWN

Description: Elasticsearch Disaster Recovery Role is Unknown

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAPURGER_DR_ES_SNAPSHOTS_GET_FAILED

Description: Data Purger failed to get snapshots for Disaster Recovery

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_DR_ES_SNAPSHOT_DELETION_FAILED

Description: Data Purger failed to delete snapshots for Disaster Recovery

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_DR_ES_SNAPSHOT_FAILED

Description: Data Purger failed to do snapshot for Disaster Recovery

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_DUCHECKER_ERROR

Description: Data Purger failed to check disk usage

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_ENFORCE_ERROR

Description: Data Purger failed to enforce event purging policy

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_EVAL_ERROR

Description: Data Purger failed to evaluate event purging policies for a particular day

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_HTTP_UPLOAD_ERROR

Description: Data Purger failed to upload disk usage to App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_INIT_ERROR

Description: Data Purger module initialization error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_OPEN_FILE_ERROR

Description: Data Purger module failed to open file

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_DATAPURGER_PARSE_XML_ERROR

Description: Data Purger module failed to parse XML containing purging policies received from App server

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAPURGER_POLICY_ERROR

Description: Data Purger failed to implement specific event purging policy

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_RESPONSE_ERROR

Description: Data Purger module failed to handle event database refresh/restore related requests from App server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_STORAGE_POLICY_CLICKHOUSE_NODES_EMPTY

Description: Data Purger failed to retrieve ClickHouse nodes from Redis

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATA_CLUSTER_ALL_COORDINATOR_DOWN

Description: All Coordinator nodes are down or not reachable or not responsive

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_DATA_CLUSTER_BUSY

Description: Elasticsearch cluster is busy

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_DATA_CLUSTER_CLICKHOUSE_CONFIG_NO_PORT

Description: ClickHouse PORT is not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_COORDINATOR_DOWN

Description: Coordinator is down or not reachable or not responsive

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_DATA_CLUSTER_COORDINATOR_UP

Description: Coordinator is up

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_HTTPPORT

Description: Elasticsearch cluster HTTP PORT is not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_IP

Description: Elasticsearch cluster IP is not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_JAVAPORT

Description: FortiSIEM Elasticsearch configuration missing Java port

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NAME

Description: FortiSIEM Elasticsearch configuration missing cluster name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NUMREPLICAS

Description: FortiSIEM Elasticsearch configuration missing number of replica

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NUMSHARD

Description: FortiSIEM Elasticsearch configuration missing number of shards

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NULL

Description: Elasticsearch cluster not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_WRONG_FORMAT

Description: Wrng response format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATA_CLUSTER_ELASTIC_EVENTID_NOT_FOUND

Description: Elasticsearch error string doesn't contain enough information

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_HTTP_CLIENT_FAIL

Description: Elasticsearch REST API call to AppSrv failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_HTTP_CMD_FAIL

Description: Elasticsearch REST API call fails

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
msg	Message	string	

EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_FAIL

Description: Elasticsearch indexing failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
size	Size	uint32	

EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_RESEND_FAIL

Description: Elasticsearch indexing failed 2nd time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
size	Size	uint32	

EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FAIL

Description: Elasticsearch indexing failed at the last time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
size	Size	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FIRST_FAIL

Description: Elasticsearch indexing failed at 1st time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
size	Size	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_UPLOAD_FAIL

Description: Elasticsearch event upload via REST API failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATA_CLUSTER_ELASTIC_WRONG_JSON_FORMAT

Description: Elasticsearch "_cat/indices" API response format wrong format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATA_CLUSTER_GET_HOSTNAME_FAIL

Description: Elasticsearch popen hostname failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_PORT

Description: HDFS port in not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_SERVER

Description: HDFS server in not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_YARN_PORT

Description: HDFS yarn port in not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_YARN_SERVER

Description: HDFS yarn server in not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NULL

Description: HDFS cluster is not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_HTTP_CMD_FAIL

Description: HDFS REST API call to AppSrv failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
infoURL	Informational URL	string	This field captures an URL if present in an event
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
msg	Message	string	

EventType: PH_DATA_CLUSTER_HDFS_LISTSTATUS_FAIL

Description: HDFS LISTSTAUTS API failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_SEND_FAIL

Description: HDFS storing events failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATA_CLUSTER_HDFS_UPLOAD_FAIL

Description: HDFS event upload via REST API failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_DATA_CLUSTER_JSON_GET_ATTRIBUTE_NAME_FAIL

Description: Elasticsearch Event Attribute name fetch failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_ARCHIVE_STORAGE_CHECK_ERROR

Description: Failed to get disk usage of Elasticsearch Cluster archive

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_ES_ARCHIVE_STORAGE_LOW

Description: The available storage of archive for Elasticsearch Cluster is low

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_ARCHIVE_STORAGE_PURGING_FAILED

Description: Failed purge snapshot from archive on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_ES_ARCHIVE_STORAGE_PURGING_FINISHED

Description: Finished purge snapshot from archive on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_ARCHIVE_STORAGE_PURGING_STARTED

Description: Start purge snapshots from archive on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_ARCHIVE_STORAGE_PURGING_SUCCESS

Description: Succeed purge snapshots from archive on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_ARCHIVE_STORAGE_USAGE

Description: Disk usage of Elasticsearch Cluster archive

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_CCR_DELAY

Description: Elasticsearch CCR delay detail

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_COLD_STORAGE_ARCHIVING_FAILED

Description: Failed to archive indices from cold nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_COLD_STORAGE_ARCHIVING_FINISHED

Description: Finished archive indices from cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_COLD_STORAGE_ARCHIVING_STARTED

Description: Start archive indices from cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_COLD_STORAGE_ARCHIVING_SUCCESS

Description: Successfully archived indices from cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_COLD_STORAGE_CHECK_ERROR

Description: Failed to get disk usage of Elasticsearch Cluster cold nodes

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_ES_COLD_STORAGE_LOW

Description: The available storage of cold nodes on Elasticsearch Cluster is low

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_COLD_STORAGE_PURGING_FAILED

Description: Failed purge indices from cold nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_COLD_STORAGE_PURGING_FINISHED

Description: Finished purge indices from cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_COLD_STORAGE_PURGING_STARTED

Description: Start purge indices from cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_COLD_STORAGE_PURGING_SUCCESS

Description: Succeed purge indices from cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_COLD_STORAGE_USAGE

Description: Disk usage of Elasticsearch Cold nodes

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_HOTCOLD_STORAGE_MOVING_FAILED

Description: Failed move indices from Hot to cold nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_HOTCOLD_STORAGE_MOVING_FINISHED

Description: Finished moved indices from Hot to cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOTCOLD_STORAGE_MOVING_STARTED

Description: Start move indices from Hot to cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOTCOLD_STORAGE_MOVING_SUCCESS

Description: Succeed moved indices from Hot to cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_ARCHIVING_FAILED

Description: Failed archive indices from hot nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_HOT_STORAGE_ARCHIVING_FINISHED

Description: Finished archive indices from hot nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_ARCHIVING_STARTED

Description: Start archive indices from hot nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_ARCHIVING_SUCCESS

Description: Succeed archive indices from hot nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_CHECK_ERROR

Description: Failed to get disk usage of Elasticsearch Cluster Hot Nodes

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_ES_HOT_STORAGE_LOW

Description: The available storage of Hot Nodes on Elasticsearch Cluster is low

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_HOT_STORAGE_MOVING_FAILED

Description: Failed move indices from Hot to warm nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_HOT_STORAGE_MOVING_FINISHED

Description: Finished moved indices from Hot to warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_MOVING_STARTED

Description: Start move indices from Hot to warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_MOVING_SUCCESS

Description: Succeed moved indices from Hot to warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_PURGING_FAILED

Description: Failed purge indices from hot nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_HOT_STORAGE_PURGING_FINISHED

Description: Finished purge indices from hot nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_PURGING_STARTED

Description: Start purge indices from hot nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_PURGING_SUCCESS

Description: Succeed purge indices from hot nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_USAGE

Description: Disk usage of Elasticsearch Hot Nodes

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_INDEX_SEGMENT_MERGE_FAILED

Description: Elasticsearch index segment merge failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_ES_REST_FAILED

Description: ES REST returns error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_SM_ADD_INDEX_FAILED

Description: Failed to add ShardManager Index

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_SM_HOURLCHECK_FAILED

Description: Failed ShardManager hourcheck

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_SM_INIT_FAILED

Description: Failed to init ShardManager

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_SM_INIT_INDEX_FAILED

Description: Failed to init ShardManager Index

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_SNAPSHOT_FAILED

Description: Failed to do snapshot for ES

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_TO_NFS_ARCHIVE_FAILED_ADD_INDEX

Description: ES TO NFS Archive failed to add an index

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_WARM_STORAGE_ARCHIVING_FAILED

Description: Failed to archive indices from warm nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_WARM_STORAGE_ARCHIVING_FINISHED

Description: Finished archive indices from warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_ARCHIVING_STARTED

Description: Start archive indices from warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_ARCHIVING_SUCCESS

Description: Successfully archived indices from warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_CHECK_ERROR

Description: Failed to get disk usage of Elasticsearch Cluster warm nodes

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_ES_WARM_STORAGE_LOW

Description: The available storage of warm nodes on Elasticsearch Cluster is low

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_WARM_STORAGE_MOVING_FAILED

Description: Failed move indices from Warm to cold nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_WARM_STORAGE_MOVING_FINISHED

Description: Finished moved indices from Warm to cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_MOVING_STARTED

Description: Start move indices from Warm to cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_MOVING_SUCCESS

Description: Succeed moved indices from Warm to cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_PURGING_FAILED

Description: Failed purge indices from warm nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_WARM_STORAGE_PURGING_FINISHED

Description: Finished purge indices from warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_PURGING_STARTED

Description: Start purge indices from warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_PURGING_SUCCESS

Description: Succeed purge indices from warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_USAGE

Description: Disk usage of Elasticsearch Warm nodes

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_HDFS_ARCHIVE_STORAGE_LOW

Description: The available storage of HDFS Archive database is low

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_HDFS_ARCHIVE_STORAGE_USAGE

Description: Storage usage of HDFS Archive database

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_HDFS_PURGING_FAILED

Description: Failed purging from HDFS Archive database

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_HDFS_PURGING_FINISHED

Description: Finished purging from HDFS Archive database - triggered by low space

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_HDFS_PURGING_STARTED

Description: Started purging from HDFS Archive database - triggered by low space

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_HDFS_PURGING_SUCCESS

Description: Successfully purged from HDFS Archive database - triggered by low space

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_SYSTEM_ARCHIVE_LOW

Description: FortiSIEM EventDB Archive disk space low

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGED_LOW_SPACE

Description: Event database archive files purged to make room for new archive

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGED_POLICY

Description: Event database archive files purged by policy

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_FAILED

Description: Failed to purge Archive FortiSIEM EventDB - purge caused by low available space

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_FINISHED

Description: Successfully purged Archive FortiSIEM EventDB -purge caused by low available space

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_STARTED

Description: Started to purge Archive FortiSIEM EventDB because of low available space

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_SUCCESS

Description: Successfully purged Archive FortiSIEM EventDB because of low available space

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_FAILED

Description: Failed to purge Archive FortiSIEM EventDB - purge caused by policy

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_FINISHED

Description: Successfully purged Archive FortiSIEM EventDB - purge caused by policy

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_STARTED

Description: Started to purge Archive FortiSIEM EventDB - purge caused by policy

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_SUCCESS

Description: Successfully purged Archive FortiSIEM EventDB - purge caused by policy

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_RETENTION_POLICY_VIOLATED

Description: Archive retention policy violation

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_SYSTEM_ARCHIVE_USAGE

Description: Archive disk usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
diskUsage	Disk Used MB	uint64	

EventType: PH_SYSTEM_DATAMGR_ARCHIVE_SKIP

Description: Online FortiSIEM EventDB Archiving skipped since the directory has data

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_ARCHIVING_FAILED

Description: Online FortiSIEM EventDB Archiving encountered errors

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_ARCHIVING_FINISHED

Description: Online FortiSIEM EventDB Archiving completed

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_ARCHIVING_STARTED

Description: Online FortiSIEM EventDB Archiving started

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_ARCHIVING_SUCCESS

Description: Online FortiSIEM EventDB Archiving success

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_PURGED

Description: Event database files purged

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_SYSTEM_DISK_PURGING_FAILED

Description: Online FortiSIEM EventDB Purging encountered errors

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_PURGING_FINISHED

Description: Online FortiSIEM EventDB Purging completed

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_PURGING_STARTED

Description: Online FortiSIEM EventDB Purging started

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_PURGING_SUCCESS

Description: Online FortiSIEM EventDB Purging success

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_USAGE

Description: Disk usage of customer

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
diskUsage	Disk Used MB	uint64	

EventType: PH_SYSTEM_DISK_USAGE_WARNING

Description: FortiSIEM EventDB disk usage close to limit

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_SYSTEM_ONLINE_RETENTION_POLICY_VIOLATED

Description: Online data retention policy violation

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
policyName	Policy Name	string	

EventType: PH_SYSTEM_RETENTION_POLICY_EXEC_TIME

Description: Data retention policy enforcement time

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
runTime	Run Time	uint64	

EventType: PH_SYSTEM_RETENTION_POLICY_FAILED

Description: Data retention policy enforcement failed

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_SYSTEM_RETENTION_POLICY_FINISHED

Description: Data retention policy enforcement finished

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_RETENTION_POLICY_STARTED

Description: Data retention policy enforcement started

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_RETENTION_POLICY_STATS

Description: Data retention policy enforcement statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_SYSTEM_RETENTION_POLICY_SUCCESS

Description: Data retention policy enforcement succeeded

Severity: 1 (Low)

Event Category: 3 (System Logs)

Discovery Logs

This section provides logs related to Test Connectivity and Discovery.

- PH_DEVICE_NOT_ADDED
- PH_DISCOVERY_COMPLETE
- PH_DISCOVERY_RESULT_SENT
- PH_DISCOV_ACCESS_IP_PARSE_ERROR
- PH_DISCOV_ADS_ACCOUNT_TO_EXPIRE
- PH_DISCOV_ADS_ACCT_DISABLED
- PH_DISCOV_ADS_DORMANT_ACCT
- PH_DISCOV_ADS_PASSWORD_NEVER_EXPIRES
- PH_DISCOV_ADS_PASSWORD_NOT_REQD
- PH_DISCOV_ADS_PASSWORD_STALE
- PH_DISCOV_ADS_PASSWORD_TO_EXPIRE
- PH_DISCOV_ARUBA_WLAN_HOST_LOCATION
- PH_DISCOV_AWS_DEVICE_DELETED
- PH_DISCOV_AWS_DEVICE_UNKNOWN
- PH_DISCOV_AWS_DISCOV_FAILED
- PH_DISCOV_AZURE_DISCOV_FAILED
- PH_DISCOV_BASIC_FAILED
- PH_DISCOV_BASIC_SKIPPED
- PH_DISCOV_BASIC_SNMP_DETAIL
- PH_DISCOV_BASIC_SNMP_ERROR
- PH_DISCOV_BASIC_SNMP_FAILED
- PH_DISCOV_BASIC_SNMP_STARTED
- PH_DISCOV_BASIC_SNMP_SUCCESS
- PH_DISCOV_BASIC_SSH_DETAIL
- PH_DISCOV_BASIC_SSH_ERROR
- PH_DISCOV_BASIC_SSH_FAILED
- PH_DISCOV_BASIC_SSH_STARTED
- PH_DISCOV_BASIC_SSH_SUCCESS
- PH_DISCOV_BASIC_STARTED
- PH_DISCOV_BGP_OSPF_FAILED
- PH_DISCOV_BROCADE_SERVER_IRON_HW_INFO_WARNING
- PH_DISCOV_CANCEL_UNKNOWN_REQ
- PH_DISCOV_CERT_FILE_DOWNLOAD_FAILURE
- PH_DISCOV_CHECKPOINT_TEST_CONN_FAILED
- PH_DISCOV_CISCO_ASA_GET_CONTEXT_FAILED
- PH_DISCOV_CISCO_ASA_IPSEC_VPN_FAILED
- PH_DISCOV_CISCO_ASA_RAS_VPN_FAILED

- PH_DISCOV_CISCO_ASA_RUN_CONFIG_FAILED
- PH_DISCOV_CISCO_ASA_SET_CONTEXT_FAILED
- PH_DISCOV_CISCO_ASA_STARTUP_CONFIG_FAILED
- PH_DISCOV_CISCO_CALL_MANAGER_WARNING
- PH_DISCOV_CISCO_CATOS_INTF_FAILED
- PH_DISCOV_CISCO_CDP_ERROR
- PH_DISCOV_CISCO_IOS_L2_WARNING
- PH_DISCOV_CISCO_IOS_TRUNK_PORT_ERROR
- PH_DISCOV_CISCO_JUNOS_L2_WARNING
- PH_DISCOV_CISCO_NXOS_HW_STATUS_WARNING
- PH_DISCOV_CISCO_NXOS_INTF_SHORT_NAME_NOT_FOUND
- PH_DISCOV_CISCO_NXOS_L2_WARNING
- PH_DISCOV_CISCO_WLAN_HOST_LOCATION
- PH_DISCOV_CLOCK_ROLLS_BACK
- PH_DISCOV_CONTACT_APP_SERVER
- PH_DISCOV_CREDEN_INSERT_ERROR
- PH_DISCOV_CUSTOM_MAP_LOAD_FAILED
- PH_DISCOV_DATA_DOMAIN_HW_STATUS_WARNING
- PH_DISCOV_DELL_BLADE_CHASSIS_WARNING
- PH_DISCOV_DELL_COMPELLENT_STORAGE_WARNING
- PH_DISCOV_DISCOV_REQ_GET_FAILED
- PH_DISCOV_DISCOV_RESULT_SENDER_THREADS_SPAWN_FAILED
- PH_DISCOV_DISCOV_THREADS_SPAWN_FAILED
- PH_DISCOV_EC2_INSTANCE_PARSE_FAILED
- PH_DISCOV EMC_CLARION_ERROR
- PH_DISCOV EMC_VNX_DISCOV_FAILED
- PH_DISCOV EMC_VNX_PING_FAILED
- PH_DISCOV_EQLOGIC_CONN_FAILED
- PH_DISCOV_EQLOGIC_HW_INFO_FAILED
- PH_DISCOV_ESX_HOST_PING_ONLY_DISCOV_ERROR
- PH_DISCOV_FAILED_INVALID_REQUEST
- PH_DISCOV_FAILED_INVALID_REQUEST_XML
- PH_DISCOV_FAILED_XML_ERROR
- PH_DISCOV_FAIL_CMDB_DEV
- PH_DISCOV_FILE_BASED_DISCOV_DIR_NOT_CONFIGURED
- PH_DISCOV_FILE_BASED_DISCOV_FAILED
- PH_DISCOV_FORTINET_CPU_INFO_WARNING
- PH_DISCOV_FORTINET_LINK_STAT_WARNING
- PH_DISCOV_FORTINET_SYS_UPDATE_VERSION_WARNING
- PH_DISCOV_GENERIC_ERROR
- PH_DISCOV_GEN_WLAN_HOST_LOCATION
- PH_DISCOV_GET_SNMP_ENGINE_ID_FAILED
- PH_DISCOV_HOST_CONVERT_PROCESS_UPTIME_ERROR

- PH_DISCOV_HOST_ERROR
- PH_DISCOV_HOST_INSTALL_SW_WARNING
- PH_DISCOV_HOST_LOCATE_PROCESS_ERROR
- PH_DISCOV_HOST_LOCATION
- PH_DISCOV_HOST_NET_INTF
- PH_DISCOV_HOST_STARTED
- PH_DISCOV_HOST_SUCCESS
- PH_DISCOV_HOST_SUCCESS_DETAIL
- PH_DISCOV_HOST_WARNING
- PH_DISCOV_HP3COM_HW_WARNING
- PH_DISCOV_HP_BLADE_HW_STATUS_WARNING
- PH_DISCOV_INIT_MODULE_FAILED
- PH_DISCOV_INTERFACE_VIA_SNMP_FAILED
- PH_DISCOV_IP_TYPE_INVALID
- PH_DISCOV_ISILON_HW_STATUS_WARNING
- PH_DISCOV_JMX_TEST_CONN_FAILED
- PH_DISCOV_JUNIPER_SSG_HW_INFO_WARNING
- PH_DISCOV_L2_FAILED
- PH_DISCOV_L2_STARTED
- PH_DISCOV_L2_SUCCESS
- PH_DISCOV_LDAP_ERROR
- PH_DISCOV_LDAP_OU_ERROR
- PH_DISCOV_LINUX_DSKTABLE_NOT_CONFIG
- PH_DISCOV_LOGIN_ERROR
- PH_DISCOV_NEXT_HOP_VIA_SNMP_FAILED
- PH_DISCOV_NIMBLE_VOLUME_WARNING
- PH_DISCOV_NOZOMI_DISCOV_FAILED
- PH_DISCOV_PARAM_PARSE_FAILED
- PH_DISCOV_PARSER_MSG_EXCEEDS_THRESHOLD
- PH_DISCOV_PARSER_MSG_THREAD_SPAWN_FAILED
- PH_DISCOV_PERF_TEMPLATE_LOAD_FAILED
- PH_DISCOV_PING_ONLY_LIST_NOT_MATCH
- PH_DISCOV_READ_COMPRESS_THRESHOLD_FAILED
- PH_DISCOV_RECVD_VALID_REQUEST
- PH_DISCOV_RESULT_SEND_FAILED
- PH_DISCOV_RESULT_SEND_WARNING
- PH_DISCOV_RESULT_XML_WRITE_FAILURE
- PH_DISCOV_RUNNING_SERVICE
- PH_DISCOV_RUN_JAVA_PROBE_ERROR
- PH_DISCOV_RUN_SW_FILTER_LOAD_FAILED
- PH_DISCOV_RUN_SW_FILTER_PARSE_FAILED
- PH_DISCOV_RUN_VM_TEST_CONN_ERROR
- PH_DISCOV_SKIPPED

- PH_DISCOV_SKIP_DEV
- PH_DISCOV_SNMP_ERROR
- PH_DISCOV_SSH_ERROR
- PH_DISCOV_START
- PH_DISCOV_TELNET_ERROR
- PH_DISCOV_TEST_CONN_GET_REQ_FAILED
- PH_DISCOV_TEST_CONN_MSRPC_ERROR
- PH_DISCOV_TEST_CONN_NO_UCSAPI_CRED
- PH_DISCOV_TEST_CONN_RESULT_SENDER_THREADS_SPAWN_FAILED
- PH_DISCOV_TEST_CONN_RESULT_SEND_ERROR
- PH_DISCOV_TEST_CONN_RESULT_SEND_WARNING
- PH_DISCOV_TEST_CONN_THREADS_SPAWN_FAILED
- PH_DISCOV_TEST_CONN_VMSDK_ERROR
- PH_DISCOV_TRIPP_UPS_HW_STATUS_WARNING
- PH_DISCOV_TRUNK_PORTS_ERROR
- PH_DISCOV_UNHANDLED_ACCESS_PROTO
- PH_DISCOV_UPLOAD_DATA_FAILED
- PH_DISCOV_VMWARE_DUP_DEV_ID
- PH_DISCOV_VMWARE_ERROR
- PH_DISCOV_VOIP_PHONE_ID
- PH_DISCOV_WMI_PULL_ERROR
- PH_LIB_TOPO_APACHE_PING_FAILED
- PH_LIB_TOPO_APP_GROUP_FILTER_PARSE_ERROR
- PH_LIB_TOPO_APP_GROUP_FILTER_PUSH_ERROR
- PH_LIB_TOPO_AWS_NEW_INSTANCE_NOT_RUN
- PH_LIB_TOPO_AWS_OBTAIN_INSTANCE_FAILURE
- PH_LIB_TOPO_CHECK_APP_LIST_WARNING
- PH_LIB_TOPO_CISCO_IOS_CBQOS_ERROR
- PH_LIB_TOPO_CISCO_MERAKI_GET_CHILD_DEVICE_WARNING
- PH_LIB_TOPO_CISCO_MERAKI_GET_INTFS_WARNING
- PH_LIB_TOPO_CISCO_MERAKI_GET_INTF_WARNING
- PH_LIB_TOPO_CISCO_MERAKI_MAC_2_HOST_LOOKUP_FAILED
- PH_LIB_TOPO_CISCO_MERAKI_MAC_2_INTF_LOOKUP_FAILED
- PH_LIB_TOPO_CISCO_UCS_LOGIN_FAILED
- PH_LIB_TOPO_CISCO_UCS_REQUEST_ERROR
- PH_LIB_TOPO_CPU_TOO_HIGH
- PH_LIB_TOPO_CUST_CONFIG_JOB_DOWNLOAD_SCRIPT_FAILED
- PH_LIB_TOPO_CUST_FIM_JOB_CHECK_PATH_ERROR
- PH_LIB_TOPO_CUST_FIM_JOB_DEVICE_UNAVAILABLE
- PH_LIB_TOPO_CUST_FIM_JOB_FILE_TOO_LARGE
- PH_LIB_TOPO_CUST_FIM_JOB_GET_DATA_FAILED
- PH_LIB_TOPO_CUST_FIM_JOB_GET_FILE_INFO_FAILED
- PH_LIB_TOPO_CUST_FIM_JOB_GET_MD5_FAILED

- PH_LIB_TOPO_CUST_FIM_JOB_GET_REMOTE_FILE_ERROR
- PH_LIB_TOPO_CUST_FIM_JOB_INCORRECT_CRED
- PH_LIB_TOPO_CUST_FIM_JOB_RUN_SCP_FAILED
- PH_LIB_TOPO_CUST_FIM_JOB_TOO_MANY_FILES
- PH_LIB_TOPO_CUST_LOGIN_JOB_CREATE_EVENT_FAILED
- PH_LIB_TOPO_CUST_LOGIN_JOB_GET_DATA_FAILED
- PH_LIB_TOPO_CUST_SNMP_JOB_CREATE_EVENT_FAILED
- PH_LIB_TOPO_CUST_SNMP_JOB_GET_DATA_FAILED
- PH_LIB_TOPO_CUST_WMI_JOB_CREATE_EVENT_FAILED
- PH_LIB_TOPO_CUST_WMI_JOB_GET_DATA_FAILED
- PH_LIB_TOPO_ETHERMIB_STAT_LOOKUP_ERROR
- PH_LIB_TOPO_EVENT_DROP_RULE_ENCODE_VALUE_GROUP_ERROR
- PH_LIB_TOPO_EVENT_DROP_RULE_PARSE_ERROR
- PH_LIB_TOPO_EXCLUDED_DISK_PARSE_ERROR
- PH_LIB_TOPO_FCT_DEV_MAPPING_ENTRY_INVALID
- PH_LIB_TOPO_FGT_FABRIC_DISCOV_FAIL
- PH_LIB_TOPO_FGT_GET_CONFIG_BACKUP_FAILED
- PH_LIB_TOPO_FGT_GET_USER_DEV_STORE_FAIL
- PH_LIB_TOPO_FGT_GET_USER_DEV_UNKNOWN
- PH_LIB_TOPO_FGT_INSTALLED_SW_FAIL
- PH_LIB_TOPO_FGT_SEC_POSTURE_RPT_API_FAIL
- PH_LIB_TOPO_FILE_READ_ERROR
- PH_LIB_TOPO_FOUNDRY_HW_STATUS_ERROR
- PH_LIB_TOPO_GEN_UPS_STATUS_GET_ERROR
- PH_LIB_TOPO_GET_NETAPP_NFS_FAILED
- PH_LIB_TOPO_H3C_CPU_UTIL_ERROR
- PH_LIB_TOPO_HP3COM_CPU_UTIL_ERROR
- PH_LIB_TOPO_HP3COM_MEM_UTIL_ERROR
- PH_LIB_TOPO_HPUX_PROC_CPU_MEM_TOO_HIGH
- PH_LIB_TOPO_HYPERV_METRICS_GET_ERROR
- PH_LIB_TOPO_IMPORTANT_INTF_PARSE_ERROR
- PH_LIB_TOPO_INTF_UTIL_ERROR
- PH_LIB_TOPO_JSON_PARSE_FAILED
- PH_LIB_TOPO_JUNIPER_INTF_SPEED_GET_ERROR
- PH_LIB_TOPO_LIEBERT_HVAC_STATUS_GET_ERROR
- PH_LIB_TOPO_LOGIN_PING_FAILED
- PH_LIB_TOPO_MAINTENANCE_DURATION_INCORRECT
- PH_LIB_TOPO_MEM_TOO_HIGH
- PH_LIB_TOPO_NETAPP_AGGREGATE_STAT_ERROR
- PH_LIB_TOPO_NETAPP_ANALYZE_VERSION_ERROR
- PH_LIB_TOPO_NETAPP_DISK_STAT_ERROR
- PH_LIB_TOPO_NETAPP_GET_NFS_METRIC_ERROR
- PH_LIB_TOPO_NETAPP_GET_VERSION_ERROR

- PH_LIB_TOPO_NETAPP_LUN_STAT_ERROR
- PH_LIB_TOPO_NETAPP_PROTO_STAT_ERROR
- PH_LIB_TOPO_NETAPP_VOLUME_STAT_ERROR
- PH_LIB_TOPO_NOT_SUPPORT_REST_API
- PH_LIB_TOPO_OPEN_FILE_FAILED
- PH_LIB_TOPO_PARSE_INTF_MAP_FAILURE
- PH_LIB_TOPO_PERF_JOB_EXEC_FAILED
- PH_LIB_TOPO_PERF_JOB_INIT_FAILED
- PH_LIB_TOPO_PERF_JOB_REMOVE_FAILED
- PH_LIB_TOPO_PERF_TEMPLATE_LOAD_ERROR
- PH_LIB_TOPO_PERF_TEMPLATE_PARSE_FAILURE
- PH_LIB_TOPO_PERF_TEMPLATE_PARSE_WARNING
- PH_LIB_TOPO_PORT_FILTER_PARSE_ERROR
- PH_LIB_TOPO_PORT_FILTER_PUSH_ERROR
- PH_LIB_TOPO_PROC_CPU_MEM_TOO_HIGH
- PH_LIB_TOPO_REST_API_FAILED
- PH_LIB_TOPO_RUN_SW_FILTER_PARSE_ERROR
- PH_LIB_TOPO_RUN_SW_FILTER_PUSH_ERROR
- PH_LIB_TOPO_SNMPWALK_ERROR
- PH_LIB_TOPO_STM_JOB_EXEC_FAILED
- PH_LIB_TOPO_STM_JOB_INIT_FAILED
- PH_LIB_TOPO_TEST_CONN_HTTP_AGENT_FAILED
- PH_LIB_TOPO_TEST_CONN_JDBC_AGENT_FAILED
- PH_LIB_TOPO_TEST_CONN_JMX_AGENT_FAILED
- PH_LIB_TOPO_TRUNK_PORT_MAP_PARSE_ERROR
- PH_LIB_TOPO_VALIDATE_ACCESS_FAILED
- PH_LIB_TOPO_WIN_GET_EXCH_DATABASE_INSTANCE_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_DATABASE_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_MAIL_SUBMISSION_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_PUB_MAILBOX_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_REG_MAILBOX_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_REPLICATION_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_RPC_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_SMTP_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_STORE_INTF_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_TRANSPORT_QUEUE_WARNING
- PH_LIB_TOPO_WMI_GET_CPU_COUNT_ERROR
- PH_LIB_TOPO_WMI_GET_CPU_WARNING
- PH_LIB_TOPO_WMI_GET_PAGE_ACTIVITY_ERROR
- PH_LIB_TOPO_WMI_GET_REAL_MEM_ERROR
- PH_LIB_TOPO_WMI_GET_RUN_SW_PERF_ERROR
- PH_MAX_DEVICES_EXCEEDED
- PH_MAX_DEVICES_LIMIT_REACHED

- PH_TEST_CONN_COMPLETE
- PH_TEST_CONN_CONTACT_APP_SERVER
- PH_TEST_CONN_FAILED
- PH_TEST_CONN_FAILED_INVALID_REQUEST
- PH_TEST_CONN_FAILED_INVALID_REQUEST_XML
- PH_TEST_CONN_RECVD_VALID_REQUEST
- PH_TEST_CONN_RESULT_SENT
- PH_TEST_CONN_STARTED

EventType: PH_DEVICE_NOT_ADDED

Description: Discovered device not added to CMDB because of license restrictions

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOVERY_COMPLETE

Description: Discovery completed

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DISCOVERY_RESULT_SENT

Description: Discovery results sent to app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_ACCESS_IP_PARSE_ERROR

Description: Discovery module failed to parse device Access IP from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_ADS_ACCOUNT_TO_EXPIRE

Description: Active Directory account to expcure in 2 weeks

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	
daysToAccountExpiry	Days To Account Expiry	uint32	

EventType: PH_DISCOV_ADS_ACCT_DISABLED

Description: Accounts Disabled

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	

EventType: PH_DISCOV_ADS_DORMANT_ACCT

Description: Dormant User Accounts - not log on in last 30 days

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	
lastLogon	Last Logon Time	Date	
daysSinceLastLogon	Days Since Last Logon	uint32	

EventType: PH_DISCOV_ADS_PASSWORD_NEVER_EXPIRES

Description: Active Directory user password never expires

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	
passwordAge	Password Age	uint32	
passwordLastSet	Password Last Set	Date	

EventType: PH_DISCOV_ADS_PASSWORD_NOT_REQD

Description: Active Directory user password not required

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	

EventType: PH_DISCOV_ADS_PASSWORD_STALE

Description: Active Directory user password stale - more than 90 days

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	
passwordAge	Password Age	uint32	
passwordLastSet	Password Last Set	Date	

EventType: PH_DISCOV_ADS_PASSWORD_TO_EXPIRE

Description: Active Directory user password to expire in 2 weeks

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	

Id	Display name	Type	Description
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	
daysToPasswordExpiry	Days To Password Expiry	uint32	
passwordLastSet	Password Last Set	Date	

EventType: PH_DISCOV_ARUBA_WLAN_HOST_LOCATION

Description: Aruba WLAN AP connected Host Identity and Location

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostMACAddr	Host MAC	string	Host Layer 2 MAC Address in the log
user	User	string	
domain	Domain	string	
nepDevIpAddr	Network Access Device IP	IP	
nepDevName	Network Access Device	string	
nepDevPort	Network Access Device Port	string	
wlanSsid	WLAN SSID	string	WLAN Service Set Identifier (SSID) found in SNMP based WLAN monitoring
wlanChannelId	WLAN Channel Id	uint32	WLAN Channel Id found in SNMP based WLAN monitoring
wlanApAssocUpTime	WLAN AP Association Uptime	uint32	WLAN AP Association Uptime found in SNMP based WLAN monitoring
wlanMaxHostTxmitRate	WLAN Max Host Txmit Rate Mbps	uint32	WLAN Max Host Txmit Rate Mbps found in SNMP based WLAN monitoring
wlanContrIpAddr	WLAN Controller IP	IP	WLAN Controller IP found in SNMP based WLAN monitoring

Id	Display name	Type	Description
wlanContrHostName	WLAN Controller Host Name	string	WLAN Controller Host Name found in SNMP based WLAN monitoring
wlanRssi	WLAN RSSI dB	int32	WLAN RSSI dB found in SNMP based WLAN monitoring
wlanProtocol	WLAN Protocol	string	WLAN Protocol found in SNMP based WLAN monitoring

EventType: PH_DISCOV_AWS_DEVICE_DELETED

Description: FortiSIEM AWS Discovery discovered a terminated device - this device will be deleted from CMDB

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ec2InstanceId	EC2 Instance Id	string	
accountId	Account Id	string	
awsRegion	AWS Region	string	
status	Status	string	

EventType: PH_DISCOV_AWS_DEVICE_UNKNOWN

Description: Discovery module failed to recognize AWS device type

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_AWS_DISCOV_FAILED

Description: Discovery module failed to discover AWS environment

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_AZURE_DISCOV_FAILED

Description: Discovery module failed to discover AZURE environment

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_BASIC_FAILED

Description: Basic discovery completely failed for a device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_BASIC_SKIPPED

Description: Device discovery skipped because of device type discovery exclusion policy

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_BASIC_SNMP_DETAIL

Description: Device discovery via SNMP details

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovSuccessCode	PH Discovery Success Code	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BASIC_SNMP_ERROR

Description: Device discovery encountered errors

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_BASIC_SNMP_FAILED

Description: Basic device discovery via SNMP completely failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_BASIC_SNMP_STARTED

Description: Starting device discovery for a device via SNMP

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BASIC_SNMP_SUCCESS

Description: Device discovery via SNMP succeeded for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BASIC_SSH_DETAIL

Description: Device discovery via SSH details

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovSuccessCode	PH Discovery Success Code	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BASIC_SSH_ERROR

Description: Basic device discovery via SSH encountered errors

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_BASIC_SSH_FAILED

Description: Basic device discovery via SSH completely failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_BASIC_SSH_STARTED

Description: Device discovery via SSH started for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BASIC_SSH_SUCCESS

Description: Device discovery via SSH succeeded for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BASIC_STARTED

Description: Starting device discovery for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BGP_OSPF_FAILED

Description: Failed to send discovery task request for BGP/OSPF change

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_BROCADE_SERVER_IRON_HW_INFO_WARNING

Description: Failed to discover Brocade server iron hardware status

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_CANCEL_UNKNOWN_REQ

Description: Discovery module received discovery cancel request with unknown request ID

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_CERT_FILE_DOWNLOAD_FAILURE

Description: Discovery module failed to download certificate file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_DISCOV_CHECKPOINT_TEST_CONN_FAILED

Description: Discovery module failed to test connectivity for a Checkpoint device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_CISCO_ASA_GET_CONTEXT_FAILED

Description: Discovery module failed to discover Cisco ASA device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
virtContext	Virtualization Context	string	

EventType: PH_DISCOV_CISCO_ASA_IPSEC_VPN_FAILED

Description: Discovery module failed to discover IPSEC VPN for Cisco ASA via SNMP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_ASA_RAS_VPN_FAILED

Description: Discovery module failed to discover RAS VPN for Cisco ASA via SNMP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_ASA_RUN_CONFIG_FAILED

Description: Discovery module failed to discover running config for Cisco ASA via Login

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
virtContext	Virtualization Context	string	

EventType: PH_DISCOV_CISCO_ASA_SET_CONTEXT_FAILED

Description: Discovery module failed to set context for Cisco ASA

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
virtContext	Virtualization Context	string	

EventType: PH_DISCOV_CISCO_ASA_STARTUP_CONFIG_FAILED

Description: Discovery module failed to discover startup config for Cisco ASA via Login

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
virtContext	Virtualization Context	string	

EventType: PH_DISCOV_CISCO_CALL_MANAGER_WARNING

Description: Discovery module failed to obtain Cisco Call Manager statistics

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_CISCO_CATOS_INTF_FAILED

Description: Discovery module failed to find interface by id and name for Cisco CatOS device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.

EventType: PH_DISCOV_CISCO_CDP_ERROR

Description: Discovery module failed to find local interface in CDP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_IOS_L2_WARNING

Description: Discovery module failed to discover Layer 2 for Cisco IOS device - no directly connected host entries

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_IOS_TRUNK_PORT_ERROR

Description: Discovery module encountered SNMP index lookup error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_JUNOS_L2_WARNING

Description: Discovery module failed to discover Layer 2 for JUNOS device - no directly connected host entries

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_NXOS_HW_STATUS_WARNING

Description: Discovery module failed to obtain Cisco NxOS hardware status

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_CISCO_NXOS_INTF_SHORT_NAME_NOT_FOUND

Description: Discovery module failed to find interface short name for Cisco NxOS

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_NXOS_L2_WARNING

Description: Discovery module failed to discover Layer 2 for Cisco NxOS device - no directly connected host entries

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_WLAN_HOST_LOCATION

Description: Cisco WLAN AP connected Host Identity and Location

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
hostMACAddr	Host MAC	string	Host Layer 2 MAC Address in the log
user	User	string	
domain	Domain	string	
nepDevIpAddr	Network Access Device IP	IP	
nepDevName	Network Access Device	string	
nepDevPort	Network Access Device Port	string	
wlanSsid	WLAN SSID	string	WLAN Service Set Identifier (SSID) found in SNMP based WLAN monitoring
wlanContrIpAddr	WLAN Controller IP	IP	WLAN Controller IP found in SNMP based WLAN monitoring
wlanContrHostName	WLAN Controller Host Name	string	WLAN Controller Host Name found in SNMP based WLAN monitoring
wlanRssi	WLAN RSSI dB	int32	WLAN RSSI dB found in SNMP based WLAN monitoring
wlanSnr	WLAN SNR dB	uint32	WLAN SNR dB found in SNMP based WLAN monitoring
wlanProtocol	WLAN Protocol	string	WLAN Protocol found in SNMP based WLAN monitoring

EventType: PH_DISCOV_CLOCK_ROLLS_BACK

Description: FortiSIEM Discovery module discovers excessive clock skew during BGP/OSPF discovery

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_CONTACT_APP_SERVER

Description: Discovery module contacting app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_DISCOV_CREDEN_INSERT_ERROR

Description: Discovery module failed to insert device credential into its memory - discovery may fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_CUSTOM_MAP_LOAD_FAILED

Description: Discovery module failed to load customer map from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_DATA_DOMAIN_HW_STATUS_WARNING

Description: Discovery module failed to obtain hardware status from Data Domain device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_DELL_BLADE_CHASSIS_WARNING

Description: Discovery module failed to discover Dell Blade Chassis

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_DELL_COMPELLENT_STORAGE_WARNING

Description: Discovery module failed to discover volume info for Dell Compellent Storage device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_DISCOV_REQ_GET_FAILED

Description: Discovery module failed to get discovery request from App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_DISCOV_RESULT_SENDER_THREADS_SPAWN_FAILED

Description: Discovery module failed to spawn discovery result sender threads

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_DISCOV_THREADS_SPAWN_FAILED

Description: Discovery module failed to spawn discover threads

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_EC2_INSTANCE_PARSE_FAILED

Description: Discovery module failed to parse EC2 instance xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV EMC_CLARION_ERROR

Description: Discovery module failed to discover EMC Clarion

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV EMC_VNX_DISCOV_FAILED

Description: Discovery module failed to discover EMC VNX via navisec client

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
filePath	File Path	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_EMC_VNX_PING_FAILED

Description: Discovery module failed to ping EMC VNX

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
filePath	File Path	string	

EventType: PH_DISCOV_EQLOGIC_CONN_FAILED

Description: Discovery module failed to obtain EqualLogic connection info

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	

Id	Display name	Type	Description
oid	Object Identifier	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_EQLOGIC_HW_INFO_FAILED

Description: Discovery module failed to obtain EqualLogic metric

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
oid	Object Identifier	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_ESX_HOST_PING_ONLY_DISCOV_ERROR

Description: Ping only discovery for ESX host/vCenter failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_FAILED_INVALID_REQUEST

Description: Discovery failed - invalid discovery request from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_FAILED_INVALID_REQUEST_XML

Description: FortiSIEM discovery module received invalid XML from App Server - discovery will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_FAILED_XML_ERROR

Description: Discovery XML request parse error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_FAIL_CMDB_DEV

Description: Existing CMDB device (re)discovery failed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_FILE_BASED_DISCOV_DIR_NOT_CONFIGURED

Description: File based discovery failed - discover_file_dir missing in phoenix_config.txt

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_FILE_BASED_DISCOV_FAILED

Description: File based discovery failed - cannot open discovery file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
filePath	File Path	string	

EventType: PH_DISCOV_FORTINET_CPU_INFO_WARNING

Description: Discovery module failed to discover cpu info for Fortinet appliance

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_FORTINET_LINK_STAT_WARNING

Description: Discovery module failed to discover link stat for Fortinet appliance

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_FORTINET_SYS_UPDATE_VERSION_WARNING

Description: Discovery module failed to discover system auto update versions for Fortinet appliance

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_GENERIC_ERROR

Description: Device discovery encountered generic errors

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_GEN_WLAN_HOST_LOCATION

Description: Generic WLAN AP connected Host Identity and Location

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostMACAddr	Host MAC	string	Host Layer 2 MAC Address in the log
user	User	string	
domain	Domain	string	
nepDevIpAddr	Network Access Device IP	IP	
nepDevName	Network Access Device	string	
nepDevPort	Network Access Device Port	string	
wlanSsid	WLAN SSID	string	WLAN Service Set Identifier (SSID) found in SNMP based WLAN monitoring
wlanContrIpAddr	WLAN Controller IP	IP	WLAN Controller IP found in SNMP based WLAN monitoring
wlanContrHostName	WLAN Controller Host Name	string	WLAN Controller Host Name found in SNMP based WLAN monitoring

EventType: PH_DISCOV_GET_SNMP_ENGINE_ID_FAILED

Description: Failed to get snmp engine ID

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_HOST_CONVERT_PROCESS_UPTIME_ERROR

Description: Discovery module failed to convert process uptime

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_HOST_ERROR

Description: Discovery module failed to discover device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_HOST_INSTALL_SW_WARNING

Description: Discovery module failed to discover installed software

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_HOST_LOCATE_PROCESS_ERROR

Description: Discovery module failed to locate running process by SNMP id

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_HOST_LOCATION

Description: Wired Host IP location message

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_HOST_NET_INTF

Description: Host network interface identity message

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostMACAddr	Host MAC	string	Host Layer 2 MAC Address in the log
computer	Computer	string	

EventType: PH_DISCOV_HOST_STARTED

Description: Host discovery started for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_HOST_SUCCESS

Description: Host discovery succeeded for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_HOST_SUCCESS_DETAIL

Description: Host discovery success details

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovSuccessCode	PH Discovery Success Code	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_HOST_WARNING

Description: Discovery module failed to discover device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	

EventType: PH_DISCOV_HP3COM_HW_WARNING

Description: Discovery module failed to discover hardware info for HP3Com

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_HP_BLADE_HW_STATUS_WARNING

Description: Discovery module failed to obtain hardware status from HP Blade device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_INIT_MODULE_FAILED

Description: Discovery module failed to initialize

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_INTERFACE_VIA_SNMP_FAILED

Description: Discovery module failed to discover network interfaces vis SNMP

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_ISILON_HW_STATUS_WARNING

Description: Discovery module failed to obtain hardware status from Isilon device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_JMX_TEST_CONN_FAILED

Description: Discovery module failed to test conn for JMX server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_JUNIPER_SSG_HW_INFO_WARNING

Description: Juniper SSG hardware warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_L2_FAILED

Description: Layer 2 device discovery completely failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_L2_STARTED

Description: Layer 2 device discovery started for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_DISCOV_L2_SUCCESS

Description: Layer 2 device discovery succeeded for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_LDAP_ERROR

Description: LDAP discovery failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_LDAP_OU_ERROR

Description: Discovery module failed to lookup LDAP OU in its memory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_LINUX_DSKTABLE_NOT_CONFIG

Description: Linux disk discovery incomplete - Dsktable MIB not configured on Linux server

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	

EventType: PH_DISCOV_LOGIN_ERROR

Description: Discovery / Perf monitoring module failed to execute command via SSH/TELNET

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	
script	Script	string	
command	Command	string	

EventType: PH_DISCOV_NEXT_HOP_VIA_SNMP_FAILED

Description: Discovery module failed to discover next hop address vis SNMP

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_NIMBLE_VOLUME_WARNING

Description: Failed to discover volume for Nimble storage

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_NOZOMI_DISCOV_FAILED

Description: Discovery module failed to discover Nozomi environment

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_PARAM_PARSE_FAILED

Description: Discovery module failed to parse parameters in discovery XML from App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_PARSER_MSG_EXCEEDS_THRESHOLD

Description: Number of parser-to-discover messages to be processed exceeds threshold, discard the oldest one

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_PARSER_MSG_THREAD_SPAWN_FAILED

Description: Discovery module failed to spawn processParserMessage thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_PERF_TEMPLATE_LOAD_FAILED

Description: Discovery module failed to load performance template from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_PING_ONLY_LIST_NOT_MATCH

Description: Discovery module found that ping-only-discover device list does not match include-ip device list. Ping-only-discovery is not effective

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_READ_COMPRESS_THRESHOLD_FAILED

Description: Discovery module failed to read discover_compress_threshold from phoenix configuration, will set it to 2048 bytes

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_RECVD_VALID_REQUEST

Description: Received valid discovery request from app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_RESULT_SEND_FAILED

Description: Discovery module failed to send discovery result to App server after many retries; discovery will fail

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_RESULT_SEND_WARNING

Description: Discovery module failed to upload discovery result to App Server, will retry

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_RESULT_XML_WRITE_FAILURE

Description: Discovery module failed to create discovery result XML file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_RUNNING_SERVICE

Description: Found running service on host

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
appName	Application Name	string	

EventType: PH_DISCOV_RUN_JAVA_PROBE_ERROR

Description: Discovery module failed to execute runJavaProbe.sh

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
exitValue	Command exit value	int32	

EventType: PH_DISCOV_RUN_SW_FILTER_LOAD_FAILED

Description: Discovery module failed to load Running Software Filter from App Server - running software filter may not be discovered correctly

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_RUN_SW_FILTER_PARSE_FAILED

Description: Discovery module failed to parse running software filter xml from App Server - running software filter may not be discovered correctly

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_RUN_VM_TEST_CONN_ERROR

Description: Discovery module failed to execute VMWare Test Connectivity (runVmTestConn.sh)

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
exitValue	Command exit value	int32	

EventType: PH_DISCOV_SKIPPED

Description: Skipping device discovery by discovery request policy

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_SKIP_DEV

Description: Discovery skipped a device for discovery

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

EventType: PH_DISCOV_SNMP_ERROR

Description: Discovery module failed to get data via SNMP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_SSH_ERROR

Description: Discovery module failed to execute command via SSH

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	
script	Script	string	
command	Command	string	

EventType: PH_DISCOV_START

Description: Discovery module starting

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TELNET_ERROR

Description: Discovery module failed to execute command via TELNET

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	
script	Script	string	
command	Command	string	

EventType: PH_DISCOV_TEST_CONN_GET_REQ_FAILED

Description: Discovery module failed to get test connectivity request from App server

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TEST_CONN_MSRPC_ERROR

Description: Discovery module failed to test connection to a Windows Server via MSRPC

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
filePath	File Path	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_TEST_CONN_NO_UCSAPI_CRED

Description: Discovery module failed to test connection to a Cisco UCS Server via UCS API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TEST_CONN_RESULT_SENDER_THREADS_SPAWN_FAILED

Description: Discovery module failed to spawn test connectivity result sender threads

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TEST_CONN_RESULT_SEND_ERROR

Description: Discovery module encountered error in sending Test Connectivity result to app server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_TEST_CONN_RESULT_SEND_WARNING

Description: Discovery module failed to upload test connectivity result to App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TEST_CONN_THREADS_SPAWN_FAILED

Description: Discovery module failed to spawn test connectivity threads

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TEST_CONN_VMSDK_ERROR

Description: Discovery module encountered VMSDK test connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_TRIPP_UPS_HW_STATUS_WARNING

Description: Discovery module failed to obtain hardware status from Tripp UPS device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_TRUNK_PORTS_ERROR

Description: Discovery module failed to get network device trunk port information from App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_UNHANDLED_ACCESS_PROTO

Description: Discovery module encountered unhandled device access method

Severity: 4 (Low)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_UPLOAD_DATA_FAILED

Description: Discovery module failed to upload discovery results to App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_VMWARE_DUP_DEV_ID

Description: Discovery module encountered VMSDK discovery error because of duplicated device id

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
filePath	File Path	string	

EventType: PH_DISCOV_VMWARE_ERROR

Description: Discovery module failed to discover device via VMSDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_VOIP_PHONE_ID

Description: VoIP phone identity message

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
computer	Computer	string	
hostMACAddr	Host MAC	string	Host Layer 2 MAC Address in the log
user	User	string	
domain	Domain	string	
voIPPhoneStatus	VoIP Phone Status	string	

EventType: PH_DISCOV_WMI_PULL_ERROR

Description: Windows WMI pulling error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_APACHE_PING_FAILED

Description: Discovery module failed to ping apache server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_APP_GROUP_FILTER_PARSE_ERROR

Description: Discovery module failed to parse Application Group filter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_APP_GROUP_FILTER_PUSH_ERROR

Description: Discovery module found empty group name in App Group Filter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_AWS_NEW_INSTANCE_NOT_RUN

Description: Discovery module found new AWS instance but it is not running

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_AWS_OBTAIN_INSTANCE_FAILURE

Description: FortiSIEM Discovery failed to obtain AWS instance

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_CHECK_APP_LIST_WARNING

Description: Discovery module failed to checking monitorability for windows servers

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CISCO_IOS_CBQOS_ERROR

Description: Discovery module encountered CBQoS monitoring error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CISCO_MERAKI_GET_CHILD_DEVICE_WARNING

Description: Discovery module failed to get Cisco Meraki child devices

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CISCO_MERAKI_GET_INTFS_WARNING

Description: Discovery module failed to get Cisco Meraki interfaces

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CISCO_MERAKI_GET_INTF_WARNING

Description: Discovery module failed to get Cisco Meraki interface

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.

EventType: PH_LIB_TOPO_CISCO_MERAKI_MAC_2_HOST_LOOKUP_FAILED

Description: Discovery module failed to get prev found Meraki device by MAC in mac-to-host table

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_CISCO_MERAKI_MAC_2_INTF_LOOKUP_FAILED

Description: Discovery module failed to get prev found Meraki device by MAC in mac-to-interface table

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_CISCO_UCS_LOGIN_FAILED

Description: Discovery module failed to login to Cisco UCS

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CISCO_UCS_REQUEST_ERROR

Description: Discovery module failed to send request to Cisco UCS

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_CPU_TOO_HIGH

Description: Discovery / Perf Monitoring module found CPU util for device to be too high

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cpuUtil	CPU Util	double	

EventType: PH_LIB_TOPO_CUST_CONFIG_JOB_DOWNLOAD_SCRIPT_FAILED

Description: Discovery / Perf Monitoring module failed to download expect script from app server for custom config job

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
filePath	File Path	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_CHECK_PATH_ERROR

Description: Discovery / Perf Monitoring module failed to check configured path name for custom FIM job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_DEVICE_UNAVAILABLE

Description: Discovery / Perf Monitoring module found that device is not available for custom FIM job

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
command	Command	string	
exitValue	Command exit value	int32	

EventType: PH_LIB_TOPO_CUST_FIM_JOB_FILE_TOO_LARGE

Description: Discovery / Perf Monitoring FIM module found that file is too large to be pulled

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
filePath	File Path	string	
fileSize64	File Size64 Bytes	uint64	

EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_DATA_FAILED

Description: Discovery / Perf Monitoring failed to get data for custom FIM job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_FILE_INFO_FAILED

Description: Discovery / Perf Monitoring failed to get general file info for FIM job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_MD5_FAILED

Description: Discovery / Perf Monitoring failed to get file MD5 for FIM job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_REMOTE_FILE_ERROR

Description: Discovery / Perf Monitoring failed to get remote file for FIM

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
filePath	File Path	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_INCORRECT_CRED

Description: Discovery / Perf Monitoring found incorrect username or password for custom FIM job

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
command	Command	string	
exitValue	Command exit value	int32	

EventType: PH_LIB_TOPO_CUST_FIM_JOB_RUN_SCP_FAILED

Description: Discovery / Perf Monitoring module failed to runScp.exp for FIM job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_TOO_MANY_FILES

Description: Discovery / Perf Monitoring module found that files count exceeds the max files count limitation under one directory for custom FIM job

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
dirName	Directory Name	string	

EventType: PH_LIB_TOPO_CUST_LOGIN_JOB_CREATE_EVENT_FAILED

Description: Discovery / Perf Monitoring module failed to create event for custom LOGIN job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_LOGIN_JOB_GET_DATA_FAILED

Description: Discovery / Perf Monitoring module failed to get data for custom LOGIN job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_SNMP_JOB_CREATE_EVENT_FAILED

Description: Discovery / Perf Monitoring module failed to create event for custom SNMP job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_SNMP_JOB_GET_DATA_FAILED

Description: Discovery / Perf Monitoring module failed to get data for custom SNMP job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_WMI_JOB_CREATE_EVENT_FAILED

Description: Discovery / Perf Monitoring module failed to create event for custom WMIjob

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_WMI_JOB_GET_DATA_FAILED

Description: Discovery / Perf Monitoring module failed to get data for custom WMI job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_ETHERMIB_STAT_LOOKUP_ERROR

Description: Discovery / Perf Monitoring module failed to get ethermib stat for interface

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
srcSnmplntfIndex	Source Interface SNMP Index	uint16	SNMP index of the network interface through which a packet enters a network device. This information is typically present in Firewall logs.

EventType: PH_LIB_TOPO_EVENT_DROP_RULE_ENCODE_VALUE_GROUP_ERROR

Description: Discovery / Perf Monitoring module failed to encode value group

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_EVENT_DROP_RULE_PARSE_ERROR

Description: Parser module failed to parse event dropping rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_EXCLUDED_DISK_PARSE_ERROR

Description: Discovery / Perf Monitoring module failed to parse excluded disks

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_FCT_DEV_MAPPING_ENTRY_INVALID

Description: FortiClient device type mapping in /opt/phoenix/data-definition/FortiClientOSVersionMap.csv is invalid.

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_FGT_FABRIC_DISCOV_FAIL

Description: FortiGate Fabric Discovery Failure, if security fabric not enabled, this may be normal

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_FGT_GET_CONFIG_BACKUP_FAILED

Description: Failed to get config backup for FortiGate. Ensure that the FortiGate's rest api user role allows WRITE for System -> Administrator Users access permissions.

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_FGT_GET_USER_DEV_STORE_FAIL

Description: FortiGate User Device Store record retrieval failed. This is optional data

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_FGT_GET_USER_DEV_UNKNOWN

Description: FortiGate User Device Store identified an unknown device type. Add mapping to /opt/phoenix/data-definition/FortiClientOSVersionMap.csv

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_FGT_INSTALLED_SW_FAIL

Description: FortiGate failed to collect software module status via /api/v2/monitor/license/status.

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_FGT_SEC_POSTURE_RPT_API_FAIL

Description: FortiGate security posture report could not be retrieved via API on root fabric firewall.

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_FILE_READ_ERROR

Description: Discovery / Perf Monitoring module failed to read file

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_LIB_TOPO_FOUNDRY_HW_STATUS_ERROR

Description: Discovery / Perf Monitoring module failed to get hardware status for Foundry Iron device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oid	Object Identifier	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_GEN_UPS_STATUS_GET_ERROR

Description: Discovery / Perf Monitoring module failed to get hardware status via SNMP for GEN UPS device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_GET_NETAPP_NFS_FAILED

Description: Discovery / Perf Monitoring module failed to get NFS metrics via SNMP or ONTAP SDK for NetApp Filer

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_H3C_CPU_UTIL_ERROR

Description: Discovery / Perf Monitoring module failed to get CPU Util of H3C via SNMP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oid	Object Identifier	string	

EventType: PH_LIB_TOPO_HP3COM_CPU_UTIL_ERROR

Description: Discovery / Perf Monitoring module failed to get CPU Util of Hp3Com via SNMP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oid	Object Identifier	string	

EventType: PH_LIB_TOPO_HP3COM_MEM_UTIL_ERROR

Description: Discovery / Perf Monitoring module failed to get CPU Util of Hp3Com device via SNMP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oid	Object Identifier	string	

EventType: PH_LIB_TOPO_HPUX_PROC_CPU_MEM_TOO_HIGH

Description: Discovery / Perf Monitoring module found HPUX Process CPU Util or Mem Util too high

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
procName	Process Name	string	
cpuUtil	CPU Util	double	
memUtil	Memory Util	double	

EventType: PH_LIB_TOPO_HYPERV_METRICS_GET_ERROR

Description: Discovery / Perf Monitoring module failed to get HyperV metrics

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_IMPORTANT_INTF_PARSE_ERROR

Description: Discovery / Perf Monitoring module failed to parse important interfaces

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_INTF_UTIL_ERROR

Description: Discovery / Perf Monitoring module found interface util monitoring data inconsistency

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.

EventType: PH_LIB_TOPO_JSON_PARSE_FAILED

Description: Failed to parse JSON

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_JUNIPER_INTF_SPEED_GET_ERROR

Description: Discovery / Perf Monitoring module failed to get interface speed from Juniper firewall

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.

EventType: PH_LIB_TOPO_LIEBERT_HVAC_STATUS_GET_ERROR

Description: Discovery / Perf Monitoring module failed to get hardware status via SNMP for LIEBERT HAVC device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_LOGIN_PING_FAILED

Description: Discovery / Perf Monitoring module failed to execute a login command for discovery purposes

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
ipPort	IP Port	uint16	IP port number
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_MAINTENANCE_DURATION_INCORRECT

Description: Perf Monitoring module failed to properly parse device maintenance duration from App Server

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	

EventType: PH_LIB_TOPO_MEM_TOO_HIGH

Description: Discovery / Perf Monitoring module memory util for device to be too high

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
memUtil	Memory Util	double	

EventType: PH_LIB_TOPO_NETAPP_AGGREGATE_STAT_ERROR

Description: Discovery / Perf Monitoring module failed to get NetApp Aggregate Stat via ONTAP SDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NETAPP_ANALYZE_VERSION_ERROR

Description: Discovery / Perf Monitoring module failed to analyze NetApp version via ONTAP SDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NETAPP_DISK_STAT_ERROR

Description: Discovery / Perf Monitoring module failed to get NetApp Disk Stat via ONTAP SDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NETAPP_GET_NFS_METRIC_ERROR

Description: Discovery / Perf Monitoring module failed to obtain NetApp NFS V3 metrics via ONTAPI

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NETAPP_GET_VERSION_ERROR

Description: Discovery / Perf Monitoring module failed to get NetApp version -- volume latencies may not be correct

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_NETAPP_LUN_STAT_ERROR

Description: Discovery / Perf Monitoring module failed to get NetApp LUN Stat via ONTAP SDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NETAPP_PROTO_STAT_ERROR

Description: Discovery / Perf Monitoring module failed to get NetApp Protocol Stat via ONTAP SDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NETAPP_VOLUME_STAT_ERROR

Description: Discovery / Perf Monitoring module failed to get NetApp Volume Stat via ONTAP SDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NOT_SUPPORT_REST_API

Description: Rest API doesn't support in this fortigate version

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_OPEN_FILE_FAILED

Description: Unable to open file

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
details	Details	string	

EventType: PH_LIB_TOPO_PARSE_INTF_MAP_FAILURE

Description: Discovery / Perf Monitoring module failed to parse device interface map

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_PERF_JOB_EXEC_FAILED

Description: Perf Monitoring module failed to execute a specific performance monitoring job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
jobId	Job Id	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_PERF_JOB_INIT_FAILED

Description: Perf Monitoring module failed to initialize the performance monitoring job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_PERF_JOB_REMOVE_FAILED

Description: Perf Monitoring module failed to remove performance monitoring job by JOB ID

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobId	Job Id	string	

EventType: PH_LIB_TOPO_PERF_TEMPLATE_LOAD_ERROR

Description: Perf Monitoring module failed to load performance monitor template xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_PERF_TEMPLATE_PARSE_FAILURE

Description: Perf Monitoring module failed to parse performance monitor template xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_PERF_TEMPLATE_PARSE_WARNING

Description: Perf Monitoring module skipped one device type while loading Performance Monitor template xml

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_PORT_FILTER_PARSE_ERROR

Description: Perf Monitoring module failed to parse port filter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_PORT_FILTER_PUSH_ERROR

Description: Perf Monitoring module found empty protocol name in Port Filter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_PROC_CPU_MEM_TOO_HIGH

Description: Perf Monitoring module found process CPU Util or Mem Util to be too high

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
procName	Process Name	string	
cpuUtil	CPU Util	double	
memUtil	Memory Util	double	

EventType: PH_LIB_TOPO_REST_API_FAILED

Description: Failed to call a REST API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_RUN_SW_FILTER_PARSE_ERROR

Description: Discovery / Perf Monitoring module found failed to parse running software filter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_RUN_SW_FILTER_PUSH_ERROR

Description: Discovery / Perf Monitoring module found empty name and path in running software Filter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_SNMPWALK_ERROR

Description: Discovery / Perf Monitoring module found found empty or incomplete snmpwalk response

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
oid	Object Identifier	string	

EventType: PH_LIB_TOPO_STM_JOB_EXEC_FAILED

Description: Discovery / Perf Monitoring module failed to execute STM job for device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	

EventType: PH_LIB_TOPO_STM_JOB_INIT_FAILED

Description: Perf Monitoring module failed to initialize the STM job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_TEST_CONN_HTTP_AGENT_FAILED

Description: Discovery module failed to test connectivity for http java agent

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LIB_TOPO_TEST_CONN_JDBC_AGENT_FAILED

Description: Discovery module failed to test connectivity for jdbc java agent

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LIB_TOPO_TEST_CONN_JMX_AGENT_FAILED

Description: Discovery module failed to test connectivity for jmx java agent

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LIB_TOPO_TRUNK_PORT_MAP_PARSE_ERROR

Description: Discovery module failed to parse trunk port map

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_VALIDATE_ACCESS_FAILED

Description: Perf Monitor module found device credential issues during initialization

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_DATABASE_INSTANCE_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange Database instance metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_DATABASE_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange Database metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_MAIL_SUBMISSION_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange mail submission metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_PUB_MAILBOX_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange public mailbox metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_REG_MAILBOX_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange regular mailbox metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_REPLICATION_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange replication metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_RPC_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange RPC metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_SMTP_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange SMTP metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_STORE_INTF_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange store interface metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_TRANSPORT_QUEUE_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange transport queue metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WMI_GET_CPU_COUNT_ERROR

Description: Discovery/Perf Monitor module failed to get Windows CPU count via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WMI_GET_CPU_WARNING

Description: Discovery/Perf Monitor module failed to get CPU info for Windows device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WMI_GET_PAGE_ACTIVITY_ERROR

Description: Discovery/Perf Monitor module failed to get Windows paging activity via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WMI_GET_REAL_MEM_ERROR

Description: Discovery/Perf Monitor module failed to get Windows real memory via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WMI_GET_RUN_SW_PERF_ERROR

Description: Discovery/Perf Monitor module failed to get Windows running software performance via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MAX_DEVICES_EXCEEDED

Description: Max number of devices exceeded license

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_MAX_DEVICES_LIMIT_REACHED

Description: Max number of devices exceeded license

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_TEST_CONN_COMPLETE

Description: Test Connectivity completed

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_TEST_CONN_CONTACT_APP_SERVER

Description: Test Connectivity module contacting app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_TEST_CONN_FAILED

Description: Test Connectivity failed

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_TEST_CONN_FAILED_INVALID_REQUEST

Description: Test Connectivity failed - invalid discovery request from App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_TEST_CONN_FAILED_INVALID_REQUEST_XML

Description: Test Connectivity failed - invalid discovery request XML from App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_TEST_CONN_RECVD_VALID_REQUEST

Description: Received valid test connectivity request from app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_TEST_CONN_RESULT_SENT

Description: Test Connectivity results sent to app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_TEST_CONN_STARTED

Description: Starting test connectivity for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

Event Collection and Forwarding Logs

This section provides logs related to event collection and forwarding via syslog, WMI/OMI and other collection methods

- PH_AGENTMGR_ACI_ATTR_NOT_FOUND
- PH_AGENTMGR_ACI_CURL_HANDLE_GET_FAILED
- PH_AGENTMGR_ACI_FILE_WRITE_ERROR
- PH_AGENTMGR_ACI_JSON_PARSE_FAILED
- PH_AGENTMGR_ACI_SERVER_EMPTY
- PH_AGENTMGR_ACI_TOKEN_GET_FAILED
- PH_AGENTMGR_ALERTLOGIC_CURL_HANDLE_GET_FAILED
- PH_AGENTMGR_ALERTLOGIC_FILE_LOAD_ERROR
- PH_AGENTMGR_ALERTLOGIC_FILE_READ_ERROR
- PH_AGENTMGR_ALERTLOGIC_FILE_WRITE_ERROR
- PH_AGENTMGR_ALERTLOGIC_INVALID_DATA
- PH_AGENTMGR_ALERTLOGIC_INVALID_PATH
- PH_AGENTMGR_ALERTLOGIC_QUERY_INTERVAL_TOO_LONG
- PH_AGENTMGR_ALERTLOGIC_SERVER_EMPTY
- PH_AGENTMGR_AMPCLOUD_CURL_CONNECT_FAILED
- PH_AGENTMGR_AMPCLOUD_CURL_HANDLE_GET_FAILED
- PH_AGENTMGR_AMPCLOUD_FILE_LOAD_ERROR
- PH_AGENTMGR_AMPCLOUD_FILE_READ_ERROR
- PH_AGENTMGR_AMPCLOUD_INVALID_DATA
- PH_AGENTMGR_AMPCLOUD_JSON_PARSE_FAILED
- PH_AGENTMGR_AMPCLOUD_NO_DEFINE_SEVERITY
- PH_AGENTMGR_AMPCLOUD_SERVER_EMPTY
- PH_AGENTMGR_API_PERMISSION_MISSING
- PH_AGENTMGR_AWSCLOUDWATCH_GETLOGS
- PH_AGENTMGR_AWSFLOWLOG_EVENT_PULL_FAILED
- PH_AGENTMGR_AWSFLOWLOG_FILE_WRITE_ERROR
- PH_AGENTMGR_AWSFLOWLOG_LOG_FORMAT_WRONG
- PH_AGENTMGR_AWSKINESIS_CONSUMER_START_FAILED
- PH_AGENTMGR_AWS_CACHE_FILE_ERROR
- PH_AGENTMGR_AWS_DELETE_OJECTKEY_FAILED
- PH_AGENTMGR_AWS_DOWNLOAD_OJECT_FAILED
- PH_AGENTMGR_AWS_EVT_DOWNLOAD_FAILED
- PH_AGENTMGR_AWS_EVT_SEND_FAILED
- PH_AGENTMGR_AWS_GET_OJECTKEY_FAILED
- PH_AGENTMGR_AWS_GZ_FILE_OPEN_ERROR
- PH_AGENTMGR_AWS_JSON_PARSE_FAILED

- PH_AGENTMGR_AWS_SQSURL_FORMAT_ERROR
- PH_AGENTMGR_BOX_API_CALL_FAILED
- PH_AGENTMGR_BOX_ATTR_NOT_FOUND
- PH_AGENTMGR_BOX_EVENT_PULL_FAILED
- PH_AGENTMGR_BOX_FILE_ID_EMPTY
- PH_AGENTMGR_BOX_FILE_LIMIT_EXCEED
- PH_AGENTMGR_BOX_FILE_NOT_MONITORED_ERROR
- PH_AGENTMGR_BOX_FILE_PATH_PARSE_FAILED
- PH_AGENTMGR_BOX_FILE_TYPE_WRONG
- PH_AGENTMGR_BOX_FOLDER_TYPE_WRONG
- PH_AGENTMGR_BOX_HTTP_NO_RESPONSE
- PH_AGENTMGR_BOX_JSON_PARSE_FAILED
- PH_AGENTMGR_BOX_RESPONSE_NO_SPECIAL_ATTRIBUTE
- PH_AGENTMGR_BOX_TIME_CONVERT_FAILED
- PH_AGENTMGR_BOX_XML_PARSE_FAILED
- PH_AGENTMGR_CISCOAMP_CONSUMER_START_FAILED
- PH_AGENTMGR_CLOUDPASSAGE_API_CALL_FAILED
- PH_AGENTMGR_CLOUDPASSAGE_FILE_WRITE_ERROR
- PH_AGENTMGR_CLOUDPASSAGE_GET_EVENT_FAILED
- PH_AGENTMGR_CLOUDPASSAGE_JSON_EMPTY
- PH_AGENTMGR_CLOUDPASSAGE_JSON_PARSE_FAILED
- PH_AGENTMGR_CLOUDPASSAGE_TOKEN_EMPTY
- PH_AGENTMGR_CLOUDTRAIL_FILE_READ_FAILED
- PH_AGENTMGR_CONFIG_ERROR
- PH_AGENTMGR_CONFIG_VERSION_SEND_FAILED
- PH_AGENTMGR_CONFIG_WARNING
- PH_AGENTMGR_CREDENTIAL_GET_FAILED
- PH_AGENTMGR_CROWDSTRIKE_GET_DATAFEED_URL_FAILED
- PH_AGENTMGR_CUST_RESULT_UPLOAD_FAILED
- PH_AGENTMGR_DIR_CREATE_FAILED
- PH_AGENTMGR_EVENT_PULL_FAILED
- PH_AGENTMGR_FALCONDATAREP_SCRIPT_FAILED
- PH_AGENTMGR_FILE_PARSE_ERROR
- PH_AGENTMGR_FILE_WRITE_ERROR
- PH_AGENTMGR_FIREAMP_CERT_DOWNLOAD_FAILED
- PH_AGENTMGR_FIREAMP_DATA_FORMAT_SET_FAILED
- PH_AGENTMGR_FIREAMP_EVENT_PULL_FAILED
- PH_AGENTMGR_FIREAMP_EVT_TYPE_LOAD_FAILED
- PH_AGENTMGR_FIREAMP_FILE_LOAD_ERROR
- PH_AGENTMGR_FIREAMP_FILE_OPEN_ERROR
- PH_AGENTMGR_FIREAMP_INVALID_DATA
- PH_AGENTMGR_FIREAMP_NEW_AGENT_FAILED
- PH_AGENTMGR_FIREAMP_NO_ATTR

- PH_AGENTMGR_FIREAMP_NO_PROTOCOL
- PH_AGENTMGR_FORTICASB_GET_SERVICE_ALERT_ERROR
- PH_AGENTMGR_FORTICASB_GET_SERVICE_ERROR
- PH_AGENTMGR_FORTINDR_GET_API_CALL_FAILED
- PH_AGENTMGR_FORTINDR_GET_API_CALL_NEXT_PAGE
- PH_AGENTMGR_FORTINDR_GET_API_CALL_NO_RESULTS
- PH_AGENTMGR_FORTINDR_GET_API_CALL_RESULTS
- PH_AGENTMGR_FORTINDR_GET_BUCKET_KEY
- PH_AGENTMGR_FORTINDR_GET_BUCKET_OBJ
- PH_AGENTMGR_GET_SCAN_RESULTS_FAILED
- PH_AGENTMGR_GITHUB_API_CALL_FAILED
- PH_AGENTMGR_GITHUB_CREDENTIAL_GET_FAILED
- PH_AGENTMGR_GITHUB_EVENT_PULL_FAILED
- PH_AGENTMGR_GITHUB_FILE_OPEN_ERROR
- PH_AGENTMGR_GITHUB_JSON_PARSE_FAILED
- PH_AGENTMGR_GITHUB_TIME_CONVERT_FAILED
- PH_AGENTMGR_GIT_CLONE_REPO_FAILED
- PH_AGENTMGR_GIT_HANDLE_ERR_FILE_FAILED
- PH_AGENTMGR_GIT_PULL_EVT_FAILED
- PH_AGENTMGR_GIT_SAVE_COMMITID_FAILED
- PH_AGENTMGR_GZ_FILE_OPEN_ERROR
- PH_AGENTMGR_INIT_AGENT
- PH_AGENTMGR_INIT_CACHE_FILE_FAILED
- PH_AGENTMGR_INIT_NO_CRED
- PH_AGENTMGR_INVALID_MGR
- PH_AGENTMGR_IPS_AUTH_FAILED
- PH_AGENTMGR_IPS_EVENT_PULL_FAILED
- PH_AGENTMGR_IPS_FILE_OPEN_ERROR
- PH_AGENTMGR_IPS_OBTAIN_SUBSCRIPTION_FAILED
- PH_AGENTMGR_IPS_SET_SSL_FAILED
- PH_AGENTMGR_JAVA_AGENT_PIPE_WRITE_FAILED
- PH_AGENTMGR_JAVA_AGENT_START_FAILED
- PH_AGENTMGR_JAVA_AGENT_TYPE_UNKNOWN
- PH_AGENTMGR_JAVA_AGENT_USER_MISSING
- PH_AGENTMGR_JAVA_AGENT_ZOMBIE
- PH_AGENTMGR_JAVA_CMD_SEND_FAILED
- PH_AGENTMGR_JAVA_FORK_FAILED
- PH_AGENTMGR_JAVA_INCOMPLETE_DEV_INFO
- PH_AGENTMGR_JAVA_NO_DEV_TYPE_FOR_JDBC
- PH_AGENTMGR_JAVA_NO_STATUS_FILE
- PH_AGENTMGR_JAVA_PIPE_FAILED
- PH_AGENTMGR_JAVA_PROCESS_STATE_GET_FAILED
- PH_AGENTMGR_JAVA_SIGKILL_SEND_FAILED

- PH_AGENTMGR_JAVA_UNSUPPORT_DEV_TYPE_FOR_JDBC
- PH_AGENTMGR_JAVA_USER_PWD_GET_FAILED
- PH_AGENTMGR_JSON_PARSE_FAILED
- PH_AGENTMGR_KAFKA_CONSUME_LOG_FAILED
- PH_AGENTMGR_KAFKA_CREATE_CONSUMER
- PH_AGENTMGR_KAFKA_CREATE_CONSUMER_FAILED
- PH_AGENTMGR_KAFKA_CREATE_PRODUCER_FAILED
- PH_AGENTMGR_KAFKA_CREATE_TOPIC_FAILED
- PH_AGENTMGR_KAFKA_ERROR
- PH_AGENTMGR_KAFKA_METADATA_FAILED
- PH_AGENTMGR_KAFKA_PRODUCER_ERROR
- PH_AGENTMGR_KAFKA_PULL_JOB_FAILED
- PH_AGENTMGR_KAFKA_REBALANCE
- PH_AGENTMGR_KAFKA_RELEASE_CONSUMER
- PH_AGENTMGR_KAFKA_START_FAILED
- PH_AGENTMGR_KAFKA_SUBSCRIBE_FAILED
- PH_AGENTMGR_KAFKA_UPDATE_CONFIG_FAILED
- PH_AGENTMGR_KAFKA_UPDATE_ERROR
- PH_AGENTMGR_KILL_PROCESS
- PH_AGENTMGR_MSAZURE_CONFIG_ARM_FAILED
- PH_AGENTMGR_MSAZURE_DOWNLOAD_FAILED
- PH_AGENTMGR_MSAZURE_JSON_EMPTY
- PH_AGENTMGR_MSAZURE_JSON_FILE_NAME_EMPTY
- PH_AGENTMGR_MSAZURE_JSON_FILE_PARSE_FAILED
- PH_AGENTMGR_MSAZURE_JSON_PARSE_FAILED
- PH_AGENTMGR_MSAZURE_LOGIN_FAILED
- PH_AGENTMGR_MSG_QUEUE_ACCESS_FAILED
- PH_AGENTMGR_MSG_RECV_FAILED
- PH_AGENTMGR_OCI_SET_INSTANCE_NAME_FAILED
- PH_AGENTMGR_OFFICE365_API_CALL_FAILED
- PH_AGENTMGR_OFFICE365_EVENT_PULL_FAILED
- PH_AGENTMGR_OFFICE365_FILE_WRITE_ERROR
- PH_AGENTMGR_OFFICE365_GET_SUBSCRIBE_FAILED
- PH_AGENTMGR_OFFICE365_JSON_PARSE_FAILED
- PH_AGENTMGR_OFFICE365_START_SUBSCRIBE_FAILED
- PH_AGENTMGR_OFFICE365_SUBSCRIBE_EMPTY
- PH_AGENTMGR_OFFICE365_SUBSCRIBE_FAILED
- PH_AGENTMGR_OFFICE365_TOKEN_EMPTY
- PH_AGENTMGR_OKTA_EVT_DOWNLOAD_FAILED
- PH_AGENTMGR_OKTA_FILE_WRONG
- PH_AGENTMGR_OKTA_NO_USER_INFO
- PH_AGENTMGR_OKTA_RESULT_UPLOAD_FAILED
- PH_AGENTMGR_OKTA_RESULT_UPLOAD_WARNING

- PH_AGENTMGR_PARSER_UNABLE_CONNECT
- PH_AGENTMGR_PERF_OBJ_PARSE_FAILURE
- PH_AGENTMGR_PROCESS_INIT_FAILED
- PH_AGENTMGR_PULLING_JOB_OUTDATE
- PH_AGENTMGR_REMOVE_FILE_FAILED
- PH_AGENTMGR_REST_API_CALL_FAILED
- PH_AGENTMGR_RSAS_XML_PARSE_FAILED
- PH_AGENTMGR_RUN_CMD_FAILED
- PH_AGENTMGR_RUN_SCRIPT_FAILED
- PH_AGENTMGR_RUN_SCRIPT_WITHOUT_TASK_ID
- PH_AGENTMGR_SALESFORCE_ATTR_NOT_FOUND
- PH_AGENTMGR_SALESFORCE_COLUMN_NOT_FOUND
- PH_AGENTMGR_SALESFORCE_CURL_EXECUTE_FAILED
- PH_AGENTMGR_SALESFORCE_CURL_HANDLE_GET_FAILED
- PH_AGENTMGR_SALESFORCE_FILE_LOAD_ERROR
- PH_AGENTMGR_SALESFORCE_FILE_WRITE_ERROR
- PH_AGENTMGR_SALESFORCE_INVALID_DATA
- PH_AGENTMGR_SALESFORCE_INVALID_LOG_FILE
- PH_AGENTMGR_SALESFORCE_JSON_PARSE_FAILED
- PH_AGENTMGR_SALESFORCE_LOGIN_FAILED
- PH_AGENTMGR_SALESFORCE_SERVER_EMPTY
- PH_AGENTMGR_SALESFORCE_TOKEN_GET_FAILED
- PH_AGENTMGR_SALESFORCE_TOKEN_REGET_FAILED
- PH_AGENTMGR_SALESFORCE_VERSION_PATH_EMPTY
- PH_AGENTMGR_SALESFORCE_XML_PARSE_FAILED
- PH_AGENTMGR_SCRIPT_NOTIFICATION_SPAWN_FAILED
- PH_AGENTMGR_SERVER_HOST_NAME_RESOLVE_FAILED
- PH_AGENTMGR_SERVER_HOST_NAME_RESOLVE_WARNING
- PH_AGENTMGR_SERVER_IP_RESOLVE_FAILED
- PH_AGENTMGR_SERVER_IP_RESOLVE_WARNING
- PH_AGENTMGR_SETUP_STREAM_FAILED
- PH_AGENTMGR_START_THREAD_FAILED
- PH_AGENTMGR_STATUS_REPORT_FAILED
- PH_AGENTMGR_STATUS_REPORT_INIT_FAILED
- PH_AGENTMGR_STOP_STREAM_FAILED
- PH_AGENTMGR_TENABLE_EXPORT_SCAN_FAILED
- PH_AGENTMGR_TENABLE_GET_DOWNLOAD_FAILED
- PH_AGENTMGR_TENABLE_GET_SCANS_FAILED
- PH_AGENTMGR_TENABLE_GET_STATUS_FAILED
- PH_AGENTMGR_TENABLE_PULL_FAILED
- PH_AGENTMGR_TIME_CONVERSION_FAILED
- PH_AGENTMGR_TIME_STR_FORMAT_INVALID
- PH_AGENTMGR_TOKEN_GET_FAILED

- PH_AGENTMGR_UNPACK_FILE_FAILED
- PH_AGENTMGR_UPDATE_AGENT
- PH_AGENTMGR_UPDATE_BOOKMARK_FAILED
- PH_AGENTMGR_UPDATE_WEBHOOK_CRED_FAILED
- PH_AGENTMGR_UPDATE_WEBHOOK_CRED_SUCCESS
- PH_AGENTMGR_WINDEFATP_API_CALL_FAILED
- PH_AGENTMGR_WINDEFATP_FILE_WRITE_ERROR
- PH_AGENTMGR_WINDEFATP_GET_ALERT_FAILED
- PH_AGENTMGR_WINDEFATP_JSON_EMPTY
- PH_AGENTMGR_WINDEFATP_JSON_PARSE_FAILED
- PH_AGENTMGR_WINDEFATP_TOKEN_EMPTY
- PH_AGENTMGR_WMI_EVENT_PULL_ERROR
- PH_AGENTMGR_WMI_EVENT_PULL_WARNING
- PH_AGENTMGR_WMI_FILE_OPEN_ERROR
- PH_AGENTMGR_WMI_LOG_PULL_ERROR
- PH_AGENTMGR_WMI_MISSING_LOG
- PH_AGENTMGR_WMI_STATUS_REPORT_FAILED
- PH_AGENTMGR_WMI_USER_PWD_GET_FAILED
- PH_AGENTMGR_WVSS_XML_PARSE_FAILED
- PH_AGENTMGR_XML_PARSE_FAILED
- PH_BAD_NETFLOW_PACKET
- PH_BAD_NETFLOW_VER
- PH_CHECKPOINT_CERTHANDLER_ERROR
- PH_CHECKPOINT_CERTPULL_ERROR
- PH_CHECKPOINT_CMD_USAGE_ERROR
- PH_CHECKPOINT_CPMI_FETCH_ERROR
- PH_CHECKPOINT_DEV_INIT_ERROR
- PH_CHECKPOINT_FILE_RENAME_FAILURE
- PH_CHECKPOINT_FWLOGHANDLER_ERROR
- PH_CHECKPOINT_FWLOGHANDLER_INIT_ERROR
- PH_CHECKPOINT_HTTP_ERROR
- PH_CHECKPOINT_LOGHANDLER_ERROR
- PH_CHECKPOINT_PROCESS_GET_FAILED
- PH_CHECKPOINT_TESTCONN_ERROR
- PH_CHECKPOINT_UNABLE_PARSE_XML
- PH_COLLECTOR_CLOCK_SKEW
- PH_COLLECTOR_DOWN
- PH_COLLECTOR_EVENT_ARRIVAL_DELAYED
- PH_COLLECTOR_EVENT_ARRIVAL_OK
- PH_COLLECTOR_EVENT_STORE_DELAYED
- PH_COLLECTOR_EVENT_STORE_OK
- PH_COLLECTOR_UP
- PH_CYBERARK_INIT_ERROR

- PH_DEV_FAIL_TO_PULL_EVENTS
- PH_EVENT_FORWARDER_CHECKSUM_MISMATCH
- PH_EVENT_FORWARDER_CONNECT_ERROR
- PH_EVENT_FORWARDER_DIR_OPEN_FAILURE
- PH_EVENT_FORWARDER_FILE_OPEN_FAILURE
- PH_EVENT_FORWARDER_FILE_RENAME_FAILURE
- PH_EVENT_FORWARDER_INIT_FAILURE
- PH_EVENT_FORWARDER_INVALID_GZIP_FILE
- PH_EVENT_FORWARDER_INVALID_PHOENIX_CONFIG
- PH_EVENT_FORWARDER_INVALID_PROTOCOL
- PH_EVENT_FORWARDER_KAFKA_ERROR
- PH_EVENT_FORWARDER_KAFKA_INIT_FAILURE
- PH_EVENT_FORWARDER_KAFKA_PRODUCE_ERROR
- PH_EVENT_FORWARDER_MKDIR_FAILURE
- PH_EVENT_FORWARDER_RUN_PROCESS_ERROR
- PH_EVENT_FORWARDER_SOCKET_ERROR
- PH_EVENT_FORWARDER_SOCKET_WRITE_ERROR
- PH_EVENT_FORWARDER_SSL_CERT_ERROR
- PH_EVENT_FORWARDER_SSL_ERROR
- PH_EVENT_FWD_CERT_LOAD_FAILED
- PH_EVENT_FWD_CERT_UNPAIRED
- PH_EVENT_FWD_DIR_MAKE_FAILED
- PH_EVENT_FWD_DIR_OPEN_FAILED
- PH_EVENT_FWD_FILE_RENAME_FAILED
- PH_EVENT_FWD_FULL_FORWARDING_FAILED
- PH_EVENT_FWD_GET_FILE_NUM_FAILURE
- PH_EVENT_FWD_GZ_CLOSE_ERROR
- PH_EVENT_FWD_GZ_FILE_OPEN_ERROR
- PH_EVENT_FWD_GZ_MD5_ERROR
- PH_EVENT_FWD_GZ_RENAME_ERROR
- PH_EVENT_FWD_GZ_SIZE_MISMATCH
- PH_EVENT_FWD_KAFKA_WARNING
- PH_EVENT_FWD_MD5_CHECKSUM_MISMATCH
- PH_EVENT_FWD_NETFLOW_REGEX_IGNORED
- PH_EVENT_FWD_PARTIAL_FORWARDING_FAILED
- PH_EVENT_FWD_PARTIAL_FORWARDING_WARNING
- PH_EVENT_FWD_PCRE_ERROR
- PH_EVENT_FWD_PROCESS_INIT_FAILED
- PH_EVENT_FWD_PROCESS_START_FAILED
- PH_EVENT_FWD_PROTO_FORWARDED_WRONG
- PH_EVENT_FWD_RENAME_GZ_ERROR
- PH_EVENT_FWD_RULE_PARSE_ERROR
- PH_EVENT_FWD_SOCKET_CONNECT_FAILED

- PH_EVENT_FWD_SOCKET_GET_FAILED
- PH_EVENT_FWD_SOCKET_WRITE_FAILED
- PH_EVENT_FWD_SSL_CREATE_FAILED
- PH_EVENT_FWD_SSL_SESSION_BUILD_FAILED
- PH_EVENT_FWD_UNEXPECTED_FILE_REMOVED
- PH_EVENT_PKG_ATTR_NOT_FOUND
- PH_EVENT_PKG_EMPTY_FILE_REMOVED
- PH_EVENT_PKG_FILE_ADD_TO_SVN_FAILED
- PH_EVENT_PKG_FILE_REMOVED_ERROR
- PH_EVENT_PKG_FILE_RENAME_FAILED
- PH_EVENT_PKG_FILE_STAT_FAILED
- PH_EVENT_PKG_FILE_UPLOAD_FAILED
- PH_EVENT_PKG_FILE_UPLOAD_SUCCESS_HIGH
- PH_EVENT_PKG_FILE_UPLOAD_SUCCESS_LOW
- PH_EVENT_PKG_GZ_CLOSE_FAILED
- PH_EVENT_PKG_GZ_FILE_OPEN_ERROR
- PH_EVENT_PKG_HTTP_FAILED
- PH_EVENT_PKG_HTTP_INIT_FAILED
- PH_EVENT_PKG_INSERT_TASK_FAILED
- PH_EVENT_PKG_NO_EVENT
- PH_EVENT_PKG_OPEN_DIR_FAILED
- PH_EVENT_PKG_PROCESS_INIT_FAILED
- PH_EVENT_PKG_PROCESS_START_FAILED
- PH_EVENT_PKG_QUEUE_GET_FAILED
- PH_EVENT_PKG_SERVER_LIST_UPLOAD_FAILED
- PH_EVENT_PKG_SERVICE_LIST_EMPTY
- PH_EVENT_PKG_TASK_ADD_TO_QUEUE_FAILED
- PH_EVENT_PKG_XML_PARSE_FAILED
- PH_EVTPKGGER_FILE_UPLOAD_FAILED
- PH_EVT_HANDLER_DBG
- PH_EVT_HANDLER_ERR
- PH_EVT_HANDLER_EVT_QUEUE_LARGE
- PH_EVT_HANDLER_EVT_QUEUE_WARNING
- PH_EVT_HANDLER_INFO
- PH_EVT_HANDLER_SVN_QUEUE_LARGE
- PH_EVT_HANDLER_SVN_QUEUE_WARNING
- PH_EVT_PACKAGER_COND_WAIT_ERROR
- PH_EVT_PACKAGER_FILE_CLOSE_FAILURE
- PH_EVT_PACKAGER_FILE_OPEN_FAILURE
- PH_EVT_PACKAGER_FILE_REMOVE_FAILURE
- PH_EVT_PACKAGER_FILE_RENAME_FAILURE
- PH_EVT_PACKAGER_FILE_STAT_FAILURE
- PH_EVT_PACKAGER_FILE_UPLOAD_FAILURE

- PH_EVT_PACKAGER_HTTP_RESPONSE_ERROR
- PH_EVT_PACKAGER_INIT_FAILURE
- PH_EVT_PACKAGER_REST_PARSE_ERROR
- PH_EVT_PACKAGER_RUN_PROCESS_ERROR
- PH_JAVA_AGENT_APPSERVER_CONN_ERROR
- PH_JAVA_AGENT_APPSERVER_EXECUTE_ERROR
- PH_JAVA_AGENT_CONTROLLER_CMD_PARSE_ERROR
- PH_JAVA_AGENT_CONTROLLER_CMD_READ_ERROR
- PH_JAVA_AGENT_CONTROLLER_GENERIC_ERROR
- PH_JAVA_AGENT_CONTROLLER_LINE_READ_ERROR
- PH_JAVA_AGENT_CONTROLLER_XML_READ_ERROR
- PH_JAVA_AGENT_CUSTOM_JDBC_CONN_ERROR
- PH_JAVA_AGENT_CUSTOM_JDBC_EXEC_ERROR
- PH_JAVA_AGENT_DISCOVERY_TEST_ERROR
- PH_JAVA_AGENT_ERROR
- PH_JAVA_AGENT_GLASSFISH_MONITOR_ERROR
- PH_JAVA_AGENT_GLASS_FISH_WARNING
- PH_JAVA_AGENT_GOOGLEAPPS_EXEC_ERROR
- PH_JAVA_AGENT_IBMDB2_AUDIT_CONN_ERROR
- PH_JAVA_AGENT_IBMDB2_AUDIT_EXEC_ERROR
- PH_JAVA_AGENT_IBM_DB2_CAT_READ_ERROR
- PH_JAVA_AGENT_IBM_DB2_CONN_ERROR
- PH_JAVA_AGENT_IBM_DB2_INTERNAL_ERROR
- PH_JAVA_AGENT_INFO
- PH_JAVA_AGENT_JBOSS_CONN_ERROR
- PH_JAVA_AGENT_JBOSS_EXEC_ERROR
- PH_JAVA_AGENT_JBOSS_MONITOR_ERROR
- PH_JAVA_AGENT_JDBC_PULL_UNSUPP_ERROR
- PH_JAVA_AGENT_JDBC_SQL_NOT_SUPPORT_ERROR
- PH_JAVA_AGENT_JMX_CONN_ERROR
- PH_JAVA_AGENT_JMX_EXEC_ERROR
- PH_JAVA_AGENT_JOB_EXECUTOR_ERROR
- PH_JAVA_AGENT_JOB_STATUS_UPLOAD_ERROR
- PH_JAVA_AGENT_JOB_TYPE_ERROR
- PH_JAVA_AGENT_JOB_XML_LOAD_ERROR
- PH_JAVA_AGENT_JOB_XML_PARSE_ERROR
- PH_JAVA_AGENT_MCAFEE_MYSQL_MONITOR_ERROR
- PH_JAVA_AGENT_MCAFEE_VULN_SCANNER_ERROR
- PH_JAVA_AGENT_MONITOR_GEN_ERROR
- PH_JAVA_AGENT_MONITOR_TIMEOUT_ERROR
- PH_JAVA_AGENT_MSSQL_DDL_CONN_ERROR
- PH_JAVA_AGENT_MSSQL_LOGON_CONN_ERROR
- PH_JAVA_AGENT_MSSQL_LOGON_EXEC_ERROR

- PH_JAVA_AGENT_MSSQL_MONITOR_ERROR
- PH_JAVA_AGENT_MSSQL_PERF_CONN_ERROR
- PH_JAVA_AGENT_MSSQL_PERF_EXECUTE_ERROR
- PH_JAVA_AGENT_MYSQL_PERF_CONN_ERROR
- PH_JAVA_AGENT_MYSQL_PERF_EXEC_ERROR
- PH_JAVA_AGENT_NESSUS_REPORT_PARSE_ERROR
- PH_JAVA_AGENT_ORACLE_DB_ERROR
- PH_JAVA_AGENT_ORADB_AUDIT_CONN_ERROR
- PH_JAVA_AGENT_ORADB_AUDIT_EXEC_ERROR
- PH_JAVA_AGENT_ORADB_LOGON_EXEC_ERROR
- PH_JAVA_AGENT_ORADB_PERF_CONN_ERROR
- PH_JAVA_AGENT_ORADB_PERF_EXEC_ERROR
- PH_JAVA_AGENT_SNORT_CONN_ERROR
- PH_JAVA_AGENT_SNORT_EVENTID_ERROR
- PH_JAVA_AGENT_SNORT_EXEC_ERROR
- PH_JAVA_AGENT_SNORT_SENSORID_ERROR
- PH_JAVA_AGENT_SNORT_TCP_OPTION_ERROR
- PH_JAVA_AGENT_TOMCAT_MONITOR_ERROR
- PH_JAVA_AGENT_UTILS_ERROR
- PH_JAVA_AGENT_VMWARE_HWSTATUS_EXEC_ERROR
- PH_JAVA_AGENT_VMWARE_LOG_CONN_ERROR
- PH_JAVA_AGENT_VMWARE_LOG_EXEC_ERROR
- PH_JAVA_AGENT_VMWARE_MONITOR_ERROR
- PH_JAVA_AGENT_VMWARE_PERF_COUNTER_MISSING
- PH_JAVA_AGENT_VMWARE_PERF_DATA_RETRIEVE_ERROR
- PH_JAVA_AGENT_VMWARE_PERF_ENTITY_MISSING
- PH_JAVA_AGENT_VMWARE_PERF_HOST_MISSING
- PH_JAVA_AGENT_VMWARE_PERF_MON_EXCEPTION
- PH_JAVA_AGENT_VMWARE_PERF_ROLLUP_MISSING
- PH_JAVA_AGENT_VMWARE_PERF_STAT_NAME_MISSING
- PH_JAVA_AGENT_VMWARE_PERF_VM_MISSING
- PH_JAVA_AGENT_VMWARE_THREAD_EXEC_ERROR
- PH_JAVA_AGENT_VULN_REPORT_PARSER_ERROR
- PH_JAVA_AGENT_VULN_REPORT_VERIFY_ERROR
- PH_JAVA_AGENT_WEBLOGIC_MONITOR_ERROR
- PH_JAVA_AGENT_WEBSense_EMAIL_MISSING_LOGDB
- PH_JAVA_AGENT_WEBSense_JDBC_PULL_ERROR
- PH_JAVA_AGENT_WEBSense_MAIL_CONN_ERROR
- PH_JAVA_AGENT_WEBSense_MAIL_EXEC_ERROR
- PH_JAVA_AGENT_WEBSense_MAIL_PULL_ERROR
- PH_JAVA_AGENT_WEBSense_WEB_CONN_ERROR
- PH_JAVA_AGENT_WEBSense_WEB_EXEC_ERROR
- PH_JAVA_AGENT_WEBSense_WEB_MISSING_LOGDB

- PH_JAVA_AGENT_WEBSPHERE_CONN_ERROR
- PH_JAVA_AGENT_WEBSPHERE_EXEC_ERROR
- PH_JAVA_AGENT_WEBSPHERE_MONITOR_ERROR
- PH_LINUX_AGENT_ACCOUT_MISSING
- PH_LINUX_AGENT_BIND_PORT_FAILED
- PH_LINUX_AGENT_CONFIG_ATTR_DECRYPTED_FAILED
- PH_LINUX_AGENT_CONFIG_ATTR_ENCRYPTED_FAILED
- PH_LINUX_AGENT_CONFIG_ATTR_NOT_FOUND
- PH_LINUX_AGENT_CONFIG_MISS_ATTR
- PH_LINUX_AGENT_CREATE_SOCKET_FAILED
- PH_LINUX_AGENT_EXIT
- PH_LINUX_AGENT_HOST_IP_GOT_FAILED
- PH_LINUX_AGENT_INCREASE_RECV SOCK_BUF_MAX_FAILED
- PH_LINUX_AGENT_INIT_FIM_FAILED
- PH_LINUX_AGENT_INIT_HTTP_FAILED
- PH_LINUX_AGENT_LOG_GENERIC
- PH_LINUX_AGENT_NEW_FIM_LOADED
- PH_LINUX_AGENT_OPEN_FILE_FAILED
- PH_LINUX_AGENT_OPEN_PORT_FAILED
- PH_LINUX_AGENT_PWD_MISSING
- PH_LINUX_AGENT_RECV_ERROR
- PH_LINUX_AGENT_REGISSTER_FAILED
- PH_LINUX_AGENT_TEMPLATE_STATUS
- PH_LINUX_AGENT_UNINSTALL
- PH_LINUX_AGENT_UPLOAD_FILE_FAILED
- PH_LINUX_AGENT_UPLOAD_FILE_SUCCESS
- PH_LINUX_AGENT_USER_FILE_LOG_GENERIC
- PH_LINUX_AGENT_VERIFIER_ERROR
- PH_NETFLOW_BAD_FLOW
- PH_NETFLOW_BAD_FLOW_END
- PH_NETFLOW_BAD_HEADER_PROTOCOL
- PH_NETFLOW_BAD_PACKET
- PH_NETFLOW_BAD_RECORD
- PH_NETFLOW_BAD_TYPE
- PH_NETFLOW_BAD_VER
- PH_NETFLOW_EXCEPTION
- PH_SYSTEM_DEVAPP_EVENTS_PER_SEC
- PH_SYSTEM_DEVAPP_NO_EVENTS
- PH_SYSTEM_DEVICE_NO_EVENTS
- PH_SYSTEM_EPS_GLOBAL
- PH_SYSTEM_EPS_NODE
- PH_SYSTEM_EPS_ORG
- PH_SYSTEM_EVENTS_FWD_STAT

- [PH_SYSTEM_EVENTS_PER_SEC](#)
- [PH_SYSTEM_EVENTS_VIA_ZMQ_EPS](#)
- [PH_SYSTEM_INTERNAL_EVENTS_PER_SEC](#)
- [PH_SYSTEM_IP_EVENTS_PER_SEC](#)
- [PH_SYSTEM_PERF_EVENTS_PER_SEC](#)
- [PH_SYSTEM_STORED_EVENTS_PER_SEC](#)
- [PH_SYSTEM_SUMM_EVENTS_STORED_EPS](#)
- [PH_VA_EVENTS_PER_SEC](#)

EventType: PH_AGENTMGR_ACI_ATTR_NOT_FOUND

Description: Agent Manager Cisco ACI monitoring module cannot find specific attribute

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ACI_CURL_HANDLE_GET_FAILED

Description: Agent Manager Cisco ACI monitoring module unable to get curl handle

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ACI_FILE_WRITE_ERROR

Description: Agent Manager Cisco ACI monitoring module unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_ACI_JSON_PARSE_FAILED

Description: Agent Manager Cisco ACI monitoring module failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ACI_SERVER_EMPTY

Description: Agent Manager Cisco ACI monitoring module found server is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ACI_TOKEN_GET_FAILED

Description: Agent Manager Cisco ACI monitoring module cannot get login token

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ALERTLOGIC_CURL_HANDLE_GET_FAILED

Description: Agent Manager Alert Logic log parsing module unable to get curl handle

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ALERTLOGIC_FILE_LOAD_ERROR

Description: Agent Manager Alert Logic log parsing module failed to load file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_ALERTLOGIC_FILE_READ_ERROR

Description: Agent Manager Alert Logic log parsing module found wrong format in file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_ALERTLOGIC_FILE_WRITE_ERROR

Description: Agent Manager Alert Logic log parsing module unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_ALERTLOGIC_INVALID_DATA

Description: Agent Manager Alert Logic log parsing module found invalid data format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ALERTLOGIC_INVALID_PATH

Description: Agent Manager Alert Logic log parsing module found invalid incident path

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_ALERTLOGIC_QUERY_INTERVAL_TOO_LONG

Description: Agent Manager Alert Logic log parsing module found query interval is larger, it will be narrowed in one week

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ALERTLOGIC_SERVER_EMPTY

Description: Agent Manager Alert Logic log parsing module found server is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AMPCLOUD_CURL_CONNECT_FAILED

Description: Agent Manager AMP Cloud log parsing module unable to connect server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
httpStatusCode	HTTP Status	string	

EventType: PH_AGENTMGR_AMPCLOUD_CURL_HANDLE_GET_FAILED

Description: Agent Manager AMP Cloud log parsing module unable to get curl handle

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AMPCLOUD_FILE_LOAD_ERROR

Description: Agent Manager AMP Cloud log parsing module failed to load file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_AMPCLOUD_FILE_READ_ERROR

Description: Agent Manager AMP Cloud log parsing module found wrong format in file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_AMPCLOUD_INVALID_DATA

Description: Agent Manager AMP Cloud log parsing module found Invalid data format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AMPCLOUD_JSON_PARSE_FAILED

Description: Agent Manager AMP Cloud log parsing module failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AGENTMGR_AMPCLOUD_NO_DEFINE_SEVERITY

Description: Agent Manager AMP Cloud log parsing module found event severity is not defined

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AMPCLOUD_SERVER_EMPTY

Description: Agent Manager AMP Cloud log parsing module found server is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_API_PERMISSION_MISSING

Description: There is no permission

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_AWSCLOUDWATCH_GETLOGS

Description: Attempting to get cloudwatch logs from log group and stream

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
groupName	Group Name	string	
streamName	AWS Stream Name	string	
startTime	Start Time	Date	This is the start time of a given item or task, and is stored in epoch milliseconds
endTime	End Time	Date	This is the end time of a given item or task, stored in epoch milliseconds.

EventType: PH_AGENTMGR_AWSFLOWLOG_EVENT_PULL_FAILED

Description: Agent Manager AWS module failed to get AWS Flow log after 5 tries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_AWSFLOWLOG_FILE_WRITE_ERROR

Description: Agent Manager AWS Flow log handling module unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_AWSFLOWLOG_LOG_FORMAT_WRONG

Description: Agent Manager AWS Flow log handling module encountered wrong log format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AWSKINESIS_CONSUMER_START_FAILED

Description: Failed to start Kinesis consumer process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_AWS_CACHE_FILE_ERROR

Description: Agent Manager AWS Cache file is not available

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AWS_DELETE_OJBJECTKEY_FAILED

Description: Failed to delete object key from SQS

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_AWS_DOWNLOAD_OJBJECT_FAILED

Description: Failed to download object from bucket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_AWS_EVT_DOWNLOAD_FAILED

Description: Agent Manager AWS module failed to download event by do_system failed

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_AGENTMGR_AWS_EVT_SEND_FAILED

Description: Agent Manager AWS module failed to send cloudtrail event to phParser after 5 tries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AWS_GET_OJBJECTKEY_FAILED

Description: Agent Manager AWS agent failed to get object key from SQS

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_AWS_GZ_FILE_OPEN_ERROR

Description: Agent Manager AWS module gailed to open gz file, or not enough memory to open it

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_AWS_JSON_PARSE_FAILED

Description: Agent Manager AWS module failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AWS_SQSURL_FORMAT_ERROR

Description: Agent Manager AWS Sqs Url format is wrong

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_API_CALL_FAILED

Description: Agent Manager BOX module failed to call BOX API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_ATTR_NOT_FOUND

Description: Agent Manager BOX module cannot find attribute

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_EVENT_PULL_FAILED

Description: Agent Manager BOX module failed to pull BOX log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
accountName	Account Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_BOX_FILE_ID_EMPTY

Description: Agent Manager BOX module found empty file ID

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_FILE_LIMIT_EXCEED

Description: Agent Manager BOX module found that the number of monitoring file exceeded limit

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_FILE_NOT_MONITORED_ERROR

Description: Agent Manager BOX module found that the file is not monitored before

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_BOX_FILE_PATH_PARSE_FAILED

Description: Agent Manager BOX module could not parse file path

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_BOX_FILE_TYPE_WRONG

Description: Agent Manager BOX module found wrong file type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileType	File Type	string	

EventType: PH_AGENTMGR_BOX_FOLDER_TYPE_WRONG

Description: Agent Manager BOX module found wrong folder type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_HTTP_NO_RESPONSE

Description: Agent Manager BOX module did not find response from App Server Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_AGENTMGR_BOX_JSON_PARSE_FAILED

Description: Agent Manager BOX module failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_RESPONSE_NO_SPECIAL_ATTRIBUTE

Description: Agent Manager BOX module response doesn't have special node

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_TIME_CONVERT_FAILED

Description: Agent Manager BOX module could not convert time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_BOX_XML_PARSE_FAILED

Description: Agent Manager BOX module failed to parse XML from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_CISCOAMP_CONSUMER_START_FAILED

Description: Failed to start Cisco AMP consumer process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_CLOUDPASSAGE_API_CALL_FAILED

Description: CloudPassage Halo REST API call api failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_CLOUDPASSAGE_FILE_WRITE_ERROR

Description: Unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_CLOUDPASSAGE_GET_EVENT_FAILED

Description: Failed to get event from CloudPassage API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_CLOUDPASSAGE_JSON_EMPTY

Description: JSON is empty

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_CLOUDPASSAGE_JSON_PARSE_FAILED

Description: Failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_CLOUDPASSAGE_TOKEN_EMPTY

Description: Token is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_CLOUDTRAIL_FILE_READ_FAILED

Description: Agent Manager AWS CloudTrail module encountered error while reading Cloudtrail queue cache file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_CONFIG_ERROR

Description: Agent Manager own configuration error

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_CONFIG_VERSION_SEND_FAILED

Description: Agent Manager failed to send config version to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_AGENTMGR_CONFIG_WARNING

Description: FortiSIEM Agent Manager configuration warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AGENTMGR_CREDENTIAL_GET_FAILED

Description: Agent Manager failed to get credentials

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobName	Job Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_CROWDSTRIKE_GET_DATAFEED_URL_FAILED

Description: Failed to get crowdstrike datafeed url

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_CUST_RESULT_UPLOAD_FAILED

Description: Agent Manager failed to upload test custom performance monitor result xml to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_DIR_CREATE_FAILED

Description: Could not create dir

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_AGENTMGR_EVENT_PULL_FAILED

Description: Agent Manager Rapid7 InsightVM pulling engine failed to pull log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
accountName	Account Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_FALCONDATAREP_SCRIPT_FAILED

Description: Failed to run Falcon Data Replicator script

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_FILE_PARSE_ERROR

Description: Agent Manager/module failed to parse file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_FILE_WRITE_ERROR

Description: Agent Manager Rapid7 InsightVM pulling engine failed to write file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_FIREAMP_CERT_DOWNLOAD_FAILED

Description: Agent Manager/FireAMP Module cannot download certificate file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_FIREAMP_DATA_FORMAT_SET_FAILED

Description: Agent Manager/FireAMP Module encountered missing event mapping configuration

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_FIREAMP_EVENT_PULL_FAILED

Description: Agent Manager/FireAMP Module failed to pull log from server!

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_FIREAMP_EVT_TYPE_LOAD_FAILED

Description: Agent Manager/FireAMP Module encountered empty event mapping configuration

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_FIREAMP_FILE_LOAD_ERROR

Description: Agent Manager/FireAMP Module failed to load file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_FIREAMP_FILE_OPEN_ERROR

Description: Agent Manager/FireAMP Module failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_FIREAMP_INVALID_DATA

Description: Agent Manager/FireAMP Module found invalid response data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_FIREAMP_NEW_AGENT_FAILED

Description: Agent Manager/FireAMP Module - new agent failed

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_FIREAMP_NO_ATTR

Description: No configuration event attribute

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_FIREAMP_NO_PROTOCOL

Description: Can't find protocol number from IANA table

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_FORTICASB_GET_SERVICE_ALERT_ERROR

Description: Failed to get services alerts

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serviceName	Service Name	string	

EventType: PH_AGENTMGR_FORTICASB_GET_SERVICE_ERROR

Description: Failed to get services

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
unitId	Unit Id	string	

EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_FAILED

Description: FortiNDR cloud integration failed to call API URI

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_NEXT_PAGE

Description: FortiNDR paginated api call being made

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_NO_RESULTS

Description: API call to FortiNDR api returned no results, this is normal if no results in defined time interval

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_RESULTS

Description: FortiNDR cloud integration called API URI successfully

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

EventType: PH_AGENTMGR_FORTINDR_GET_BUCKET_KEY

Description: FortiNDR integration is processing an s3 bucket key

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
bucketName	Bucket Name	string	
userKey	User Key	string	
categoryType	Category Type	string	

EventType: PH_AGENTMGR_FORTINDR_GET_BUCKET_OBJ

Description: FortiNDR integration is downloading an object from s3 bucket

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
bucketName	Bucket Name	string	
userKey	User Key	string	
categoryType	Category Type	string	

EventType: PH_AGENTMGR_GET_SCAN_RESULTS_FAILED

Description: Failed to get the scan result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_GITHUB_API_CALL_FAILED

Description: Agent Manager/GitHub module failed to call Github API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_GITHUB_CREDENTIAL_GET_FAILED

Description: Agent Manager/GitHub module failed to get credential from App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_AGENTMGR_GITHUB_EVENT_PULL_FAILED

Description: Agent Manager/GitHub module failed to pull log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
accountName	Account Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_GITHUB_FILE_OPEN_ERROR

Description: Agent Manager/GitHub module failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_GITHUB_JSON_PARSE_FAILED

Description: Agent Manager/GitHub module failed to parse JSON response from GitHub server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_GITHUB_TIME_CONVERT_FAILED

Description: Agent Manager/GitHub module failed to convert time in JSON response from GitHub server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_GIT_CLONE_REPO_FAILED

Description: Failed to git clone by do_system

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_AGENTMGR_GIT_HANDLE_ERR_FILE_FAILED

Description: Failed to handle error file

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_GIT_PULL_EVT_FAILED

Description: Failed to get git log by do_system

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_AGENTMGR_GIT_SAVE_COMMITID_FAILED

Description: Failed to save CommitId of repository

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_GZ_FILE_OPEN_ERROR

Description: Failed to open gz file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_INIT_AGENT

Description: Initialize agent

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_INIT_CACHE_FILE_FAILED

Description: FortiSIEM Agent Manager failed to initialize cache

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobName	Job Name	string	

EventType: PH_AGENTMGR_INIT_NO_CRED

Description: Agent Manager/Cisco IPS log pulling module failed to initialize due to missing credentials

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobName	Job Name	string	

EventType: PH_AGENTMGR_INVALID_MGR

Description: Invalid Agent Manager

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_IPS_AUTH_FAILED

Description: Agent Manager/Cisco IPS log pulling module found wrong user name, password for logging to IPS appliance

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_IPS_EVENT_PULL_FAILED

Description: Agent Manager/Cisco IPS log pulling module failed to pull Cisco IPS log from server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_AGENTMGR_IPS_FILE_OPEN_ERROR

Description: Agent Manager/Cisco IPS log pulling module failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_IPS_OBTAIN_SUBSCRIPTION_FAILED

Description: Agent Manager/Cisco IPS log pulling module failed to obtain subscription id

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_IPS_SET_SSL_FAILED

Description: SSL setting doesn't work

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_JAVA_AGENT_PIPE_WRITE_FAILED

Description: Failed to write to java agent pipe

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_JAVA_AGENT_START_FAILED

Description: Agent Manager failed to start Java agent, will retry

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_JAVA_AGENT_TYPE_UNKNOWN

Description: Agent Manager encountered unknown java agent job type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_JAVA_AGENT_USER_MISSING

Description: FortiSIEM Agent Manager found user name missing in java Agent configuration

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_AGENTMGR_JAVA_AGENT_ZOMBIE

Description: Agent Manager found Java Agent is in zombie state

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_JAVA_CMD_SEND_FAILED

Description: Agent Manager failed to send commands to java agent, need to be killed

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_JAVA_FORK_FAILED

Description: Agent Manager failed to fork Java Agent

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_JAVA_INCOMPLETE_DEV_INFO

Description: Agent Manager found incomplete device info for Java Agent

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_JAVA_NO_DEV_TYPE_FOR_JDBC

Description: Agent Manager encountered missing device type for Java Agent JDBC monitoring

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_AGENTMGR_JAVA_NO_STATUS_FILE

Description: Agent Manager missing status file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_JAVA_PIPE_FAILED

Description: Agent Manager failed to Pipe command for Java Agent

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_JAVA_PROCESS_STATE_GET_FAILED

Description: Agent Manager failed to get Java Agent process state

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_JAVA_SIGKILL_SEND_FAILED

Description: Agent Manager failed to send SIGKILL to java agent

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_JAVA_UNSupport_DEV_Type_FOR_JDBC

Description: Agent Manager encountered unsupported device type for Java Agent JDBC monitoring

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_AGENTMGR_JAVA_USER_PWD_GET_FAILED

Description: Agent Manager failed to get user name and password

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_JSON_PARSE_FAILED

Description: Agent Manager Rapid7 InsightVM monitoring module failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_KAFKA_CONSUME_LOG_FAILED

Description: Agent Manager / Kafka Consumer failed to pull log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_CREATE_CONSUMER

Description: phKafkaConsumer creates a consumer handle successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
groupName	Group Name	string	
user	User	string	
topicName	Topic Name	string	Kafka Topic Name

EventType: PH_AGENTMGR_KAFKA_CREATE_CONSUMER_FAILED

Description: Agent Manager / Kafka Consumer failed to create consumer

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_CREATE_PRODUCER_FAILED

Description: Agent Manager / Kafka Consumer failed to create producer

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_CREATE_TOPIC_FAILED

Description: Agent Manager / Kafka Consumer failed to create topic

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
topicName	Topic Name	string	Kafka Topic Name
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_ERROR

Description: Agent Manager / Kafka Consumer encountered occur

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_AGENTMGR_KAFKA_METADATA_FAILED

Description: Agent Manager / Kafka Consumer failed to get metadata

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_PRODUCER_ERROR

Description: Event Forwarder failed to write events into Kafka

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_AGENTMGR_KAFKA_PULL_JOB_FAILED

Description: Agent Manager / Kafka Consumer failed to Consume log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_KAFKA_REBALANCE

Description: Kafka rebalanceCb

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_KAFKA_RELEASE_CONSUMER

Description: phKafkaConsumer releases a consumer handle

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
groupName	Group Name	string	
user	User	string	
topicName	Topic Name	string	Kafka Topic Name

EventType: PH_AGENTMGR_KAFKA_START_FAILED

Description: Agent Manager / Kafka Consumer failed to start

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_SUBSCRIBE_FAILED

Description: Agent Manager / Kafka Consumer failed to subscribe topic

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
topicName	Topic Name	string	Kafka Topic Name
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_UPDATE_CONFIG_FAILED

Description: Agent Manager / Kafka Consumer failed to update attribute in config

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_UPDATE_ERROR

Description: Agent Manager / Kafka Consumer failed to update failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KILL_PROCESS

Description: Try to kill process

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_MSAZURE_CONFIG_ARM_FAILED

Description: Agent Manager / MS Azure config mode arm failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_MSAZURE_DOWNLOAD_FAILED

Description: Agent Manager / MS Azure failed to download Azure audit log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_MSAZURE_JSON_EMPTY

Description: Agent Manager / MS Azure found empty returned JSON from Azure

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_MSAZURE_JSON_FILE_NAME_EMPTY

Description: Agent Manager / MS Azure JSON file name is empty from Azure

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_MSAZURE_JSON_FILE_PARSE_FAILED

Description: Agent Manager / MS Azure found malformed JSON file from Azure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_MSAZURE_JSON_PARSE_FAILED

Description: Agent Manager / MS Azure found malformed JSON from Azure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_MSAZURE_LOGIN_FAILED

Description: Agent Manager / MS Azure failed to login to Azure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_MSG_QUEUE_ACCESS_FAILED

Description: Agent Manager failed to access message queue

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_MSG_RECV_FAILED

Description: Agent Manager failed to receive msg

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_OCI_SET_INSTANCE_NAME_FAILED

Description: Failed to set Oracle OCI Instance Name to hostname of this node, leaving as instance1

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_OFFICE365_API_CALL_FAILED

Description: Agent Manager / Office365 log pulling engine failed to call api

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_OFFICE365_EVENT_PULL_FAILED

Description: Agent Manager / Office365 log pulling engine failed to pull log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
accountName	Account Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_OFFICE365_FILE_WRITE_ERROR

Description: Agent Manager / Office365 log pulling engine unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_OFFICE365_GET_SUBSCRIBE_FAILED

Description: FortiSIEM Agent Manager failed to get Office365 subscription

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_OFFICE365_JSON_PARSE_FAILED

Description: Agent Manager / Office365 log pulling engine failed to parse Office365 JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_OFFICE365_START_SUBSCRIBE_FAILED

Description: FortiSIEM Agent Manager failed to start Office365 subscription

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_OFFICE365_SUBSCRIBE_EMPTY

Description: FortiSIEM Agent Manager found Office365 subscription to be empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_OFFICE365_SUBSCRIBE_FAILED

Description: Agent Manager / Office365 log pulling engine failed to get subscription list

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_OFFICE365_TOKEN_EMPTY

Description: Agent Manager / Office365 log pulling engine found empty Token

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_OKTA_EVT_DOWNLOAD_FAILED

Description: Agent Manager / OKTA failed to download events

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_OKTA_FILE_WRONG

Description: Agent Manager / OKTA encountered wrong Okta user list file. Please download again

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_OKTA_NO_USER_INFO

Description: Agent Manager / OKTA user list file doesn't contain any user info

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_OKTA_RESULT_UPLOAD_FAILED

Description: Agent Manager / OKTA failed to upload discovery result to App server

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_OKTA_RESULT_UPLOAD_WARNING

Description: FortiSIEM Agent Manager failed to upload OKTA User list to App Server

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_PARSER_UNABLE_CONNECT

Description: Agent Manager unable to connect to parser host

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
ipPort	IP Port	uint16	IP port number

EventType: PH_AGENTMGR_PERF_OBJ_PARSE_FAILURE

Description: Agent Manager did not find any performance objects to monitor

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_PROCESS_INIT_FAILED

Description: Agent Manager failed to initialize

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_PULLING_JOB_OUTDATE

Description: FortiSIEM Agent Manager job pull error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobName	Job Name	string	
serverIpAddr	Server IP	IP	

EventType: PH_AGENTMGR_REMOVE_FILE_FAILED

Description: Failed to remove file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_AGENTMGR_REST_API_CALL_FAILED

Description: Agent fails to call rest API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
infoURL	Informational URL	string	This field captures an URL if present in an event
httpStatusCode	HTTP Status	string	

EventType: PH_AGENTMGR_RSAS_XML_PARSE_FAILED

Description: AgentManager failed to parse XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_RUN_CMD_FAILED

Description: do_system failed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_RUN_SCRIPT_FAILED

Description: AgentManager failed to run script

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_RUN_SCRIPT_WITHOUT_TASK_ID

Description: AgentManager found missing task id in run script notification

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_ATTR_NOT_FOUND

Description: Agent Manager / Salesforce log pulling engine cannot find attribute

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_COLUMN_NOT_FOUND

Description: Agent Manager / Salesforce log pulling engine can not find a specific column in Salesforce Event Log File

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_CURL_EXECUTE_FAILED

Description: Agent Manager / Salesforce log pulling engine failed to execute curl to get Salesforce log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_AGENTMGR_SALESFORCE_CURL_HANDLE_GET_FAILED

Description: Agent Manager / Salesforce log pulling engine unable to get curl handle

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_FILE_LOAD_ERROR

Description: Agent Manager / Salesforce log pulling engine failed to load file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_SALESFORCE_FILE_WRITE_ERROR

Description: Agent Manager / Salesforce log pulling engine unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_SALESFORCE_INVALID_DATA

Description: Agent Manager / Salesforce log pulling engine received invalid response from Salesforce

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_INVALID_LOG_FILE

Description: Agent Manager / Salesforce log pulling engine received invalid Salesforce Event Log File csv

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_JSON_PARSE_FAILED

Description: Agent Manager / Salesforce log pulling engine received failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_LOGIN_FAILED

Description: Agent Manager / Salesforce log pulling engine failed to login to Salesforce

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
infoURL	Informational URL	string	This field captures an URL if present in an event

EventType: PH_AGENTMGR_SALESFORCE_SERVER_EMPTY

Description: Agent Manager / Salesforce log pulling engine found Server is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_TOKEN_GET_FAILED

Description: Agent Manager / Salesforce log pulling engine can't get login token

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_TOKEN_REGET_FAILED

Description: Agent Manager / Salesforce log pulling engine login session is expired and failed to re-get token

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_VERSION_PATH_EMPTY

Description: Agent Manager / Salesforce log pulling engine found empty version path

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_XML_PARSE_FAILED

Description: Agent Manager / Salesforce log pulling engine failed to parse XML from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SCRIPT_NOTIFICATION_SPAWN_FAILED

Description: Agent Manager encountered error in spawning run script notification thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SERVER_HOST_NAME_RESOLVE_FAILED

Description: Agent Manager could not resolve server host name

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SERVER_HOST_NAME_RESOLVE_WARNING

Description: FortiSIEM Agent Manager failed to resolve Host Name to IP

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	
jobName	Job Name	string	

EventType: PH_AGENTMGR_SERVER_IP_RESOLVE_FAILED

Description: Agent Manager could not resolve server IP

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SERVER_IP_RESOLVE_WARNING

Description: FortiSIEM Agent Manager failed to resolve IP to Host Name

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
jobName	Job Name	string	

EventType: PH_AGENTMGR_SETUP_STREAM_FAILED

Description: Failed to setup stream connection

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_START_THREAD_FAILED

Description: Failed to start thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_STATUS_REPORT_FAILED

Description: Agent Manager failed to report task status to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_STATUS_REPORT_INIT_FAILED

Description: Agent Manager failed to initialize job status reporter

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_STOP_STREAM_FAILED

Description: Failed to stop stream connection

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_TENABLE_EXPORT_SCAN_FAILED

Description: Exported scan failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_TENABLE_GET_DOWNLOAD_FAILED

Description: Download exported scan failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_TENABLE_GET_SCANS_FAILED

Description: Get the scan list failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_TENABLE_GET_STATUS_FAILED

Description: Check the file status of exported scan failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_TENABLE_PULL_FAILED

Description: Failed to pull Tenable.io data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_TIME_CONVERSION_FAILED

Description: Agent Manager/module failed to convert time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_TIME_STR_FORMAT_INVALID

Description: The format of time string is wrong

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
paraName	Param Name	string	

EventType: PH_AGENTMGR_TOKEN_GET_FAILED

Description: Agent Manager monitoring module cannot get login token

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_UNPACK_FILE_FAILED

Description: Agent Manager unpack file failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_AGENTMGR_UPDATE_AGENT

Description: Update agent

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_UPDATE_BOOKMARK_FAILED

Description: Failed to update bookmark

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_UPDATE_WEBHOOK_CRED_FAILED

Description: Failed to update Webhook credential

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_UPDATE_WEBHOOK_CRED_SUCCESS

Description: Update Webhook credential successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_WINDEFATP_API_CALL_FAILED

Description: Windows Defender ATP REST API call api failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_WINDEFATP_FILE_WRITE_ERROR

Description: Unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_WINDEFATP_GET_ALERT_FAILED

Description: Failed to get alert from Windows Defender ATP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_WINDEFATP_JSON_EMPTY

Description: JSON is empty

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_WINDEFATP_JSON_PARSE_FAILED

Description: Failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_WINDEFATP_TOKEN_EMPTY

Description: Token is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_WMI_EVENT_PULL_ERROR

Description: Agent Manager / Windows WMI event log pulling engine encountered error

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_WMI_EVENT_PULL_WARNING

Description: FortiSIEM Agent Manager WMI event pull warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_WMI_FILE_OPEN_ERROR

Description: Agent Manager / Windows WMI event log pulling engine failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_WMI_LOG_PULL_ERROR

Description: Failed to pull logs by WMI

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
errorString	Error String	string	This is the error message, synonymous to attribute errReason
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AGENTMGR_WMI_MISSING_LOG

Description: Some logs are missing

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AGENTMGR_WMI_STATUS_REPORT_FAILED

Description: Agent Manager / Windows WMI event log pulling engine failed to report task status to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_WMI_USER_PWD_GET_FAILED

Description: Agent Manager / Windows WMI event log pulling engine failed to get WMI user name and password

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_WVSS_XML_PARSE_FAILED

Description: Agent Manager / Windows WMI event log pulling engine failed to parse XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_XML_PARSE_FAILED

Description: Agent Manager / Windows WMI event log pulling engine failed to parse XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorMsg	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_BAD_NETFLOW_PACKET

Description: Bad netflow packet

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BAD_NETFLOW_VER

Description: Unsupported netflow version

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CHECKPOINT_CERTHANDLER_ERROR

Description: Checkpoint failed to parse device certificate received from App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_CERTPULL_ERROR

Description: Checkpoint failed to obtain certificate from App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_CMD_USAGE_ERROR

Description: Checkpoint command usage error

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_CPMI_FETCH_ERROR

Description: Checkpoint CPMI fetch error. Events may miss some metadata

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
errReason	Reason for Error	string	This is the reason for an error if given.

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_CHECKPOINT_DEV_INIT_ERROR

Description: Checkpoint device initialization error. Checkpoint device can not be monitored

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_FILE_RENAME_FAILURE

Description: FortiSIEM Checkpoint module failed to rename file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_CHECKPOINT_FWLOGHANDLER_ERROR

Description: Checkpoint LEA handler protocol error. Checkpoint device can not be monitored

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_FWLOGHANDLER_INIT_ERROR

Description: Checkpoint OPSEC log handler initialization error. Checkpoint device can not be monitored

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_HTTP_ERROR

Description: Checkpoint module failed to connect to App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_CHECKPOINT_LOGHANDLER_ERROR

Description: Checkpoint OPSEC log handler internal error

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_PROCESS_GET_FAILED

Description: Checkpoint module failed to get its parent process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CHECKPOINT_TESTCONN_ERROR

Description: Checkpoint test connectivity error. Checkpoint device can not be discovered

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_CHECKPOINT_UNABLE_PARSE_XML

Description: Checkpoint module unable to parse device credential XML received from App Server

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_COLLECTOR_CLOCK_SKEW

Description: Clock skew between Collector and Super

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
collectorId	Collector ID	uint32	This field captures the ID of a FortiSIEM Collector
collectorIp	Collector IP	IP	This field captures the IP address of a FortiSIEM Collector
superTime	Supervisor Time	Date	This field represents SupervisorTime used to determine Clock Skew between Collector and Supervisor. A Clock Skew may develop if NTP is not configured correctly in both Collector and Supervisor.
collectorTime	Collector Time	Date	This field represents Collector Time used to determine Clock Skew between Collector and Supervisor. A Clock Skew may develop if NTP is not configured correctly in both Collector and Supervisor.
timeSkewSec	Time skew	uint32	Time skew between Collector and Supervisor. If there is significant time skew then rules may not trigger, since rules need to be evaluated based on a time window.

EventType: PH_COLLECTOR_DOWN

Description: Collector down

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_COLLECTOR_EVENT_ARRIVAL_DELAYED

Description: Collector event delayed

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_COLLECTOR_EVENT_ARRIVAL_OK

Description: Collector event arrived on time

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_COLLECTOR_EVENT_STORE_DELAYED

Description: Collector event file delayed

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_COLLECTOR_EVENT_STORE_OK

Description: Collector event file on time

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_COLLECTOR_UP

Description: Collector up

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CYBERARK_INIT_ERROR

Description: FortiSIEM CyberArk module initialization error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DEV_FAIL_TO_PULL_EVENTS

Description: Fail to pull events

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_EVENT_FORWARDER_CHECKSUM_MISMATCH

Description: FortiSIEM Event Forwarder module encountered checksum error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FORWARDER_CONNECT_ERROR

Description: FortiSIEM Event Forwarder failed to connect to forwarding destination host

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_EVENT_FORWARDER_DIR_OPEN_FAILURE

Description: FortiSIEM Event Forwarder failed to open directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_EVENT_FORWARDER_FILE_OPEN_FAILURE

Description: FortiSIEM Event Forwarder failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FORWARDER_FILE_RENAME_FAILURE

Description: FortiSIEM Event Forwarder failed to rename file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	

EventType: PH_EVENT_FORWARDER_INIT_FAILURE

Description: FortiSIEM Event Forwarder module initialization failure

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_EVENT_FORWARDER_INVALID_GZIP_FILE

Description: FortiSIEM Event Forwarder module encountered invalid gzip file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FORWARDER_INVALID_PHOENIX_CONFIG

Description: FortiSIEM Event Forwarder module encountered invalid phoenix_config file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	
configName	Config Name	string	
configValue	Config Value	string	

EventType: PH_EVENT_FORWARDER_INVALID_PROTOCOL

Description: FortiSIEM Event Forwarder module encountered invalid forwarding protocol

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FORWARDER_KAFKA_ERROR

Description: FortiSIEM Event Forwarder module encountered Kafka protocol error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
actionName	Notification Action Name	string	

EventType: PH_EVENT_FORWARDER_KAFKA_INIT_FAILURE

Description: FortiSIEM Event Forwarder module initialization failure

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_EVENT_FORWARDER_KAFKA_PRODUCE_ERROR

Description: FortiSIEM Event Forwarder module encountered error while forwarding via Kafka protocol

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_EVENT_FORWARDER_MKDIR_FAILURE

Description: FortiSIEM Event Forwarder failed to create directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_EVENT_FORWARDER_RUN_PROCESS_ERROR

Description: FortiSIEM Event Forwarder failed to run process during execution

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FORWARDER_SOCKET_ERROR

Description: FortiSIEM Event Forwarder failed to create socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_EVENT_FORWARDER_SOCKET_WRITE_ERROR

Description: FortiSIEM Event Forwarder failed to write to socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_EVENT_FORWARDER_SSL_CERT_ERROR

Description: FortiSIEM Event Forwarder SSL certification error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_EVENT_FORWARDER_SSL_ERROR

Description: FortiSIEM Event Forwarder Generic SSL error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_EVENT_FWD_CERT_LOAD_FAILED

Description: Event Forwarder module failed to load certification file or key file for TLS based forwarding - forwarding via this method will not occur

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_EVENT_FWD_CERT_UNPAIRED

Description: Event Forwarder module detected unpaired certification file or key file - forwarding via this method will not occur

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_EVENT_FWD_DIR_MAKE_FAILED

Description: Event Forwarder module failed to create a directory during initialization

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_EVENT_FWD_DIR_OPEN_FAILED

Description: Event Forwarder module failed to open a directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_EVENT_FWD_FILE_RENAME_FAILED

Description: Event Forwarder module failed to rename a file

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	

EventType: PH_EVENT_FWD_FULL_FORWARDING_FAILED

Description: Event Forwarder failed to forward all events in one file to the destination, will retry

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_EVENT_FWD_GET_FILE_NUM_FAILURE

Description: Event Forwarder module failed to get event file count in /opt/phoenix/cache/parser/fwd

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_GZ_CLOSE_ERROR

Description: Event Forwarder module cannot close gz file stored in /opt/phoenix/cache/parser/fwd - event will not be forwarded

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FWD_GZ_FILE_OPEN_ERROR

Description: Event Forwarder failed to open event file (gz), or not enough memory to open it

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FWD_GZ_MD5_ERROR

Description: Event Forwarder module cannot get md5 of event file (gz)

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FWD_GZ_RENAME_ERROR

Description: Event Forwarder module cannot rename event file (gz)

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_GZ_SIZE_MISMATCH

Description: Event Forwarder found malformed event file (gz) - length mismatch

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FWD_KAFKA_WARNING

Description: Event Forwarder module failed on event serialization to send via Kafka

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_MD5_CHECKSUM_MISMATCH

Description: Event Forwarder found event file (gz) MD5 checksum

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_NETFLOW_REGEX_IGNORED

Description: Event Forwarder ignores regex filter in forwarding rule for Netflow since Netflow is binary

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_PARTIAL_FORWARDING_FAILED

Description: Event Forwarder failed to forward a subset of events in one file to the destination. Those events will be lost

Severity: 8 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_PARTIAL_FORWARDING_WARNING

Description: FortiSIEM Event Forwarder was able to do partial forwarding

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_EVENT_FWD_PCRE_ERROR

Description: Event Forwarder module failed to Pcre compile - this means the regular expression in the forwarding rule is invalid

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_PROCESS_INIT_FAILED

Description: Event Forwarder failed to initialize this process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_PROCESS_START_FAILED

Description: Event Forwarder failed to run

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_PROTO_FORWARDED_WRONG

Description: Event Forwarder found incorrect proto in the forwarding rule

Severity: 8 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_RENAME_GZ_ERROR

Description: FortiSIEM Event Forwarder failed to rename gz file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FWD_RULE_PARSE_ERROR

Description: Event forwarder module failed to parse event forwarding rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_SOCKET_CONNECT_FAILED

Description: Event Forwarder failed to connect the destination for TCP based forwarding

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_EVENT_FWD_SOCKET_GET_FAILED

Description: Event Forwarder failed to get socket for connecting the destination

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_EVENT_FWD_SOCKET_WRITE_FAILED

Description: Event Forwarder failed to write to socket for sending events

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_EVENT_FWD_SSL_CREATE_FAILED

Description: Event Forwarder unable to create new SSL context structure for TLS based forwarding

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_EVENT_FWD_SSL_SESSION_BUILD_FAILED

Description: Event Forwarder unable to build SSL session for TLS based forwarding

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_UNEXPECTED_FILE_REMOVED

Description: Event Forwarder removed unexpected event file (mismatched name format)

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_PKG_ATTR_NOT_FOUND

Description: Event Packager cannot find Worker name in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_EMPTY_FILE_REMOVED

Description: Event Packager found an empty event file - file will be removed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_PKG_FILE_ADD_TO_SVN_FAILED

Description: Event Packager failed to add configuration file to svn upload queue

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_PKG_FILE_REMOVED_ERROR

Description: Event Packager failed to remove event file after upload

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_PKG_FILE_RENAME_FAILED

Description: Event Packager failed to rename configuration file after scanning

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
exitValue	Command exit value	int32	

EventType: PH_EVENT_PKG_FILE_STAT_FAILED

Description: Event Packager failed to stat configuration or event file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_EVENT_PKG_FILE_UPLOAD_FAILED

Description: Event Packager failed to upload event file to Worker or Super; will retry

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
serverIpAddr	Server IP	IP	

EventType: PH_EVENT_PKG_FILE_UPLOAD_SUCCESS_HIGH

Description: Event file upload success is high

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ratio	Ratio	double	

EventType: PH_EVENT_PKG_FILE_UPLOAD_SUCCESS_LOW

Description: Event file upload success is low

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ratio	Ratio	double	

EventType: PH_EVENT_PKG_GZ_CLOSE_FAILED

Description: Event Packager failed to close event file after writing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_EVENT_PKG_GZ_FILE_OPEN_ERROR

Description: Event Packager failed to open gz file or not enough memory to open it

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_PKG_HTTP_FAILED

Description: Event Packager encountered HTTPS error response code

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_EVENT_PKG_HTTP_INIT_FAILED

Description: Event Packager HTTP client initialization failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_EVENT_PKG_INSERT_TASK_FAILED

Description: Failed to insert task into event file upload queue

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_NO_EVENT

Description: Event Packager did not upload any event in last 10 minutes

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_OPEN_DIR_FAILED

Description: Failed to open directory

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_EVENT_PKG_PROCESS_INIT_FAILED

Description: Event Packager failed to initialize

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_PROCESS_START_FAILED

Description: Event Packager failed to run

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_QUEUE_GET_FAILED

Description: Event Packager failed to get event file from the queue

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_EVENT_PKG_SERVER_LIST_UPLOAD_FAILED

Description: Event Packager failed to get upload server list from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_EVENT_PKG_SERVICE_LIST_EMPTY

Description: Empty upload service list

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_TASK_ADD_TO_QUEUE_FAILED

Description: Event Packager failed to add file upload task to queue

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_XML_PARSE_FAILED

Description: Event Packager failed to parse XML from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVTPKGER_FILE_UPLOAD_FAILED

Description: File upload failed

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_EVT_HANDLER_DBG

Description: Event handler debug message

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_ERR

Description: Event handler error message

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_EVT_QUEUE_LARGE

Description: Uploaded event files on Worker has a size of more than 100MB

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_EVT_QUEUE_WARNING

Description: Worker Input Event Queue large

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_INFO

Description: Event handler information

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_SVN_QUEUE_LARGE

Description: Uploaded SVN files size large

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_SVN_QUEUE_WARNING

Description: Worker Input Event Queue large

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_EVT_PACKAGER_COND_WAIT_ERROR

Description: FortiSIEM Event Packager Conditional Wait Error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_EVT_PACKAGER_FILE_CLOSE_FAILURE

Description: FortiSIEM Event Packager file close error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_EVT_PACKAGER_FILE_OPEN_FAILURE

Description: FortiSIEM Event Packager file open error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVT_PACKAGER_FILE_REMOVE_FAILURE

Description: FortiSIEM Event Packager file remove error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_EVT_PACKAGER_FILE_RENAME_FAILURE

Description: FortiSIEM Event Packager file rename error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	

EventType: PH_EVT_PACKAGER_FILE_STAT_FAILURE

Description: FortiSIEM Event Packager file stat error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_EVT_PACKAGER_FILE_UPLOAD_FAILURE

Description: FortiSIEM Event Packager file upload failure

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_EVT_PACKAGER_HTTP_RESPONSE_ERROR

Description: FortiSIEM Event Packager http response error from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_EVT_PACKAGER_INIT_FAILURE

Description: FortiSIEM Event Packager module initialization error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_EVT_PACKAGER_REST_PARSE_ERROR

Description: FortiSIEM Event Packager module failed to parse REST output

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVT_PACKAGER_RUN_PROCESS_ERROR

Description: FortiSIEM Event Packager module encountered error to run process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_APPSERVER_CONN_ERROR

Description: FSM FSM Java Agent failed to connect to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_APPSERVER_EXECUTE_ERROR

Description: FSM FSM Java Agent app server JMX Pull SQL Error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CONTROLLER_CMD_PARSE_ERROR

Description: FSM Java Agent parse file failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CONTROLLER_CMD_READ_ERROR

Description: FSM Java Agent control channel problem, exiting ...

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CONTROLLER_GENERIC_ERROR

Description: FSM Java Agent parse file failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CONTROLLER_LINE_READ_ERROR

Description: FSM Java Agent hit exception while reading line type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CONTROLLER_XML_READ_ERROR

Description: FSM Java Agent hit exception while reading command XML from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CUSTOM_JDBC_CONN_ERROR

Description: FSM Java Agent failed to execute custom JDBC monitoring job - connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CUSTOM_JDBC_EXEC_ERROR

Description: FSM Java Agent failed to execute custom JDBC monitoring job - execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_DISCOVERY_TEST_ERROR

Description: FSM Java Agent failed to connect to Snort database for testing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ERROR

Description: PH java agent generic error

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_GLASSFISH_MONITOR_ERROR

Description: FSM Java Agent GlassFish monitoring failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_GLASS_FISH_WARNING

Description: FSM Java Agent GlassFish monitoring warning

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_GOOGLEAPPS_EXEC_ERROR

Description: FSM Java Agent Google Apps Monitor Exception

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_IBMDB2_AUDIT_CONN_ERROR

Description: FSM Java Agent IBM DB2 connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_IBMDB2_AUDIT_EXEC_ERROR

Description: FSM Java Agent IBM DB2 audit error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_IBM_DB2_CAT_READ_ERROR

Description: FSM Java Agent IBM loading error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_IBM_DB2_CONN_ERROR

Description: FSM Java Agent failed to connect to IBM DB2 for collecting audit logs

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_IBM_DB2_INTERNAL_ERROR

Description: FSM Java Agent IBM Sleep Interrupted error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_INFO

Description: PH java agent generic info

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JBOSS_CONN_ERROR

Description: FSM Java Agent app server connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JBOSS_EXEC_ERROR

Description: FSM Java Agent app server connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JBOSS_MONITOR_ERROR

Description: Fail to monitor Jboss

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JDBC_PULL_UNSUPP_ERROR

Description: No connection for job when pulling JDBC

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JDBC_SQL_NOT_SUPPORT_ERROR

Description: FSM Java Agent cannot support such a SQL

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JMX_CONN_ERROR

Description: FSM Java Agent jmx JDBC error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JMX_EXEC_ERROR

Description: FSM Java Agent JMX monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JOB_EXECUTOR_ERROR

Description: Exception in AgentJobExecutor.run error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JOB_STATUS_UPLOAD_ERROR

Description: Failed to upload job status xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JOB_TYPE_ERROR

Description: AgentUtils createAndInitAgent serverType is not defined

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JOB_XML_LOAD_ERROR

Description: Exception caught while parsing JobXml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JOB_XML_PARSE_ERROR

Description: Exception caught while parsing JobXml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MCAFEE_MYSQL_MONITOR_ERROR

Description: FSM Java Agent my sql performance monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MCAFEE_VULN_SCANNER_ERROR

Description: FSM Java Agent vulnerability pulling error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MONITOR_GEN_ERROR

Description: FSM Java Agent job monitor rest error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MONITOR_TIMEOUT_ERROR

Description: FSM Java Agent job monitor execute too long

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MSSQL_DDL_CONN_ERROR

Description: FSM Java Agent JDBC pull don't support dev error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MSSQL_LOGON_CONN_ERROR

Description: FSM Java Agent MySql Connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MSSQL_LOGON_EXEC_ERROR

Description: FSM Java Agent app server JMX Pull SQL Error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MSSQL_MONITOR_ERROR

Description: FSM Java Agent ms sql performance error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MSSQL_PERF_CONN_ERROR

Description: FSM Java Agent job connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MSSQL_PERF_EXECUTE_ERROR

Description: FSM Java Agent MSSQL job execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MYSQL_PERF_CONN_ERROR

Description: FSM Java Agent MYSQL connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MYSQL_PERF_EXEC_ERROR

Description: FSM Java Agent mysql audit performance error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_NESSUS_REPORT_PARSE_ERROR

Description: FSM Java Agent nessus report parse error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ORACLE_DB_ERROR

Description: FSM Java Agent Oracle DB performance metrics error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ORADB_AUDIT_CONN_ERROR

Description: FSM Java Agent Oracle DB connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ORADB_AUDIT_EXEC_ERROR

Description: FSM Java Agent Oracle DB execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ORADB_LOGON_EXEC_ERROR

Description: FSM Java Agent Oracle Audit trail pull error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ORADB_PERF_CONN_ERROR

Description: FSM Java Agent Oracle Database performance metrics collection error - connection issue

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ORADB_PERF_EXEC_ERROR

Description: FSM Java Agent Oracle Database performance metrics collection error - SQL exec error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_SNORT_CONN_ERROR

Description: FSM Java Agent Snort IPS connect error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_SNORT_EVENTID_ERROR

Description: FSM Java Agent Snort IPS alert collection error - exception in setMaxEventId function

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_SNORT_EXEC_ERROR

Description: FSM Java Agent Snort IPS alert collection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_SNORT_SENSORID_ERROR

Description: FSM Java Agent Snort IPS alert collection error - exception in setSensorId2MaxEventId function

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_SNORT_TCP_OPTION_ERROR

Description: FSM Java Agent Snort IPS alert collection error - exception in getTcpOptions functions

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_TOMCAT_MONITOR_ERROR

Description: FSM Java Agent Tomcat Application Server monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_UTILS_ERROR

Description: FSM Java Agent status file error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_HWSTATUS_EXEC_ERROR

Description: FSM Java Agent failed to collect VMWare ESX hardware status

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_LOG_CONN_ERROR

Description: FSM Java Agent failed to connect VMWare ESX / Vcenter for collecting logs

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_LOG_EXEC_ERROR

Description: FSM Java Agent hit an exception while collecting logs from VMWare ESX / Vcenter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_MONITOR_ERROR

Description: FSM Java Agent hit an error while connecting to VMWare ESX / Vcenter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_COUNTER_MISSING

Description: FSM Java Agent VMWare performance pull error - missing performance counter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_DATA_RETRIEVE_ERROR

Description: FSM Java Agent VMWare performance pull error - data retrieve error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_ENTITY_MISSING

Description: FSM Java Agent VMWare performance pull error - missing performance entity

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_HOST_MISSING

Description: FSM Java Agent VMWare performance pull error - missing host

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_MON_EXCEPTION

Description: FSM Java Agent VMWare performance pull error - hit exception

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_ROLLUP_MISSING

Description: FSM Java Agent VMWare performance pull error - missing rollup

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_STAT_NAME_MISSING

Description: FSM Java Agent VMWare performance pull error - missing stat name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_VM_MISSING

Description: FSM Java Agent VMWare performance pull error - missing VM

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_THREAD_EXEC_ERROR

Description: FSM Java Agent VMWare performance pull error - thread execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VULN_REPORT_PARSER_ERROR

Description: FSM Java Agent failed to parse external vulnerability scanner report

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VULN_REPORT_VERIFY_ERROR

Description: FSM Java Agent failed to verify external vulnerability scanner report

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBLOGIC_MONITOR_ERROR

Description: FSM Java Agent Weblogic monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSENSE_EMAIL_MISSING_LOGDB

Description: FSM Java Agent Websense Email Gateway log collection error - logDBName is null

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSENSE_JDBC_PULL_ERROR

Description: FSM Java Agent Websense WebSecurity Gateway log collection error - Event Pull SQL Error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSENSE_MAIL_CONN_ERROR

Description: FSM Java Agent Websense Email Gateway connection audit error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSENSE_MAIL_EXEC_ERROR

Description: FSM Java Agent Websense Email Gateway execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSENSE_MAIL_PULL_ERROR

Description: FSM Java Agent Websense Email Gateway mail pulling error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSENSE_WEB_CONN_ERROR

Description: FSM Java Agent WebSecurity Gateway connection audit error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSENSE_WEB_EXEC_ERROR

Description: FSM Java Agent WebSecurity execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSENSE_WEB_MISSING_LOGDB

Description: FSM Java Agent WebSecurity log collection error - logDBName or urlDBName or urlCategoryDBName or dispositionDBName is null

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSPHERE_CONN_ERROR

Description: FSM Java Agent IBM Web sphere monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSPHERE_EXEC_ERROR

Description: FSM Java Agent IBM Web sphere log pulling error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSPHERE_MONITOR_ERROR

Description: FSM Java Agent IBM Web sphere monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_ACCOUT_MISSING

Description: Registration user name is missing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_BIND_PORT_FAILED

Description: Socket failed to bind port

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_LINUX_AGENT_CONFIG_ATTR_DECRYPTED_FAILED

Description: Failed to decrypt attr in config file.

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_LINUX_AGENT_CONFIG_ATTR_ENCRYPTED_FAILED

Description: Failed to encrypt attr in config file.

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_LINUX_AGENT_CONFIG_ATTR_NOT_FOUND

Description: Cannot find attribute in config file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_LINUX_AGENT_CONFIG_MISS_ATTR

Description: Cannot find attribute in config file

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_LINUX_AGENT_CREATE_SOCKET_FAILED

Description: Failed to create socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LINUX_AGENT_EXIT

Description: Linux agent received exit signal

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_HOST_IP_GOT_FAILED

Description: Failed to get host ip

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_INCREASE_RECV SOCK_BUF_MAX_FAILED

Description: Failed to increase Linux Agent recv socket buffe size

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_INIT_FIM_FAILED

Description: Linux Agent FIM Init Failed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LINUX_AGENT_INIT_HTTP_FAILED

Description: Failed to initial http client

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_LINUX_AGENT_LOG_GENERIC

Description: Linux agent generic log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_NEW_FIM_LOADED

Description: Linux Agent New FIM Config Loaded

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_OPEN_FILE_FAILED

Description: Linux agent open file failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LINUX_AGENT_OPEN_PORT_FAILED

Description: Failed to open port

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ipPort	IP Port	uint16	IP port number

EventType: PH_LINUX_AGENT_PWD_MISSING

Description: Registration password is missing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_RECV_ERROR

Description: Linux agent received error from socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.

EventType: PH_LINUX_AGENT_REGISSTER_FAILED

Description: Failed to register linux agent

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_TEMPLATE_STATUS

Description: Linux Agent State

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
status	Status	string	

EventType: PH_LINUX_AGENT_UNINSTALL

Description: Linux agent received uninstall signal

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_UPLOAD_FILE_FAILED

Description: File Upload to destHost failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_LINUX_AGENT_UPLOAD_FILE_SUCCESS

Description: File is uploaded to collector successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_LINUX_AGENT_USER_FILE_LOG_GENERIC

Description: Linux agent generic user file log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_VERIFIER_ERROR

Description: Linux agent verifier error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
size	Size	uint32	

EventType: PH_NETFLOW_BAD_FLOW

Description: Parser module module received a netflow packet with wrong length

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_FLOW_END

Description: Parser module received a netflow packet with unsupported end of netflow datagram

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_HEADER_PROTOCOL

Description: Parser module received a netflow packet with unsupported netflow header protocol

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_PACKET

Description: Parser module received a incorrectly formatted netflow packet

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_RECORD

Description: Parser module received a incorrectly formatted netflow flow

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_TYPE

Description: Parser module received a netflow packet with unsupported netflow sample type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_VER

Description: Parser module received a netflow packet with unsupported netflow version

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_NETFLOW_EXCEPTION

Description: Parser module encountered netflow parsing error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DEVAPP_EVENTS_PER_SEC

Description: FortiSIEM per application EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptVendor	Reporting Vendor	string	This field captures the vendor of the reported event
reptModel	Reporting Model	string	This field captures the model of the reported event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_SYSTEM_DEVAPP_NO_EVENTS

Description: No events from a reporting module in last 1 hour

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptVendor	Reporting Vendor	string	This field captures the vendor of the reported event
reptModel	Reporting Model	string	This field captures the model of the reported event
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.

EventType: PH_SYSTEM_DEVICE_NO_EVENTS

Description: No events from a device in last 1 hour

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_EPS_GLOBAL

Description: FortiSIEM Global event handling statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
licenseEventsPerSec	License EPS	uint64	
incomingEventsPerSec	Incoming Event Rate	double	This is a FortiSIEM event ingestion rate calculated every 3 minutes, divided by 180 to generate a rolling EPS (Events Per Second) interval.
peakIncomingEventsPerSec	Peak Incoming Event Rate	double	This is the spike or max event ingestion rate seen during a 3 minute interval averaged overall data points.
dropLicenseEventsPerSec	License Dropped Event Rate	double	The number of events dropped due to exceeding license in past 3 minutes.
peakDropLicenseEventsPerSec	Peak License Dropped Event Rate	double	The max value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.
unusedEvents	Unused Event Count	uint64	The difference between licenseEventsPerSec and incomingEventsPerSec accumulated.

EventType: PH_SYSTEM_EPS_NODE

Description: FortiSIEM per Node event handling statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
role	Role	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
guaranteedEventsPerSec	Guaranteed EPS	uint64	
incomingEventsPerSec	Incoming Event Rate	double	This is a FortiSIEM event ingestion rate calculated every 3 minutes, divided by 180 to generate a rolling EPS (Events Per Second) interval.
peakIncomingEventsPerSec	Peak Incoming Event Rate	double	This is the spike or max event ingestion rate seen during a 3 minute interval averaged overall data points.
ingestedEventsPerSec	Ingested Event Rate	double	
dropPolicyEvents	Policy Dropped Events	uint64	The number of events dropped by Event Dropping Rules in the last 3 minutes.
dropPolicyEventsPerSec	Policy Droppped Event Rate	double	This is the per second count of events dropped by policy, which is calculated as dropPolicyEvents (3min interval) / 180 seconds.
peakDropPolicyEventsPerSec	Peak Policy Dropped Event Rate	double	The max value of dropPolicyEventsPerSec, over all 3-minute periods, since phParser started.
dropLicenseEvents	License Dropped Events	uint64	This is the total count of events dropped due to exceeding license over all 3 minute intervals since phParser started.
dropLicenseEventsPerSec	License Dropped Event Rate	double	The number of events dropped due to exceeding license in past 3 minutes.
peakDropLicenseEventsPerSec	Peak License Dropped Event Rate	double	The max value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.
dropLicenseEventRatio	License Dropped Event Ratio	uint16	Ratio of dropped events due to license to total incoming events in last 3 minutes.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_SYSTEM_EPS_ORG

Description: FortiSIEM per Organization event handling statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
incomingEventsPerSec	Incoming Event Rate	double	This is a FortiSIEM event ingestion rate calculated every 3 minutes, divided by 180 to generate a rolling EPS (Events Per Second) interval.
peakIncomingEventsPerSec	Peak Incoming Event Rate	double	This is the spike or max event ingestion rate seen during a 3 minute interval averaged overall data points.
dropLicenseEventsPerSec	License Dropped Event Rate	double	The number of events dropped due to exceeding license in past 3 minutes.
peakDropLicenseEventsPerSec	Peak License Dropped Event Rate	double	The max value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.

EventType: PH_SYSTEM_EVENTS_FWD_STAT

Description: Forwarded EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
role	Role	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.

Id	Display name	Type	Description
fwdEventsPerSec	Forwarded Event Rate	double	This field represents the average rate (events per sec) over a 3 minute window, at which events are forwarded from FortiSIEM to an external system
peakFwdEventsPerSec	Peak Forwarded Event Rate	double	This field represents the maximum rate (events per sec) over a 3 minute window, at which events are forwarded from FortiSIEM to an external system
dropFwdEventsPerSec	Dropped Forwarded Event Rate	double	
peakDropFwdEventsPerSec	Peak Dropped Forwarded Event Rate	double	
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.

EventType: PH_SYSTEM_EVENTS_PER_SEC

Description: Received EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
peakEventsPerSec	Peak Event Rate	double	
guaranteedEventsPerSec	Guaranteed EPS	uint64	

EventType: PH_SYSTEM_EVENTS_VIA_ZMQ_EPS

Description: Events Pushed by ZMQ EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totEventCount	Total Event Count	uint32	
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_SYSTEM_INTERNAL_EVENTS_PER_SEC

Description: FortiSIEM Internal EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
peakEventsPerSec	Peak Event Rate	double	

EventType: PH_SYSTEM_IP_EVENTS_PER_SEC

Description: FortiSIEM per device EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_SYSTEM_PERF_EVENTS_PER_SEC

Description: FortiSIEM performance monitoring EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
peakEventsPerSec	Peak Event Rate	double	

EventType: PH_SYSTEM_STORED_EVENTS_PER_SEC

Description: Stored EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
peakEventsPerSec	Peak Event Rate	double	

EventType: PH_SYSTEM_SUMM_EVENTS_STORED_EPS

Description: Summary Events Stored EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totEventCount	Total Event Count	uint32	
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_VA_EVENTS_PER_SEC

Description: Total event rate to an FortiSIEM VA

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
peakEventsPerSec	Peak Event Rate	double	

Identity and Location Logs

This section provides related to Identity and Location discovery

- [PH_IDENTITYMASTER_HTTP_UPLOAD_ERROR](#)
- [PH_IDENTITYMASTER_INIT_ERROR](#)
- [PH_IDENTITYWORKER_ATTRIB_ERROR](#)
- [PH_IDENTITYWORKER_EVT_LOAD_ERROR](#)
- [PH_IDENTITYWORKER_EVT_SEND_ERROR](#)
- [PH_IDENTITYWORKER_INIT_ERROR](#)
- [PH_IDENTITYWORKER_PARAM_ERROR](#)
- [PH_IDENTITYWORKER_PROCESSING_EPS](#)
- [PH_IDENTITYWORKER_SS_OBTAIN_ERROR](#)

EventType: PH_IDENTITYMASTER_HTTP_UPLOAD_ERROR

Description: Identity Master failed to upload identity location information to App server

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_IDENTITYMASTER_INIT_ERROR

Description: Identity Master initialization error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_IDENTITYWORKER_ATTRIB_ERROR

Description: Identity Worker found invalid event attribute in identityDef.xml

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_IDENTITYWORKER_EVT_LOAD_ERROR

Description: Identity Worker failed to load event from shared store

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_IDENTITYWORKER_EVT_SEND_ERROR

Description: Identity Worker failed to send event to Identity Master

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.

EventType: PH_IDENTITYWORKER_INIT_ERROR

Description: Identity Worker initialization error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_IDENTITYWORKER_PARAM_ERROR

Description: Identity Worker configuration parameter undefined in phoenix_config.txt

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_IDENTITYWORKER_PROCESSING_EPS

Description: IP Identity Worker EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_IDENTITYWORKER_SS_OBTAIN_ERROR

Description: Identity Worker failed to create shared store

Severity: 10 (High)

Event Category: 3 (System Logs)

License Logs

This section provides logs related to licensing.

- [PH_CLUSTER_NO_LICENSE](#)
- [PH_COLLECTOR_LICENSE_UPDATE](#)
- [PH_LICENSE_ERROR](#)
- [PH_LICENSE_INFO_FAILURE](#)
- [PH_LICENSE_INFO_INVALIDATED](#)
- [PH_LICENSE_NOT_EXIST](#)
- [PH_MODULE_LICENSE_FAILURE](#)
- [PH_MONITOR_LICENSE_ERROR](#)
- [PH_MONITOR_QUERY_LICENSE_FAILED](#)
- [PH_MONITOR_REPORTSERVER_LICENSE_INVALID](#)
- [PH_PARSER_GLOBAL_LICENSE_EXCEED](#)
- [PH_SYSTEM_DISK_USAGE_EXCEED_LICENSE](#)
- [PH_SYSTEM_EVENT_RATE_EXCEED_LICENSE](#)
- [PH_TASK_NO_LICENSE](#)
- [PH_VA_LICENSE_UPDATE](#)

EventType: PH_CLUSTER_NO_LICENSE

Description: 670-Cluster: There is no license

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_COLLECTOR_LICENSE_UPDATE

Description: License on collector updated

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LICENSE_ERROR

Description: FortiSIEM discovered license parsing error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LICENSE_INFO_FAILURE

Description: Failed to get license info

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LICENSE_INFO_INVALIDATED

Description: Invalid license

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LICENSE_NOT_EXIST

Description: There is no license file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MODULE_LICENSE_FAILURE

Description: Module failed to get license

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_LICENSE_ERROR

Description: phMonitor encountered license file error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_QUERY_LICENSE_FAILED

Description: Follower Super query license failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_REPORTSERVER_LICENSE_INVALID

Description: phMonitor found invalid Report Server license

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_GLOBAL_LICENSE_EXCEED

Description: Global EPS license exceeded and events will be dropped

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
licenseEventsPerSec	License EPS	uint64	

EventType: PH_SYSTEM_DISK_USAGE_EXCEED_LICENSE

Description: Event database disk usage exceeded limit

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_SYSTEM_EVENT_RATE_EXCEED_LICENSE

Description: System event rate exceeds licensed event rate

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_TASK_NO_LICENSE

Description: There is no license

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_VA_LICENSE_UPDATE

Description: License on VA has been updated

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Parser Logs

This section provides logs related to parsing of events/logs

- PH_EVENT_ATTR_XML_ISSUE
- PH_LIBEVENT_BUFFER_OVERFLOW
- PH_LIBEVENT_IP_TYPE_INVALID
- PH_LIBEVENT_UNKNOWN_ATTR_ID
- PH_LIBEVENT_UNKNOWN_ATTR_NAME
- PH_NO_PARSER_FOR_EVENT
- PH_PARSER_BIND_PORT_FAILURE
- PH_PARSER_DATA_SIZE_OVERFLOW
- PH_PARSER_DIR_OPEN_FAILURE
- PH_PARSER_EVENT_PARSER_ERROR
- PH_PARSER_EVENT_SERIALIZE_ERROR
- PH_PARSER_FILE_DELETE_FAILURE
- PH_PARSER_FILE_DELETE_FAILURE_RENAME
- PH_PARSER_FILE_INVALID_FORMAT
- PH_PARSER_FILE_INVALID_HEADER
- PH_PARSER_FILE_NOT_EXIST
- PH_PARSER_FILE_OPEN_FAILURE
- PH_PARSER_FILE_PARSE_FAILURE
- PH_PARSER_FILE_READ_FAILURE
- PH_PARSER_FILE_RENAME_FAILURE
- PH_PARSER_FILE_SIZE_MISMATCH
- PH_PARSER_FILE_STAT_FAILURE
- PH_PARSER_FILE_WRITE_FAILURE
- PH_PARSER_GEO_WRONG_ATTR_NUMBER
- PH_PARSER_GEO_WRONG_CACHE_NUMBER
- PH_PARSER_GET_PROCESS_ERROR
- PH_PARSER_HTTP_RESPONSE_ERROR
- PH_PARSER_HTTP_UPLOAD_FAILURE
- PH_PARSER_INIT_DEV_CRED_FAILED
- PH_PARSER_INIT_FAILURE
- PH_PARSER_INVALID_CSV
- PH_PARSER_INVALID_EXT_LOG_PROTO
- PH_PARSER_INVALID_ORG_NAME
- PH_PARSER_INVALID_PHOENIX_CONFIG
- PH_PARSER_IP_TYPE_INVALID
- PH_PARSER_JSON_PARSE_FAILURE
- PH_PARSER_MALLOC_FAILURE

- PH_PARSER_PACK_EVENT_ERROR
- PH_PARSER_RAWEVENT_TOO_LARGER
- PH_PARSER_REST_PARSE_ERROR
- PH_PARSER_RUN_PROCESS_ERROR
- PH_PARSER_SEND_EVENT_FAILURE
- PH_PARSER_SEND_TO_DISCOV_FAILURE
- PH_PARSER_SEND_TO_MONITOR_FAILURE
- PH_PARSER_SET_USER_ID_FAILURE
- PH_PARSER_SHARED_STORE_ERROR
- PH_PARSER_SNMPTRAP_INIT_FAILURE
- PH_PARSER_SOCKET_ERROR
- PH_PARSER_SOCKET_RECV_ERROR
- PH_PARSER_SOCKET_SELECT_ERROR
- PH_PARSER_SPAWN_THREAD_FAILURE
- PH_PARSER_SSL_ACCEPT_ERROR
- PH_PARSER_SSL_CERT_LOAD_ERROR
- PH_PARSER_TCP_SOCKET_ACCEPT_ERROR
- PH_PARSER_TEST_RULES_PARSE_ALL_EVENTS_BEGIN
- PH_PARSER_TEST_RULES_PARSE_ALL_EVENTS_END
- PH_PARSER_TEST_RULES_PARSE_ONE_EVENT_BEGIN
- PH_PARSER_TEST_RULES_PARSE_ONE_EVENT_END
- PH_PARSER_TOO_MANY_UNKNOWN_EVENTS
- PH_PARSER_UPDATE_FAILURE
- PH_PARSER_USE_ERROR_BEFORE_INIT
- PH_PARSER_WRONG_EVENT_SIZE
- PH_PARSER_WRONG_PARAMETER
- PH_PARSER_WTAP_ERR_BAD_FILE
- PH_PARSER_WTAP_ERR_CANT_OPEN
- PH_PARSER_WTAP_ERR_COMPRESSION_NOT_SUPPORTED
- PH_PARSER_WTAP_ERR_DECOMPRESS
- PH_PARSER_WTAP_ERR_ENCAP_PER_PACKET_UNSUPPORTED
- PH_PARSER_WTAP_ERR_FILE_UNKNOWN_FORMAT
- PH_PARSER_WTAP_ERR_NOT_REGULAR_FILE
- PH_PARSER_WTAP_ERR_RANDOM_OPEN_PIPE
- PH_PARSER_WTAP_ERR_SHORT_READ
- PH_PARSER_WTAP_ERR_SHORT_WRITE
- PH_PARSER_WTAP_ERR_UNSUPPORTED
- PH_PARSER_XML_PARSE_ERROR
- PH_PARSER_XML_PARSE_FAILURE
- PH_PARSE_CONFIG_CHANGE_FAILED
- PH_VULN_LOAD_ERROR
- PH_VULN_UPDATE_ERROR

EventType: PH_EVENT_ATTR_XML_ISSUE

Description: Event attribute xml issue

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIBEVENT_BUFFER_OVERFLOW

Description: FortiSIEM module encountered error while reading events from shared buffer

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIBEVENT_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIBEVENT_UNKNOWN_ATTR_ID

Description: Query/Report/Rule module encountered unknown event attribute id

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIBEVENT_UNKNOWN_ATTR_NAME

Description: Query/Report/Rule module encountered unknown event attribute name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NO_PARSER_FOR_EVENT

Description: No parser available for event

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventName	Event Name	string	This is the eventType display name, or human readable name. In many cases the eventType is sufficiently labeled.

EventType: PH_PARSER_BIND_PORT_FAILURE

Description: Parser module failed to bind to a TCP/UDP ports

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_DATA_SIZE_OVERFLOW

Description: Data size exceeding capacity

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_DIR_OPEN_FAILURE

Description: Parser module failed to open directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_PARSER_EVENT_PARSER_ERROR

Description: Parser module failed to parse event parsing xml from local disk or App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
tagName	Tag Name	string	
parserName	Event Parser Name	string	The name of parser that parsed the event
funName	Function Name	string	

EventType: PH_PARSER_EVENT_SERIALIZE_ERROR

Description: Parser module failed to serialize event before writing to shared buffer

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_FILE_DELETE_FAILURE

Description: Parser module failed to delete file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_FILE_DELETE_FAILURE_RENAME

Description: Parser module failed to delete file but succeeded to rename. These files may fill up disk

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_FILE_INVALID_FORMAT

Description: Parser module failed to parse event or metadata files with invalid file format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_FILE_INVALID_HEADER

Description: Parser module failed to parse event files with invalid file header

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_FILE_NOT_EXIST

Description: File doesn't exist

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_FILE_OPEN_FAILURE

Description: Parser module failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_FILE_PARSE_FAILURE

Description: Failed to parse file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_FILE_READ_FAILURE

Description: Parser module failed to read file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_FILE_RENAME_FAILURE

Description: Parser module failed to rename file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_FILE_SIZE_MISMATCH

Description: Parser module ignored event file from collector because of file size mismatch

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_FILE_STAT_FAILURE

Description: Parser module failed to obtain file status and will skip the file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_FILE_WRITE_FAILURE

Description: Parser module failed to write file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_GEO_WRONG_ATTR_NUMBER

Description: Parser module internal error - mismatched GEO attribute count

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_GEO_WRONG_CACHE_NUMBER

Description: Parser module internal error - incorrect GEO cache attribute count

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_GET_PROCESS_ERROR

Description: Parser module failed to get own process information

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_HTTP_RESPONSE_ERROR

Description: Parser module failed to get response from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_PARSER_HTTP_UPLOAD_FAILURE

Description: Parser module failed to upload information to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_INIT_DEV_CRED_FAILED

Description: Failed to initialize device credential

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_INIT_FAILURE

Description: Parser module failed to initialize

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_INVALID_CSV

Description: Parser module failed to load CSV file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_INVALID_EXT_LOG_PROTO

Description: Parser module encountered unsupported external log receive protocol

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_INVALID_ORG_NAME

Description: Parser module received invalid organization in event

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.

EventType: PH_PARSER_INVALID_PHOENIX_CONFIG

Description: Parser module found incorrectly formatted phoenix config file entry

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	
configName	Config Name	string	
configValue	Config Value	string	

EventType: PH_PARSER_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_JSON_PARSE_FAILURE

Description: Parser module failed to parse Json

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
jsonBody	JSON Body	string	

EventType: PH_PARSER_MALLOC_FAILURE

Description: Parser module failed to dynamically allocate memory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_PACK_EVENT_ERROR

Description: Parser module failed to pack event before sending to other modules for internal communication

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_PARSER_RAWEVENT_TOO_LARGER

Description: Raw event's size is more than 10M. Save it to tmp file and not send to parser

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_REST_PARSE_ERROR

Description: Parser module failed to parse REST api from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_RUN_PROCESS_ERROR

Description: Parser module failed to start

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_SEND_EVENT_FAILURE

Description: Parser module failed to send event

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_SEND_TO_DISCOV_FAILURE

Description: Parser module failed to send internal event to discovery module

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_SEND_TO_MONITOR_FAILURE

Description: Parser module failed to send internal event to Supervisor phMonitor process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_SET_USER_ID_FAILURE

Description: Parser module unable to set effective user ID

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_SHARED_STORE_ERROR

Description: FortiSIEM Parser module encountered shared store error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_SNMPTRAP_INIT_FAILURE

Description: Parser module failed to initialize snmptrap

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_SOCKET_ERROR

Description: Parser module failed to open socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_SOCKET_RECV_ERROR

Description: Parser module failed to receive message via socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_SOCKET_SELECT_ERROR

Description: Parser module failed to select in socket API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_SPAWN_THREAD_FAILURE

Description: Parser module failed to spawn thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_PARSER_SSL_ACCEPT_ERROR

Description: Parser module failed to accept SSL connection

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_SSL_CERT_LOAD_ERROR

Description: Parser module failed to load SSL certificate

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_TCP_SOCKET_ACCEPT_ERROR

Description: Failed to accept connect

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_TEST_RULES_PARSE_ALL_EVENTS_BEGIN

Description: Parser beginning to parse all events

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_PARSER_TEST_RULES_PARSE_ALL_EVENTS_END

Description: Parser finished parsing all events

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_PARSER_TEST_RULES_PARSE_ONE_EVENT_BEGIN

Description: Event parsing begins

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_PARSER_TEST_RULES_PARSE_ONE_EVENT_END

Description: Event parsing ends

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventId	Event ID	uint64	This is a globally unique ID assigned to every raw event ingested into the SIEM. This is used by the system for tying events to incidents, and is typically not needed by end users.

EventType: PH_PARSER_TOO_MANY_UNKNOWN_EVENTS

Description: Too many unknown events

Notes: This event is generated by the phParser process running on a FortiSIEM node when too many unknown events are received from a single source IP (Reporting IP). Unknown events implies that there is no matching parser to parse those events. The thresholds are defined in /opt/phoenix/config/phoenix_config.txt.

[BEGIN PHPARSER]

unknown_event_skip_eps=20

unknown_event_skip_size=10240 # 10kB

[END PHPARSER]

The explanation of these attributes is as follows. The attribute `unknown_event_skip_eps` is used to calculate the maximum number of allowed unparsed events from a source. The attribute `unknown_event_skip_size` is used to calculate the maximum size of allowed unparsed raw events from a source.

The window for detecting excessive unknown events in 3 minutes (or 180 seconds). In this window:

- the maximum number of allowed unparsed events from a single source is `unknown_event_skip_eps` times 180, and
- the maximum cumulative raw event size (in bytes) of all unparsed events from a single source is `unknown_event_skip_size`.

For example: For `unknown_event_skip_eps=20` and `unknown_event_skip_size=10240`, if either 3600 unknown events is received from one source or the total size of unknown events from one source reaches 10kB in a 3 minute window, then the event `PH_PARSER_TOO_MANY_UNKNOWN_EVENTS` is generated and parsing stops for that reporting IP for the remainder of the 3 minute window. Once the 3 minute window expires, the restriction is lifted and events from that IP are parsed again. If the condition happens again in the new window, then the same action is taken as the previous window.

This action is taken to reduce the load on the parser module in the case of excessive unknown events. Increasing the values of `unknown_event_skip_eps` and `unknown_event_skip_size` may have a performance impact on the CPU and memory consumption by the parser module on that FortiSIEM node.

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
relayDevIpAddr	Relaying IP	IP	Relaying IP is most commonly used to specify the log relay appliance, usually a collector.

EventType: PH_PARSER_UPDATE_FAILURE

Description: Parser module failed to update internal information from REST API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_USE_ERROR_BEFORE_INIT

Description: Parser module attempted to use an object before initialization

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_WRONG_EVENT_SIZE

Description: FortiSIEM module failed to load serialized event

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_WRONG_PARAMETER

Description: Parser module encountered wrong parameter during event parsing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id				Display name				Type				Description			
funName				Function Name				string							
paraName				Param Name				string							
parserName				Event Parser Name				string				The name of parser that parsed the event			

EventType: PH_PARSER_WTAP_ERR_BAD_FILE

Description: The file is damaged or corrupt

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id				Display name				Type				Description			
filePath				File Path				string							
errorString				Error String				string				This is the error message, synonymous to attribute errReason			

EventType: PH_PARSER_WTAP_ERR_CANT_OPEN

Description: Parser module failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_COMPRESSION_NOT_SUPPORTED

Description: Parser module failed to write this file type as a compressed file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_DECOMPRESS

Description: The compressed file appears to be damaged or corrupt

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_WTAP_ERR_ENCAP_PER_PACKET_UNSUPPORTED

Description: Parser module doesn't support the network type in the file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_FILE_UNKNOWN_FORMAT

Description: Parser module doesn't support this file format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_NOT_REGULAR_FILE

Description: Parser module failed to parse a special file or socket or other non-regular file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_RANDOM_OPEN_PIPE

Description: Parser module can't parse a pipe or FIFO files

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_SHORT_READ

Description: The file has been cut short in the middle of a packet

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_SHORT_WRITE

Description: Parser module failed to write a full header in the file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_UNSUPPORTED

Description: Parser module doesn't support record data in the file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_XML_PARSE_ERROR

Description: Parser module failed to parse generic xml document

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
tagName	Tag Name	string	
parserName	Event Parser Name	string	The name of parser that parsed the event

EventType: PH_PARSER_XML_PARSE_FAILURE

Description: Parser module failed to parse XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propName	Property Name	string	
propValue	Property Value	string	

EventType: PH_PARSE_CONFIG_CHANGE_FAILED

Description: FortiSIEM bRule/Report Master/Worker modules failed to parse performance monitoring config change

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_VULN_LOAD_ERROR

Description: Parser module failed to load external scanner-found vulnerabilities from App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_VULN_UPDATE_ERROR

Description: Parser module failed to upload external scanner-found vulnerabilities to App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

Performance and Availability Monitoring Logs

This section provides logs related to Performance and Availability Monitoring

- PH_DEV_MON_ACME_PACKET_SESSION_AGENT_STATUS
- PH_DEV_MON_ACME_PACKET_SYS_STATUS
- PH_DEV_MON_APP_APACHE_MET
- PH_DEV_MON_APP_ASPNET_MET
- PH_DEV_MON_APP_DHCP_MET
- PH_DEV_MON_APP_DNS_MET
- PH_DEV_MON_APP_ICA_SESS_MET
- PH_DEV_MON_APP_IIS_MET
- PH_DEV_MON_APP_MSEXCH_ERR_MET
- PH_DEV_MON_APP_MSEXCH_ISDB_INST_MET
- PH_DEV_MON_APP_MSEXCH_ISDB_MET
- PH_DEV_MON_APP_MSEXCH_MBOX_MET
- PH_DEV_MON_APP_MSEXCH_MET
- PH_DEV_MON_APP_MSEXCH_REPL_MET
- PH_DEV_MON_APP_MSEXCH_SMTP_MET
- PH_DEV_MON_APP_MSEXCH_STORE_INTF_MET
- PH_DEV_MON_APP_MSEXCH_SUBMIT_MET
- PH_DEV_MON_APP_MSEXCH_TRANS_MET
- PH_DEV_MON_APP_MSEXCH_WS_MET
- PH_DEV_MON_APP_NTDS_MET
- PH_DEV_MON_ARUBA_WLAN_RADIO_METRIC
- PH_DEV_MON_AUTH_STATS
- PH_DEV_MON_AUTO_SVC_START_TO_STOP
- PH_DEV_MON_AUTO_SVC_STOP
- PH_DEV_MON_AUTO_SVC_STOP_TO_START
- PH_DEV_MON_BC_PROXY_METRIC
- PH_DEV_MON_BGP_NBR_STATUS
- PH_DEV_MON_BOX_FILE_CREATE
- PH_DEV_MON_BOX_FILE_DELETE
- PH_DEV_MON_BOX_FILE_MODIFY
- PH_DEV_MON_BOX_FILE_SHARE
- PH_DEV_MON_CBQOS_CMSTAT
- PH_DEV_MON_CBQOS_POLICESTAT
- PH_DEV_MON_CBQOS_QUEUESTAT
- PH_DEV_MON_CCM_CTI_STAT
- PH_DEV_MON_CCM_CTI_STAT_CHANGE
- PH_DEV_MON_CCM_DEL_CTI

- PH_DEV_MON_CCM_DEL_GW
- PH_DEV_MON_CCM_DEL_H323
- PH_DEV_MON_CCM_DEL_MEDIA
- PH_DEV_MON_CCM_DEL_SIP_TRUNK
- PH_DEV_MON_CCM_DEL_VM
- PH_DEV_MON_CCM_GLOBAL_INFO
- PH_DEV_MON_CCM_GW_STAT
- PH_DEV_MON_CCM_GW_STAT_CHANGE
- PH_DEV_MON_CCM_H323_STAT
- PH_DEV_MON_CCM_H323_STAT_CHANGE
- PH_DEV_MON_CCM_MEDIA_STAT
- PH_DEV_MON_CCM_MEDIA_STAT_CHANGE
- PH_DEV_MON_CCM_NEW_CTI
- PH_DEV_MON_CCM_NEW_GW
- PH_DEV_MON_CCM_NEW_H323
- PH_DEV_MON_CCM_NEW_MEDIA
- PH_DEV_MON_CCM_NEW_SIP_TRUNK
- PH_DEV_MON_CCM_NEW_VM
- PH_DEV_MON_CCM_SIP_TRUNK_STAT
- PH_DEV_MON_CCM_VM_STAT
- PH_DEV_MON_CCM_VM_STAT_CHANGE
- PH_DEV_MON_CHANGE_CUST_CONFIG
- PH_DEV_MON_CHANGE_INST_SW
- PH_DEV_MON_CHANGE_RUN_CONFIG
- PH_DEV_MON_CHANGE_RUN_SW
- PH_DEV_MON_CHANGE_STARTUP_CONFIG
- PH_DEV_MON_CISCO_NBAR_STAT
- PH_DEV_MON_CISCO_RAS_VPN_MET
- PH_DEV_MON_CISCO_VPN_P1_TUNNEL_MET
- PH_DEV_MON_CISCO_VPN_P2_TUNNEL_MET
- PH_DEV_MON_CISCO_WLAN_RADIO_METRIC
- PH_DEV_MON_CITRIX_SDWAN_INTF
- PH_DEV_MON_CITRIX_SDWAN_LINK
- PH_DEV_MON_CLARION_ARRAY_UTIL
- PH_DEV_MON_CLARION_DISK_HEALTH
- PH_DEV_MON_CLARION_HOST_CONN
- PH_DEV_MON_CLARION_LUN_UTIL
- PH_DEV_MON_CLARION_PER_HOST_LUN_UTIL
- PH_DEV_MON_CLARION_PORT_UTIL
- PH_DEV_MON_CLARION_RG_UTIL
- PH_DEV_MON_CLARION_SP_UTIL
- PH_DEV_MON_CLARION_STORAGE_USAGE
- PH_DEV_MON_CLARION_STORE_POOL_UTIL

- PH_DEV_MON_CLARION_UNREG_HOST
- PH_DEV_MON_CLOUD_SERVICE_HEARTBEAT
- PH_DEV_MON_CMDB_DISK_PRUNE_FAILED
- PH_DEV_MON_CMDB_DISK_PRUNE_SUCCESS
- PH_DEV_MON_CUST_FILE_CHANGE_ATTRIB
- PH_DEV_MON_CUST_FILE_CHANGE_CONTENT
- PH_DEV_MON_CUST_FILE_CREATE
- PH_DEV_MON_CUST_FILE_DELETE
- PH_DEV_MON_CUST_FILE_SCAN
- PH_DEV_MON_CUST_TARGET_FILE_CHANGE
- PH_DEV_MON_DATASTORE_UTIL
- PH_DEV_MON_DCDIAG
- PH_DEV_MON_DDNS_UPDATE_STAT
- PH_DEV_MON_DELLFORCE10_EXT_INTF_UTIL
- PH_DEV_MON_DELL_BLADE_POWER_STATUS
- PH_DEV_MON_DELL_BLADE_PSU_STATUS
- PH_DEV_MON_DELTA_CONFIG
- PH_DEV_MON_DGA_DETECTED
- PH_DEV_MON_DHCP_SUBNET_USAGE
- PH_DEV_MON_DISK_IO_UTIL
- PH_DEV_MON_DISK_MON_SKIP
- PH_DEV_MON_DNS_CLUST_REPL_STAT
- PH_DEV_MON_DNS_PERF_STAT
- PH_DEV_MON_DNS_ZONETX_MET
- PH_DEV_MON_DST_AD_REPL_STAT
- PH_DEV_MON_EBS_METRIC
- PH_DEV_MON_EC2_INSTANCE_DOWN
- PH_DEV_MON_EC2_INSTANCE_UP
- PH_DEV_MON_EC2_METRIC
- PH_DEV_MON EMC_DATADOMAIN_DISK_PERF
- PH_DEV_MON EMC_DATADOMAIN_OVERALL_PERF
- PH_DEV_MON_EQL_CONN_MET
- PH_DEV_MON_EQL_DISK_HEALTH
- PH_DEV_MON_EQL_DISK_MET
- PH_DEV_MON_EQL_GROUP_MET
- PH_DEV_MON_ESX_DATASTORE_IO
- PH_DEV_MON_ESX_DISK_IO
- PH_DEV_MON_ESX_DISK_UTIL
- PH_DEV_MON_ESX_STATE
- PH_DEV_MON_ESX_UPTIME
- PH_DEV_MON_EUM_FAIL
- PH_DEV_MON_EUM_INTERNAL_ERR
- PH_DEV_MON_EUM_STATUS

- PH_DEV_MON_EUM_SUCCESS
- PH_DEV_MON_F5_ACTIVE_CONN
- PH_DEV_MON_F5_LTM_NODE_STAT
- PH_DEV_MON_F5_LTM_POOL_MEMBER_STAT
- PH_DEV_MON_F5_LTM_POOL_STAT
- PH_DEV_MON_F5_LTM_VIRT_ADDR_STAT
- PH_DEV_MON_F5_LTM_VIRT_SERVER_STAT
- PH_DEV_MON_F5_NEW_CONN
- PH_DEV_MON_F5_RAM_CACHE
- PH_DEV_MON_F5_THROUGHPUT
- PH_DEV_MON_F5_TMM_MEM_UTIL
- PH_DEV_MON_FGT_SEC_POSTURE_DETAILS
- PH_DEV_MON_FGT_SEC_POSTURE_DETECTED_ENDPOINTS
- PH_DEV_MON_FGT_SEC_POSTURE_FABRIC_GRADE
- PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_GRADE
- PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_STATS
- PH_DEV_MON_FGT_SEC_POSTURE_PER_DEVICE_STATS
- PH_DEV_MON_FGT_USER_INFO
- PH_DEV_MON_FILE_CONTENT_CHANGE
- PH_DEV_MON_FIREAMP_DISCOVERY_CLIENT_APP
- PH_DEV_MON_FIREAMP_DISCOVERY_NETWORK_PROTOCOL
- PH_DEV_MON_FIREAMP_DISCOVERY_OS_FINGERPRINT
- PH_DEV_MON_FIREAMP_DISCOVERY_SERVER
- PH_DEV_MON_FIREAMP_FILE
- PH_DEV_MON_FIREAMP_IMPACT_FLAG
- PH_DEV_MON_FIREAMP_INTRUSION
- PH_DEV_MON_FIREAMP_MALWARE
- PH_DEV_MON_FIREAMP_USER_LOGIN
- PH_DEV_MON_FORTIAP_INTF_UTIL
- PH_DEV_MON_FORTIAP_PERF
- PH_DEV_MON_FORTIAP_STAT
- PH_DEV_MON_FORTIGATE_INTF_UTIL
- PH_DEV_MON_FORTIGATE_PERF
- PH_DEV_MON_FORTIMAIL_SESSION_COUNT
- PH_DEV_MON_FORTIMAIL_SYS_LOAD
- PH_DEV_MON_FORTINET_PROCESSOR_USAGE
- PH_DEV_MON_FORTINET_QOS
- PH_DEV_MON_FORTISWITCH_PERF
- PH_DEV_MON_FORTIWLC_QOS_STAT
- PH_DEV_MON_FORTIWLC_STATIONS
- PH_DEV_MON_FORTIWLC_SYS_THRUPUT
- PH_DEV_MON_FPC_LIEBERT_METRIC
- PH_DEV_MON_FW_CONN_UTIL

- PH_DEV_MON_GITHUB_BRANCH_EVENT
- PH_DEV_MON_GITHUB_COMMIT
- PH_DEV_MON_GITHUB_EVENT
- PH_DEV_MON_GITHUB_FORK_REPOSITORY_EVENT
- PH_DEV_MON_GITHUB_ISSUE_EVENT
- PH_DEV_MON_GITHUB_MEMBER_EVENT
- PH_DEV_MON_GITHUB_ORG_EVENT
- PH_DEV_MON_GITHUB_PROJECT_EVENT
- PH_DEV_MON_GITHUB_PULL_REQUEST_EVENT
- PH_DEV_MON_GITHUB_PULL_REQUEST_REVIEW_EVENT
- PH_DEV_MON_GITHUB_REPOSITORY_EVENT
- PH_DEV_MON_GITHUB_TAG_EVENT
- PH_DEV_MON_GLASSFISH_APP
- PH_DEV_MON_GLASSFISH_CONN_STAT
- PH_DEV_MON_GLASSFISH_CPU
- PH_DEV_MON_GLASSFISH_DB_POOL
- PH_DEV_MON_GLASSFISH_EJB
- PH_DEV_MON_GLASSFISH_JMS
- PH_DEV_MON_GLASSFISH_MEMORY
- PH_DEV_MON_GLASSFISH_REQUEST_PROCESSOR
- PH_DEV_MON_GLASSFISH_SERVLET
- PH_DEV_MON_GLASSFISH_SESSION
- PH_DEV_MON_GLASSFISH_THREAD_POOL
- PH_DEV_MON_HARDWARE_STATUS
- PH_DEV_MON_HOST_PERF_STATE
- PH_DEV_MON_HVAC_LIEBERT_METRIC
- PH_DEV_MON_HW_AIRFLOW
- PH_DEV_MON_HW_AMP
- PH_DEV_MON_HW_AUDIO
- PH_DEV_MON_HW_CAMERA_MOTION
- PH_DEV_MON_HW_CHASSIS_COMP_STAT
- PH_DEV_MON_HW_CURRENT
- PH_DEV_MON_HW_DEWPT
- PH_DEV_MON_HW_DOOR_SWITCH
- PH_DEV_MON_HW_DRY_CONTACT
- PH_DEV_MON_HW_FAN_SPEED
- PH_DEV_MON_HW_HUMIDITY
- PH_DEV_MON_HW_POWER
- PH_DEV_MON_HW_PS_STAT
- PH_DEV_MON_HW_STACK_UNIT
- PH_DEV_MON_HW_STATUS
- PH_DEV_MON_HW_STATUS_AIRFLOW_CRIT
- PH_DEV_MON_HW_STATUS_AIRFLOW_WARN

- PH_DEV_MON_HW_STATUS_ALARMDEVICE_CRIT
- PH_DEV_MON_HW_STATUS_ALARMDEVICE_WARN
- PH_DEV_MON_HW_STATUS_AMP_CRIT
- PH_DEV_MON_HW_STATUS_AMP_WARN
- PH_DEV_MON_HW_STATUS_AUDIO_CRIT
- PH_DEV_MON_HW_STATUS_AUDIO_WARN
- PH_DEV_MON_HW_STATUS_BATTERY_CRIT
- PH_DEV_MON_HW_STATUS_BATTERY_WARN
- PH_DEV_MON_HW_STATUS_CAMERA_MOTION_CRIT
- PH_DEV_MON_HW_STATUS_CAMERA_MOTION_WARN
- PH_DEV_MON_HW_STATUS_DEWPT_CRIT
- PH_DEV_MON_HW_STATUS_DEWPT_WARN
- PH_DEV_MON_HW_STATUS_DISK_CRIT
- PH_DEV_MON_HW_STATUS_DISK_WARN
- PH_DEV_MON_HW_STATUS_DOOR_SWITCH_CRIT
- PH_DEV_MON_HW_STATUS_DOOR_SWITCH_WARN
- PH_DEV_MON_HW_STATUS_DRY_CONTACT_CRIT
- PH_DEV_MON_HW_STATUS_DRY_CONTACT_WARN
- PH_DEV_MON_HW_STATUS_FAN_CRIT
- PH_DEV_MON_HW_STATUS_FAN_WARN
- PH_DEV_MON_HW_STATUS_FILESYSTEM_CRIT
- PH_DEV_MON_HW_STATUS_FILESYSTEM_WARN
- PH_DEV_MON_HW_STATUS_GEN_NUMERIC_SENSOR_CRIT
- PH_DEV_MON_HW_STATUS_GEN_NUMERIC_SENSOR_WARN
- PH_DEV_MON_HW_STATUS_GEN_STATE_SENSOR_CRIT
- PH_DEV_MON_HW_STATUS_GEN_STATE_SENSOR_WARN
- PH_DEV_MON_HW_STATUS_HUMIDITY_CRIT
- PH_DEV_MON_HW_STATUS_HUMIDITY_WARN
- PH_DEV_MON_HW_STATUS_INPUTCONTACT_CRIT
- PH_DEV_MON_HW_STATUS_INPUTCONTACT_WARN
- PH_DEV_MON_HW_STATUS_LCC_CRIT
- PH_DEV_MON_HW_STATUS_LCC_WARN
- PH_DEV_MON_HW_STATUS_LINK_CRIT
- PH_DEV_MON_HW_STATUS_LINK_WARN
- PH_DEV_MON_HW_STATUS_MEMBEACON_CRIT
- PH_DEV_MON_HW_STATUS_MEMBEACON_WARN
- PH_DEV_MON_HW_STATUS_MEMORY_CRIT
- PH_DEV_MON_HW_STATUS_MEMORY_WARN
- PH_DEV_MON_HW_STATUS_MEMOUTLET_CRIT
- PH_DEV_MON_HW_STATUS_MEMOUTLET_WARN
- PH_DEV_MON_HW_STATUS_MEMOUTPUT_CRIT
- PH_DEV_MON_HW_STATUS_MEMOUTPUT_WARN
- PH_DEV_MON_HW_STATUS_MEMSENSOR_CRIT

- PH_DEV_MON_HW_STATUS_MEMSENSOR_WARN
- PH_DEV_MON_HW_STATUS_MISC_CRIT
- PH_DEV_MON_HW_STATUS_MISC_WARN
- PH_DEV_MON_HW_STATUS_OUTLET_CRIT
- PH_DEV_MON_HW_STATUS_OUTLET_WARN
- PH_DEV_MON_HW_STATUS_OUTPUTRELAY_CRIT
- PH_DEV_MON_HW_STATUS_OUTPUTRELAY_WARN
- PH_DEV_MON_HW_STATUS_PORT_CRIT
- PH_DEV_MON_HW_STATUS_PORT_WARN
- PH_DEV_MON_HW_STATUS_POWERSUPPLY_CRIT
- PH_DEV_MON_HW_STATUS_POWERSUPPLY_WARN
- PH_DEV_MON_HW_STATUS_POWER_ENCLOSURE_CRIT
- PH_DEV_MON_HW_STATUS_POWER_ENCLOSURE_WARN
- PH_DEV_MON_HW_STATUS_PROBE_CRIT
- PH_DEV_MON_HW_STATUS_PROBE_WARN
- PH_DEV_MON_HW_STATUS_SLOT_CRIT
- PH_DEV_MON_HW_STATUS_SLOT_WARN
- PH_DEV_MON_HW_STATUS_STACKUNIT_CRIT
- PH_DEV_MON_HW_STATUS_STACKUNIT_WARN
- PH_DEV_MON_HW_STATUS_TEMP_CRIT
- PH_DEV_MON_HW_STATUS_TEMP_WARN
- PH_DEV_MON_HW_STATUS_VOLTAGE_CRIT
- PH_DEV_MON_HW_STATUS_VOLTAGE_WARN
- PH_DEV_MON_HW_TEMP
- PH_DEV_MON_HW_VOLTAGE
- PH_DEV_MON_HYPERV_CPU_GUEST_VIRTUAL_PROC
- PH_DEV_MON_HYPERV_CPU_LOGICAL_PROC
- PH_DEV_MON_HYPERV_CPU_ROOT_VIRTUAL_PROC
- PH_DEV_MON_HYPERV_MEM_OVERALL
- PH_DEV_MON_HYPERV_MEM_PARTITION
- PH_DEV_MON_HYPERV_MEM_PARTITION_PER_VM
- PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION
- PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION_ROOT
- PH_DEV_MON_HYPERV_MEM_VID_PARTITION
- PH_DEV_MON_HYPERV_MEM_VID_PARTITION_PER_VM
- PH_DEV_MON_HYPERV_NET_LEGACY_ADAPTER
- PH_DEV_MON_HYPERV_NET_VIRTUAL_ADAPTER
- PH_DEV_MON_HYPERV_NET_VIRTUAL_SWITCH
- PH_DEV_MON_HYPERV_OVERALL_HEALTH
- PH_DEV_MON_HYPERV_OVERALL_SYSINFO
- PH_DEV_MON_HYPERV_STORAGE_LOGICAL_DISK
- PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_IDE_CONTROLLER
- PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_STORAGE

- PH_DEV_MON_INCOMING_EXCEED_GUARANTEED
- PH_DEV_MON_INTF_ADMIN_DOWN_TO_UP
- PH_DEV_MON_INTF_ADMIN_UP_TO_DOWN
- PH_DEV_MON_INTF_OPER_DOWN_TO_UP
- PH_DEV_MON_INTF_OPER_UP_TO_DOWN
- PH_DEV_MON_INTF_USAGE_TOTAL
- PH_DEV_MON_IPSLA_HTTP_MET
- PH_DEV_MON_IPSLA_ICMP_MET
- PH_DEV_MON_IPSLA_MET
- PH_DEV_MON_IPSLA_UDP_MET
- PH_DEV_MON_IPSLA_VOIP_MET
- PH_DEV_MON_IRONPORT_MAIL_USAGE
- PH_DEV_MON_ISILON_CLUSTER_HEALTH
- PH_DEV_MON_ISILON_CLUSTER_MEMBERSHIP_CHANGE
- PH_DEV_MON_ISILON_CLUSTER_QUOTA
- PH_DEV_MON_ISILON_CLUSTER_SNAPSHOT
- PH_DEV_MON_ISILON_NODE_DISK_PERF
- PH_DEV_MON_ISILON_NODE_HEALTH
- PH_DEV_MON_ISILON_NODE_PROTO_PERF
- PH_DEV_MON_JBOSS_APP
- PH_DEV_MON_JBOSS_CPU
- PH_DEV_MON_JBOSS_DB_POOL
- PH_DEV_MON_JBOSS_EJB
- PH_DEV_MON_JBOSS_MEMORY
- PH_DEV_MON_JBOSS_REQUEST_PROCESSOR
- PH_DEV_MON_JBOSS_SERVLET
- PH_DEV_MON_JBOSS_SESSION
- PH_DEV_MON_JBOSS_THREAD_POOL
- PH_DEV_MON_LOG_ALL_DEVICE_DELAY_HIGH
- PH_DEV_MON_LOG_ALL_DEVICE_DELAY_LOW
- PH_DEV_MON_LOG_DEVICE_DELAY_HIGH
- PH_DEV_MON_LOG_DEVICE_DELAY_LOW
- PH_DEV_MON_MANUAL_SVC_START_TO_STOP
- PH_DEV_MON_MANUAL_SVC_STOP
- PH_DEV_MON_MANUAL_SVC_STOP_TO_START
- PH_DEV_MON_NETAPP_AGGR_MET
- PH_DEV_MON_NETAPP_CIFS_MET
- PH_DEV_MON_NETAPP_CP_MET
- PH_DEV_MON_NETAPP_DISK_HEALTH
- PH_DEV_MON_NETAPP_DISK_MET
- PH_DEV_MON_NETAPP_FCP_MET
- PH_DEV_MON_NETAPP_ISCSI_MET
- PH_DEV_MON_NETAPP_LUN_MET

- PH_DEV_MON_NETAPP_NFS3_MET
- PH_DEV_MON_NETAPP_NFS4_MET
- PH_DEV_MON_NETAPP_NFS_MET
- PH_DEV_MON_NETAPP_VOL_MET
- PH_DEV_MON_NETBOTZ_HW_EMS_STATUS
- PH_DEV_MON_NETBOTZ_HW_MODULE_SENSOR
- PH_DEV_MON_NETBOTZ_HW_PROBE
- PH_DEV_MON_NETSCALER_APP_FW
- PH_DEV_MON_NETSCALER_SERVICE
- PH_DEV_MON_NETSCALER_VIRT_SERVER
- PH_DEV_MON_NET_INTF_UTIL
- PH_DEV_MON_NIMBLE_GLOBAL_STAT
- PH_DEV_MON_NUTANIX_CLUSTER_STATUS
- PH_DEV_MON_NUTANIX_CONTAINER_INFO
- PH_DEV_MON_NUTANIX_CTRLR_VM_RESOURCE
- PH_DEV_MON_NUTANIX_DISK_STATUS
- PH_DEV_MON_NUTANIX_DISK_TEMP
- PH_DEV_MON_NUTANIX_SERVICE_STATUS
- PH_DEV_MON_NUTANIX_STORAGE_POOL_INFO
- PH_DEV_MON_OMI_PING_STAT
- PH_DEV_MON OSPF_NBR_STATUS
- PH_DEV_MON_PANASONIC_AERO_LOG_MON_STATUS
- PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_HIGH
- PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_LOW
- PH_DEV_MON_PERFMON_DEVICE_DELAY_HIGH
- PH_DEV_MON_PERFMON_DEVICE_DELAY_LOW
- PH_DEV_MON_PERFMON_JOB_DELAY_HIGH
- PH_DEV_MON_PERFMON_JOB_DELAY_LOW
- PH_DEV_MON_PERF_MSSQL_BACKUP_INFO
- PH_DEV_MON_PERF_MSSQL_BLOCKBY_INFO
- PH_DEV_MON_PERF_MSSQL_CONFIG_INFO
- PH_DEV_MON_PERF_MSSQL_ERROR_LOG_INFO
- PH_DEV_MON_PERF_MSSQL_GEN_INFO
- PH_DEV_MON_PERF_MSSQL_LOCK_INFO
- PH_DEV_MON_PERF_MSSQL_PERDB
- PH_DEV_MON_PERF_MSSQL_SYS
- PH_DEV_MON_PERF_MSSQL_TOP_QUERIES
- PH_DEV_MON_PERF_MYSQLDB
- PH_DEV_MON_PERF_MYSQLDB_TABLESPACE
- PH_DEV_MON_PERF_ORADB
- PH_DEV_MON_PERF_ORADB_CLUSTER
- PH_DEV_MON_PERF_ORADB_TABLESPACE
- PH_DEV_MON_PERF_ORADB_TOP_QUERIES

- PH_DEV_MON_PING_STAT
- PH_DEV_MON_PING_STAT_SUPPRESSED
- PH_DEV_MON_PORT_CLOSE
- PH_DEV_MON_PORT_OPEN
- PH_DEV_MON_PRINTER_OUTPUT_STATUS
- PH_DEV_MON_PRINTER_SUPPLY_STATUS
- PH_DEV_MON_PROC_CPU_UTIL
- PH_DEV_MON_PROC_MEM_UTIL
- PH_DEV_MON_PROC_RESOURCE_UTIL
- PH_DEV_MON_PROC_START
- PH_DEV_MON_PROC_STOP
- PH_DEV_MON_QUALYS_WEB_APP_FW
- PH_DEV_MON_RBD_BW
- PH_DEV_MON_RBD_CONN
- PH_DEV_MON_RBD_PEER_STAT
- PH_DEV_MON_RBD_PER_PORT_BW
- PH_DEV_MON_RBD_TOP_APP
- PH_DEV_MON_RBD_TOP_DEST
- PH_DEV_MON_RBD_TOP_SRC
- PH_DEV_MON_RBD_TOP_TALKER
- PH_DEV_MON_RDS_METRIC
- PH_DEV_MON_RUCKUS_ACCESS_POINT_STAT
- PH_DEV_MON_RUCKUS_CONTROLLER_STAT
- PH_DEV_MON_RUCKUS_SSID_PERF
- PH_DEV_MON_SERVERIRON_REAL_SERVER_STAT
- PH_DEV_MON_SLB_METRIC
- PH_DEV_MON_SNMP_PING_STAT
- PH_DEV_MON_SRC_AD_REPL_STAT
- PH_DEV_MON_STATUS
- PH_DEV_MON_STORAGE_PORT_DOWN_TO_UP
- PH_DEV_MON_STORAGE_PORT_UP_TO_DOWN
- PH_DEV_MON_SYS_CPU_UTIL
- PH_DEV_MON_SYS_DISK_FREE
- PH_DEV_MON_SYS_DISK_TREND_DAY
- PH_DEV_MON_SYS_DISK_TREND_MONTH
- PH_DEV_MON_SYS_DISK_TREND_WEEK
- PH_DEV_MON_SYS_DISK_UTIL
- PH_DEV_MON_SYS_EXT_CMD
- PH_DEV_MON_SYS_MEM_FREE
- PH_DEV_MON_SYS_MEM_UTIL
- PH_DEV_MON_SYS_PAGEFILE_USAGE
- PH_DEV_MON_SYS_PER_CPU_UTIL
- PH_DEV_MON_SYS_PROC_COUNT

- PH_DEV_MON_SYS_RESTART
- PH_DEV_MON_SYS_STAT
- PH_DEV_MON_SYS_STATUS
- PH_DEV_MON_SYS_SWAP_MEM_ERROR_MSG
- PH_DEV_MON_SYS_UPTIME
- PH_DEV_MON_SYS_VIRT_MEM_UTIL
- PH_DEV_MON_TARGET_FILE_CONTENT_CHANGE
- PH_DEV_MON_TOMCAT_CPU
- PH_DEV_MON_TOMCAT_DB
- PH_DEV_MON_TOMCAT_MEMORY
- PH_DEV_MON_TOMCAT_REQUEST_PROCESSOR
- PH_DEV_MON_TOMCAT_SERVLET
- PH_DEV_MON_TOMCAT_SESSION
- PH_DEV_MON_TOMCAT_THREAD_POOL
- PH_DEV_MON_TRACEROUTE_STAT
- PH_DEV_MON_UCS_HW_CHASSIS_STAT
- PH_DEV_MON_UCS_HW_FAN_STAT
- PH_DEV_MON_UCS_HW_MEMORY_STAT
- PH_DEV_MON_UCS_HW_PROCESSOR_STAT
- PH_DEV_MON_UCS_HW_PSU_STAT
- PH_DEV_MON_UPS_METRIC
- PH_DEV_MON_VMCLUSTER_CPU_UTIL
- PH_DEV_MON_VMCLUSTER_DATASTORE_IO
- PH_DEV_MON_VMCLUSTER_MEM_UTIL
- PH_DEV_MON_VMCLUSTER_STATUS
- PH_DEV_MON_VMRESPOOL_CPU_UTIL
- PH_DEV_MON_VMRESPOOL_MEM_UTIL
- PH_DEV_MON_VM_CPU_UTIL
- PH_DEV_MON_VM_DATASTORE_IO
- PH_DEV_MON_VM_DISK_IO
- PH_DEV_MON_VM_DISK_UTIL
- PH_DEV_MON_VM_MEM_UTIL
- PH_DEV_MON_VM_NET_INTF_UTIL
- PH_DEV_MON_VM_PER_CPU_UTIL
- PH_DEV_MON_VM_SNAPSHOT
- PH_DEV_MON_VM_STATE
- PH_DEV_MON_VM_TOOLS_STATUS
- PH_DEV_MON_VM_UPTIME
- PH_DEV_MON_VPN_CONN
- PH_DEV_MON_VPN_STATUS
- PH_DEV_MON_WATCHGUARD_POLICY_STAT
- PH_DEV_MON_WEBLOGIC_APP
- PH_DEV_MON_WEBLOGIC_DB_POOL

- PH_DEV_MON_WEBLOGIC_EJB
- PH_DEV_MON_WEBLOGIC_GEN
- PH_DEV_MON_WEBLOGIC_MEMORY
- PH_DEV_MON_WEBLOGIC_SERVLET
- PH_DEV_MON_WEBLOGIC_SESSION
- PH_DEV_MON_WEBLOGIC_THREAD_POOL
- PH_DEV_MON_WEBSPHERE_APP
- PH_DEV_MON_WEBSPHERE_AUTHENTICATION
- PH_DEV_MON_WEBSPHERE_CPU
- PH_DEV_MON_WEBSPHERE_DB_POOL
- PH_DEV_MON_WEBSPHERE_EJB
- PH_DEV_MON_WEBSPHERE_MEMORY
- PH_DEV_MON_WEBSPHERE_SERVLET
- PH_DEV_MON_WEBSPHERE_THREAD_POOL
- PH_DEV_MON_WEBSPHERE_TRANSACTION
- PH_DEV_MON_WMI_PING_STAT
- PH_JOB_STAT
- PH_JOB_STATUS_XML_SEND_ERROR
- PH_JOB_STATUS_XML_SENT
- PH_JOB_STAT_SUPPRESSED
- PH_MONITOR_ARCHIVE_GET_WORKER_FAILURE
- PH_MONITOR_ARCHIVE_UPDATE_WORKER_FAILURE
- PH_MONITOR_BEACONING_REGISTER_FAILURE
- PH_MONITOR_CHECK_DEPENDENCY_FAILED
- PH_MONITOR_CMD_FAILURE
- PH_MONITOR_CMD_SEND_FAILURE
- PH_MONITOR_COLLECTOR_REGISTER_FAILURE
- PH_MONITOR_COLLECTOR_UPDATE_STATUS_FAILURE
- PH_MONITOR_CONFIG_DOWNLOAD_FAILURE
- PH_MONITOR_DBCLUSTER_SEND_COMMAND_FAILED
- PH_MONITOR_DELETE_DR_FAILED
- PH_MONITOR_DELETE_SECONDARY_ON_WORKER_FAILED
- PH_MONITOR_DELETE_SUPER_FOLLOWER_FAILED
- PH_MONITOR_DISPATCH_CMD_MISMATCH
- PH_MONITOR_DOMAIN_CHANGE_XML_PARSE_FAILURE
- PH_MONITOR_ENT_OR_SP_MODE_MISSING
- PH_MONITOR_EXCESSIVE_DB_LOGIN_FAILURE
- PH_MONITOR_FAILED_CONN_QUERYMASTER
- PH_MONITOR_FILE_IO_ERROR
- PH_MONITOR_FILE_PERMISSION_ERROR
- PH_MONITOR_FILE_PERMISSION_WARNING
- PH_MONITOR_FLIP_PRIMARY_FAILURE
- PH_MONITOR_FSM_AGENT_UPDATE_PWD_ERROR

- PH_MONITOR_GET_REPLICATION_PROGRESS_FAILED
- PH_MONITOR_GET_UPTIME_ERROR
- PH_MONITOR_HANDLE_TASK
- PH_MONITOR_HARDWARE_SN_FORK_FAILURE
- PH_MONITOR_HOST_UUID_READ_FAILURE
- PH_MONITOR_HTTP_PULL_ERROR
- PH_MONITOR_INIT_PROC_MODULE_NOT_FOUND
- PH_MONITOR_INIT_SECONDARY_ON_WORKER_FAILED
- PH_MONITOR_INIT_SUPER_FOLLOWER_FAILED
- PH_MONITOR_INIT_SYSTEM_XML_PARSE_FAILURE
- PH_MONITOR_JDBC_POOL_NOT_EXIST
- PH_MONITOR_LIB_DEPENDENCY_WARNING
- PH_MONITOR_LOAD_CONF_FROM_APP_SERVER_FAILED
- PH_MONITOR_LOCAL_HOSTNAME_GET_FAILURE
- PH_MONITOR_MEM_FILE_OPEN_FAILURE
- PH_MONITOR_MISSING_MONITOR
- PH_MONITOR_MMAP_FAILURE
- PH_MONITOR_MOTNIROR_REGISTER_FAILURE
- PH_MONITOR_NOTIFICATION_CLIENT_CONTACT_FAILURE
- PH_MONITOR_NOTIFICATION_CMD_EMPTY
- PH_MONITOR_NOTIFICATION_CMD_MISMATCH
- PH_MONITOR_NOTIFICATION_RETURN_FAILURE
- PH_MONITOR_PHOENIX_CONFIG_GLOBAL_MISSING
- PH_MONITOR_PHOENIX_CONFIG_INVALID
- PH_MONITOR_PROCESS_OWNER_NOT_ADMIN_ERROR
- PH_MONITOR_RECVD_CONFIG_CHANGE
- PH_MONITOR_RECVD_HEARTBEAT
- PH_MONITOR_REDIS_UPDATE_FAILED
- PH_MONITOR_REGISTER_MONITOR_GET_WORKER_FAILURE
- PH_MONITOR_REGISTER_NODE
- PH_MONITOR_REGISTER_SUPER_FOLLOWER
- PH_MONITOR_REGISTER_WORKER
- PH_MONITOR_REMOVE_NODE
- PH_MONITOR_REMOVE_SUPER_FOLLOWER
- PH_MONITOR_REMOVE_WORKER
- PH_MONITOR_REPORTSERVER_NOTIFICATION_CLIENT_CONTACT_FAILURE
- PH_MONITOR_REPORTSERVER_NOTIFICATION_CLIENT_INIT_FAILURE
- PH_MONITOR_REPORTSERVER_NOTIFICATION_SERVER_RETURN_FAILURE
- PH_MONITOR_RESET_DB_SERVER_NAME_FAILED
- PH_MONITOR_RESET_JDBC_CONN_FAILED
- PH_MONITOR_RESET_STORAGE_CONFIG_FAILED
- PH_MONITOR_RESTART_MODULES
- PH_MONITOR_REST_CACHE_REQUEST_EMPTY

- PH_MONITOR_REST_CACHE_REQUEST_FAILURE
- PH_MONITOR_REST_CACHE_REQUEST_FORMAT_ILLEGAL
- PH_MONITOR_REST_CACHE_SERVER_INIT_FAILURE
- PH_MONITOR_REST_CALL_FAILURE
- PH_MONITOR_ROLE_UNDEFINED
- PH_MONITOR_SAVE_DR_CONFIG_FAILED
- PH_MONITOR_SEND_CMD_TO_MODULE
- PH_MONITOR_SEND_VG_UPDATE_CMD_TO_MODULE
- PH_MONITOR_SETUID_FAILURE
- PH_MONITOR_START_MODULE
- PH_MONITOR_START_MODULES
- PH_MONITOR_STATFS_FAILURE
- PH_MONITOR_STATUS_PUSHER_SPAWN_FAILURE
- PH_MONITOR_STOP_MODULES
- PH_MONITOR_STOP_READER
- PH_MONITOR_STORAGE_ES_CUSTOMIZED_TEMPLATE_DEPLOYED
- PH_MONITOR_STORAGE_GET_WORKER_FAILURE
- PH_MONITOR_STORAGE_LOCAL_GET_FAILURE
- PH_MONITOR_STORAGE_NFS_GET_FAILURE
- PH_MONITOR_STORAGE_TYPE_GET_FAILURE
- PH_MONITOR_STORAGE_TYPE_UNKNOWN
- PH_MONITOR_STORAGE_UPDATE_WORKER_FAILURE
- PH_MONITOR_SVC_PASSWORD_DISTRIBUTION_ERROR
- PH_MONITOR_SYSINFO_FAILURE
- PH_MONITOR_SYSTEM_DB_LOGIN_ERROR
- PH_MONITOR_SYSTEM_HEALTH_CPU
- PH_MONITOR_SYSTEM_HEALTH_ISSUE
- PH_MONITOR_SYSTEM_HEALTH_MEM
- PH_MONITOR_SYSTEM_STATUS_SPAWN_FAILURE
- PH_MONITOR_THREAD_SPAWN_FAILED
- PH_MONITOR_TUNNEL_ERROR
- PH_MONITOR_UMOUNT_NFS_FAILURE
- PH_MONITOR_UNABLE_CONTACT_APPSVR
- PH_MONITOR_UPDATE_DATA_FAILED
- PH_MONITOR_UPDATE_DR_FAILED
- PH_MONITOR_UPDATE_WORKER_INFO_FAILED
- PH_MONITOR_UPLOAD_LOG_SPAWN_FAILURE
- PH_MONITOR_WINAGENT_DELETE_PWD_SPAWN_FAILURE
- PH_MONITOR_WINAGENT_UPDATE_PWD_ERROR
- PH_MONITOR_WIN_LINUX_AGENT_PWD_UPDATE_SUCCESS
- PH_MONITOR_WORKER_NODECONFIG_UPDATE_FAILED
- PH_MONITOR_WORKER_REDIS_ADDSLAVE_UPDATE_FAILED
- PH_MONITOR_WORKER_REDIS_CONF_UPDATE_FAILED

- PH_PERFMON_COMMIT_FILE_FAILED
- PH_PERFMON_CONFIG_SEND_FAILED
- PH_PERFMON_CONFIG_VERSION_ERROR
- PH_PERFMON_CONFIG_VERSION_WARNING
- PH_PERFMON_CUST_JOB_ADD_FAILED
- PH_PERFMON_INIT_ERROR
- PH_PERFMON_INST_SW_MAP_EMPTY
- PH_PERFMON_INST_SW_NO_NAME
- PH_PERFMON_JOB_ADD_FAILED
- PH_PERFMON_MASS_PING_WARNING
- PH_PERFMON_MONITEE_BAD
- PH_PERFMON_MONITEE_NOT_FOUND
- PH_PERFMON_NO_DEV_TYPE
- PH_PERFMON_PERF_OBJ_PARSE_FAILURE
- PH_PERFMON_PING_RESULT_OPEN_FAILED
- PH_PERFMON_PROC_RUN_FAILED
- PH_PERFMON_REAL_TIME_JOB_RUN_FAILED
- PH_PERFMON_ROUTE_LOAD_ERROR
- PH_PERFMON_STATUS_REPORTER_INIT_FAILED
- PH_PERFMON_STATUS_REPORT_FAILED
- PH_PERFMON_SVN_CHECKOUT_FAILED
- PH_PERFMON_SVN_CONFIG_MISSING
- PH_PERFMON_SVN_DIR_CREATE_FAILED
- PH_PERFMON_SVN_DIR_UPDATE_FAILED
- PH_PERFMON_SVN_FILE_COPY_FAILED
- PH_PERFMON_SVN_FILE_EMPTY
- PH_PERFMON_SVN_FILE_MARK_FAILED
- PH_PERFMON_SVN_FILE_OPEN_FAILED
- PH_PERFMON_SVN_FILE_PARSE_FAILED
- PH_PERFMON_SVN_FILE_REMOVE_FAILED
- PH_PERFMON_SVN_FILE_RENAME_FAILED
- PH_PERFMON_SVN_FIM_FILE_MISSING
- PH_PERFMON_SVN_FIRSTFILELINES_EMPTY
- PH_PERFMON_SVN_FIRSTFILELINES_NOT_IN_FILE
- PH_PERFMON_SVN_GET_DEVICE_ID_FAILED
- PH_PERFMON_SVN_GET_DISCOV_TIME_FAILED
- PH_PERFMON_SVN_INFO_GET_FAILED
- PH_PERFMON_SVN_INST_SW_BAD
- PH_PERFMON_SVN_INVALID_FILE_FORMAT
- PH_PERFMON_SVN_INVALID_HEADER_IN_FILE
- PH_PERFMON_SVN_INVALID_SECONDFILENAME
- PH_PERFMON_SVN_LINE_MISMATCH
- PH_PERFMON_SVN_SECONDFILENAME_EMPTY

- PH_PERFMON_SVN_SOFTWARE_MISSING
- PH_PERFMON_TOPO_CONFIG_ERROR
- PH_PERFMON_TOPO_FILE_OPEN_FAILED
- PH_PERFMON_TOPO_LOAD_ERROR
- PH_PERFMON_TRACERT_FILE_OPEN_FAILED
- PH_PERFMON_UNKNOWN_CUST_PERF_JOB_ID
- PH_PERFMON_UNKNOWN_PERF_JOB_ID
- PH_PERFMON_UNKNOWN_PROBE_JOB_ID
- PH_PERFMON_UPDATE_CONFIG_ERROR
- PH_PERFMON_UPDATE_FILTERS_ERROR
- PH_PERFMON_UPDATE_ROUTE_DEPENDENCY_FAILED
- PH_PERFMON_USER_PWD_GET_FAILED
- PH_PERFORM_MONITOR_ERROR
- PH_PER_MON_CONFIG_ERROR
- PH_PER_MON_FETCH
- PH_PER_MON_FUNCTION
- PH_PER_MON_SNMP_DONE
- PH_PER_MON_WALK
- PH_PER_MON_WALK_ERROR
- PH_STM_ACCOUNT_UNMATCHED
- PH_STM_AUTH_TYPE_UNKNOWN
- PH_STM_BAD_ELEM
- PH_STM_BAD_ELEM_VALUE
- PH_STM_BAD_PORT
- PH_STM_BAD_RTT_LINE
- PH_STM_BAD_SSL
- PH_STM_BAD_TAG
- PH_STM_CMD_EXEC_FAILED
- PH_STM_CRED_INVALID
- PH_STM_CURL_ESCAPE_FAILED
- PH_STM_CURL_INIT_FAILED
- PH_STM_DNS_TYPE_UNSUPPORT
- PH_STM_DUPLICATED
- PH_STM_ELEM_EMPTY
- PH_STM_ELEM_MISSING
- PH_STM_ELEM_NEGATIVE
- PH_STM_ERROR
- PH_STM_FILE_OPEN_FAILED
- PH_STM_GET_HOST_FAILED
- PH_STM_GUESS_TYPE_FAILED
- PH_STM_HTTP_RESP_FAILED
- PH_STM_METHOD_UNKNOWN
- PH_STM_MONITOR_MISSING_ACTION

- PH_STM_MONITOR_RESULT_UPLOAD_FAILED
- PH_STM_NO_ORACLE_NAME
- PH_STM_PORT_UNKNOWN
- PH_STM_PROCESS_INVOKE_FAILED
- PH_STM_PROTO_UNKNOWN
- PH_STM_PROTO_UNSUPPORT
- PH_STM_SERVER_ADDR_INVALID
- PH_STM_SPECIAL_LINE_NOT_FOUND
- PH_STM_STM_GET_PROCESS_FAILED
- PH_STM_STM_GET_PROCESS_NAME_FAILED
- PH_STM_TAG_MISSING
- PH_STM_TAG_NOT_FOUND
- PH_STM_TAG_UNKNOWN
- PH_STM_TRACEROUTE_FAILED
- PH_STM_XML_PARSE_FAILED
- PH_USER_MON_SUDDEN_LOC_CHANGE
- PH_USER_MON_SUDDEN_LOGIN_DISTRIBUTION_CHANGE
- PH_USER_MON_SUDDEN_LOGIN_VOLUME_CHANGE

EventType: PH_DEV_MON_ACME_PACKET_SESSION_AGENT_STATUS

Description: Acme Packet Controller session status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
sessionAgentHostName	Agent HostName	string	
sessionAgentType	Agent Type	string	
sessionInboundCont	Session Inbound Count	uint32	
sessionInboundRate	Session Inbound Rate	uint32	
sessionOutboundCount	Session Outbound Count	uint32	

Id	Display name	Type	Description
sessionOutboundRate	Session Outbound Rate	uint32	
sessionAgentStatus	Session Agent Status	string	

EventType: PH_DEV_MON_ACME_PACKET_SYS_STATUS

Description: Acme Packet Controller system status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
apSysHealthScore	System Health Score	uint32	
apSysRedundancy	System Redundancy	uint32	
apSysGlobalConSess	System Global ConSess	uint32	
apSysGlobalCPS	System Global CPS	uint32	
apSysNATCapacity	System NAT Capacity	uint32	
apSysARPCapacity	System ARP Capacity	uint32	
apSysState	System State	uint32	
apSysLicenseCapacity	System License Capacity	uint32	
apSysSipStatsActiveLocalContacts	System Sip Stats Active Local Contacts	uint32	
apSysMgcpGWEndpoints	System Mgcp GW Endpoints	uint32	
apSysH323Registration	System H323 Registration	uint32	

Id	Display name	Type	Description
apSysRegCacheLimit	System Reg Cache Limit	uint32	
apSysApplicationCPULoadRate	System Application CPU Load Rate	uint32	
apSysRejectedMessages	System Rejected Messages	uint32	
apSysSipEndptDemTrustToUntrust	System Sip Endpt Dem Trust To Untrust	uint32	
apSysSipEndptDemUntrustToDeny	System Sip Endpt Dem Untrust To Deny	uint32	
apSysMgcpEndptDemTrustToUntrust	System Mgcp Endpt Dem Trust To Untrust	uint32	
apSysMgcpEndptDemUntrustToDeny	System Mgcp Endpt Dem Untrust To Deny	uint32	
apSysSipTotalCallsRejected	System SIP Total Calls Rejected	uint32	
apSysSipStatsActiveSubscriptions	System SIP Active Subscriptions	uint32	
apSysSipStatsPerMaxSubscriptions	System SIP Per Max Subscriptions	uint32	
apSysSipStatsPerMaximumActiveSubscriptions	System SIP Per Maximum Active Subscriptions	uint32	
apSysSipStatsTotalSubscriptions	System SIPTotal Subscriptions	uint32	

EventType: PH_DEV_MON_APP_APACHE_MET

Description: Apache Web server performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
httpTotalAccesses	HTTP Connection Count	uint32	
httpTotalKBytes	HTTP Total KBytes	uint32	
apacheCPULoad	Apache CPU Load	double	
apacheUptime	Apache Uptime	uint64	
apacheReqPerSec	Apache Request Rate /sec	double	
apacheBytesPerSec	Apache Transfer Rate Bytes/sec	double	
apacheBytesPerReq	Apache Transfer Rate Bytes/Req	double	
apacheBusyWorkers	Apache Busy Workers	uint32	
apacheldleWorkers	Apache Idle Workers	uint32	

EventType: PH_DEV_MON_APP_ASPNET_MET

Description: ASP.NET performance metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
aspReqExecTimeMs	ASP.NET Request Exec Time ms	uint32	
aspReqCurrent	ASP.NET Curent Requests	uint32	

Id	Display name	Type	Description
aspReqDisconnected	ASP.NET Disconn Requests	uint32	
aspReqQueued	ASP.NET Queued Requests	uint32	
aspReqRejected	ASP.NET Rejected Requests	uint32	
aspReqWaitTimeMs	ASP.NET Request Wait Time ms	uint32	

EventType: PH_DEV_MON_APP_DHCP_MET

Description: DHCP performance metrics collected

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
dhcpReqPerSec	DHCP Request Rate /sec	uint32	
dhcpRelPerSec	DHCP Release Rate /sec	uint32	
dhcpDeclinesPerSec	DHCP Decline Rate /sec	uint32	
dhcpDupsDroppedPerSec	DHCP Duplicate Drop Rate /sec	uint32	
dhcpPktsPerSec	DHCP Packet Rate /sec	uint32	
dhcpActiveQueueLen	DHCP Active Queue Length	uint32	
dhcpConflictQueueLen	DHCP Conflict Queue Length	uint32	
dhcpAvgRespTime	DHCP Average Resp Time	uint32	
dhcpDiscoverPerSec	DHCP Discover Rate /sec	uint32	
dhcOfferPerSec	DHCP Offer Rate /sec	uint32	

Id	Display name	Type	Description
dhcpAckPerSec	DHCP Ack Rate /sec	uint32	
dhcpNackPerSec	DHCP Nack Rate /sec	uint32	
dhcpInformPerSec	DHCP Inform Rate /sec	uint32	

EventType: PH_DEV_MON_APP_DNS_MET

Description: DNS performance metrics collected

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
dnsReqRecv	DNS Requests Recvd	uint32	
dnsRespSent	DNS Responses Sent	uint32	
winsReqRecv	WINS Requests Recvd	uint32	
winsRespSent	WINS Responses Sent	uint32	
dnsRecQueryRecv	Recursive DNS Query Recvd	uint32	
recurDnsQueryFail	Recursive DNS Query Failed	uint32	
recurDnsQueryTimeout	Recursive DNS Query Timeout	uint32	
fullDnsXferSent	Full DNS Zone Transfer Request Sent	uint32	
fullDnsXferRecv	Full DNS Zone Transfer Responses Recvd	uint32	
fullDnsXferSucc	Full DNS Zone Transfer Success	uint32	
incrDnsXferRecv	Incremental DNS Zone Transfer Responses Recvd	uint32	
incrDnsXferSucc	Incremental DNS Zone Transfer Success	uint32	

Id	Display name	Type	Description
dnsSecUpdateRecv	Secure DNS Update Recvd	uint32	
dynDnsUpdRej	Dynamic DNS Update Rejected	uint32	
dynDnsUpdTimeout	Dynamic DNS Update Timeout	uint32	
secDnsUpdFail	Secure DNS Update Failed	uint32	

EventType: PH_DEV_MON_APP_ICA_SESS_MET

Description: Citrix ICA IIS session metrics collected

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
user	User	string	
icaLatencyLast	ICA Latency Last Recorded	uint32	
icaLatencySessAvg	ICA Latency Session Average	uint32	
icaLatencySessDev	ICA Latency Session Deviation	uint32	
icaInSessBw	ICA Input Session Bandwidth	uint32	
icaInSessLineSpeed	ICA Input Session Line Speed	uint32	
icaInSessComp	ICA Input Session Compression	uint32	
icaInDriveBw	ICA Input Drive Bandwidth	uint32	
icaInEchoBw	ICA Input Text Echo Bandwidth	uint32	
icaInAudioBw	ICA Input Audio Bandwidth	uint32	

Id	Display name	Type	Description
icaInVFBw	ICA Input VideoFrame Bandwidth	uint32	
icaOutSessBw	ICA Output Session Bandwidth	uint32	
icaOutSessLineSpeed	ICA Output Session Line Speed	uint32	
icaOutSessComp	ICA Output Session Compression	uint32	
icaOutDriveBw	ICA Output Drive Bandwidth	uint32	
icaOutEchoBw	ICA Output Text Echo Bandwidth	uint32	
icaOutAudioBw	ICA Output Audio Bandwidth	uint32	
icaOutVFBw	ICA Output VideoFrame Bandwidth	uint32	

EventType: PH_DEV_MON_APP_IIS_MET

Description: Microsoft IIS performance metrics collected

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
httpCurrConnCount	HTTP Current Connection Count	uint32	
httpMaxConnCount	HTTP Max Connection Count	uint32	
httpSentFiles	HTTP Sent Files	uint32	
httpRecvFiles	HTTP Recv Files	uint32	

Id	Display name	Type	Description
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.
sysUpTime	System Uptime	uint32	
httpNotFoundErr	HTTP Not Found Errors	uint32	
srvInstName	Web Server Instance	string	

EventType: PH_DEV_MON_APP_MSEXCH_ERR_MET

Description: Microsoft Exchange performance error metrics collected

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchRPCFailed	Exch RPC Failed Count	uint32	
exchRPCSuccess	Exch RPC Success Count	uint32	
exchRPCCallFailed	Exch RPC Failed - Call Failed	uint32	
exchRPCDenied	Exch RPC Denied Count	uint32	
exchRPCFailedServBusy	Exch RPC Failed - Server Busy	uint32	
exchRPCFailedServUnavail	Exch RPC Failed - Server Unavail	uint32	
exchBgRPCFailed	Exch Background RPC Failed	uint32	

Id	Display name	Type	Description
exchFgRPCFailed	Exch Foreground RPC Failed	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_ISDB_INST_MET

Description: Microsoft Exchange Database Instance Metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
dbName	DB Name	string	
logGenCheckpointDepth	Log Gen Checkpoint Depth	uint32	
dbReadsAverageLatency	DB Read latency ms	uint32	
dbWritesAverageLatency	DB Write latency ms	uint32	
dbPhysicalWritesPerSec	DB Write Rate /sec	double	
dbSessionCount	DB Session Count	uint32	
sessPctUsed	Session Used Pct	uint32	
logBytesWritePersec	Log Write Rate Bps	uint32	
versionbucketsallocated	Version Buckets Allocated	uint32	
logThreadsWaiting	Log Threads Waiting	uint32	
tableOpenCacheHitsPersec	Table Open Cache Hit Rate /sec	uint32	
tableOpenCacheMissesPersec	Table Open Cache Miss Rate /sec	uint32	

Id	Display name	Type	Description
tableOpenCachePercentHit	Table Open Cache Hit Pct	uint32	
tableOpensPersec	Table Open Rate /sec	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_ISDB_MET

Description: Microsoft Exchange Information Store Database Metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
pageFaultsStallsPersec	Page Fault Stall Rate /sec	uint32	
pageFaultsPersec	Page Fault Rate /sec	uint32	
dbCacheSizeMB	DB Cache Size MB	uint32	
dbCachePercentHit	DB Cache Hit pct	uint32	
logBytesWritePersec	Log Write Rate Bps	uint32	
dbReadsAverageLatency	DB Read latency ms	uint32	
dbWritesAverageLatency	DB Write latency ms	uint32	
logRecordStallsPersec	Log Record Stall Rate /sec	uint32	
versionbucketsallocated	Version Buckets Allocated	uint32	
logThreadsWaiting	Log Threads Waiting	uint32	
logWritesAverageLatency	Log Write latency ms	uint32	
dbPageFaultsPersec	DB Page Fault Rate /sec	uint32	
dbPageFaultStallsPersec	DB Page Fault Stall Rate /sec	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_MBOX_MET

Description: MS Exchange mailbox utilization metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchMboxName	Exch Mailbox Name	string	
exchMboxSendQueue	Exch Mailbox Send Queue	uint32	
exchMboxRecvQueue	Exch Mailbox Recv Queue	uint32	
exchMboxSentMsg	Exch Mailbox Sent Message	uint32	
exchMboxSubmitMsg	Exch Mailbox Submitted Message	uint32	
exchMboxDelivMsg	Exch Mailbox Delivered Message	uint32	
exchMboxActiveUserCount	Exch Mailbox Active User Count	uint32	
exchMboxPeakUserCount	Exch Mailbox Peak User Count	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_MET

Description: Microsoft Exchange performance metrics collected

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchVMLargestBlockSize	Exch VM Largest Block Size	uint32	
exchVMTotallargeFreeBlockBytes	Exch VM Large Free Blocks Bytes	uint32	
exchVMTotallFreeBlocks	Exch VM Free Blocks	uint32	
exchRPCReq	Exch RPC Requests Served	uint32	
exchRPCAvgLatency	Exch Avg RPC Latency ms	uint32	
exchRPCOpsPerSec	Exch RPC Ops Rate /sec	uint32	
exchRPCReqPeak	Exch RPC Request Peak	uint32	
exchUserCount	Exch User Count	uint32	
exchActiveUserCount	Exch Active User Count	uint32	
exchPeakUserCount	Exch Peak User Count	uint32	
exchActiveConnCount	Exch Active Conn Count	uint32	
exchMaxConn	Exch Max Conn Count	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_REPL_MET

Description: Microsoft Exchange Replication Metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchReplInstName	Exch Replication Instance Name	string	
copyQueueLen	Exch TxLog Copy Queue Length	uint32	
replayQueueLength	Exch TxLog Replay Queue Length	uint32	
avgLogCopyLatencyMs	Exch Log Copy latency ms	uint32	
maxNetworkLatencyMs	Exch Log Copy network Latency ms	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_SMTP_MET

Description: MS Exchange SMTP metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchCatQueue	Exch Categorization Queue	uint32	
exchSMTPLocalQueue	Exch SMTP Local Queue	uint32	
exchSMTPRemoteQueue	Exch SMTP Remote Queue	uint32	

Id	Display name	Type	Description
exchSMTPInConn	Exch SMTP Inbound Conn	uint32	
exchSMTPOutConn	Exch SMTP Outbound Conn	uint32	
sentBytesPerSec	Sent Byte Rate	double	
recvBytesPerSec	Received Byte Rate	double	
exchSMTPRetries	Exch SMTP Retries	uint32	
exchSMTPLocalRetryQueue	Exch SMTP Local Retry Queue	uint32	
exchSMTPRemoteRetryQueue	Exch SMTP Remote Retry Queue	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_STORE_INTF_MET

Description: Microsoft Exchange Store Interface Metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchStoreIntfName	Exch Store Interface Name	string	
exchRPCAvgLatency	Exch Avg RPC Latency ms	uint32	
RPCReqOutstanding	Exch Outstanding RPC Requests	uint32	
ROPReqOutstanding	Exch Outstanding ROP Requests	uint32	

Id	Display name	Type	Description
RPCReqFailedPct	Exch RPC Failed Requests Pct	uint32	
RPCSlowReq	Exch RPC Slow Requests	uint32	
RPCSlowReqLatencyAvgMs	Exch RPC Slow Request Latency ms	uint32	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.

EventType: PH_DEV_MON_APP_MSEXCH_SUBMIT_MET

Description: Microsoft Exchange Mail Submission Metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
hubServers	Exch Hub Server Count	uint32	
hubServersInRetry	Exch Hub Servers In Retry	uint32	
failedSubmissions	Exch Failed Submissions	uint32	
successSubmissions	Exch Successful Submissions	uint32	
tempSubmissionFailures	Exch Temp Submission Failures	uint32	
hubTranspServersPrctActive	Exch Active Hub Transport Servers Pct	uint32	
failedSubmissionsPersec	Exch Failed Submission Rate /sec	uint32	

Id	Display name	Type	Description
successSubmissionsPersec	Exch Successful Submission Rate /sec	uint32	
tempSubmissionFailuresPersec	Exch Temp Submission Failure Rate /sec	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_TRANS_MET

Description: Microsoft Exchange Transport Queue Metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
aggDeliveryQueueLen	Exch Aggregate Delivery Queue	uint32	
activeRemoteDeliveryQueueLen	Exch Active Remote Delivery Queue	uint32	
activeMailboxDeliveryQueueLen	Exch Active Mailbox Delivery Queue	uint32	
submissionQueueLen	Exch Submission Queue	uint32	
activeNonSmtplibDeliveryQueueLen	Exch Active Non-SMTP Delivery Queue	uint32	
retryMailboxDeliveryQueueLen	Exch Retry Mailbox Delivery Queue	uint32	
unreachableQueueLen	Exch Unreachable Queue	uint32	
largestDeliveryQueueLen	Exch Largest Delivery Queue	uint32	
poisonQueueLength	Exch Poison Queue	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_WS_MET**Description:** MS Exchange Mailbox whitespace metric**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchMboxName	Exch Mailbox Name	string	
exchMboxWs	Exch Mailbox Whitespace MB	uint32	

EventType: PH_DEV_MON_APP_NTDS_MET**Description:** Microsoft directory service performance metrics collected**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
dirSearchesPerSec	NTDS Dir Search Rate /sec	double	
dirReadsPerSec	NTDS Dir Read Rate /sec	double	
dirWritesPerSec	NTDS Dir Write Rate /sec	double	
dirBrowsesPerSec	NTDS Dir Browse Rate /sec	double	

Id	Display name	Type	Description
LDAPSearchesPerSec	NTDS LDAP Search Rate /sec	double	
DSCClientBindsPerSec	NTDS Client Bind Rate /sec	double	
LDAPNewConnectionsPerSec	NTDS LDAP New Conn Rate /sec	double	
LDAPSuccessfulBindsPerSec	NTDS LDAP Success Bind Rate /sec	double	
LDAPActiveThreads	NTDS LDAP Active Threads	uint32	
LDAPBindTime	NTDS LDAP Bind Time	uint32	
LDAPClientSessions	NTDS LDAP Client Sessions	uint32	

EventType: PH_DEV_MON_ARUBA_WLAN_RADIO_METRIC

Description: WLAN Radio interface metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
wlanChannelId	WLAN Channel Id	uint32	WLAN Channel Id found in SNMP based WLAN monitoring
wlanProtocol	WLAN Protocol	string	WLAN Protocol found in SNMP based WLAN monitoring
wlanUserCount	WLAN User count	uint32	WLAN User count found in SNMP based WLAN monitoring
wlanChannelUtil	WLAN Channel Util	uint32	WLAN Channel Util found in SNMP based WLAN monitoring
ifIntefIdx	WLAN Interface Intereference Index	uint32	WLAN Interface Intereference Index found in SNMP based WLAN monitoring

Id	Display name	Type	Description
ifCoverageIndx	WLAN Interface Coverage Index	uint32	WLAN Interface Coverage Index found in SNMP based WLAN monitoring
ifNoiseIndx	WLAN Interface Noise Index	uint32	WLAN Interface Noise Index found in SNMP based WLAN monitoring
totBytesPerSec	Total Byte Rate	double	
totPktsPerSec	Total Packet Rate	double	

EventType: PH_DEV_MON_AUTH_STATS

Description: FortiAuthenticator Authentication status

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
authUserCount	Auth User Count	uint32	
authGroupCount	Auth Group Count	uint32	
tokenCount	Token Count	uint32	
usersRemaining	User Remaining	uint32	
groupRemaining	Group Remaining	uint32	
tokenRemaining	Token Remaining	uint32	
radiusNasCount	Radius Nas Count	uint32	
radiusNasRemaining	Radius Nas Remaining	uint32	
userCertCount	User Certification Count	uint32	
radiusLoginsTot	Radius Logins Count	uint32	
radiusLogins5Mins	Radius Logins Count 5 Mins	uint32	
radiusFailuresTot	Radius Login Failures Count	uint32	

Id	Display name	Type	Description
radiusFailures5Mins	Radius Login Failures Count 5 Mins	uint32	
radiusAccountingTot	Radius Accounting Count	uint32	
radiusAccounting5Mins	Radius Accounting Count 5 Mins	uint32	
ldapLoginsTot	LDAP Logins Count	uint32	
ldapLogins5Mins	LDAP Logins Count 5 Mins	uint32	
ldapFailuresTot	LDAP Failures Count	uint32	
ldapFailures5Mins	LDAP Failures Count 5 Mins	uint32	
authEventsTot	Auth Events Count	uint32	
authEvents5Mins	Auth Events Count 5 Mins	uint32	
authFailure	Auth Failures	uint32	
authFailures5Mins	Auth Failures Count 5 Mins	uint32	
radiusProxyInTot	Radius Proxy Requests Received	uint32	
radiusProxyOutTot	Radius Proxy Requests Sent	uint32	

EventType: PH_DEV_MON_AUTO_SVC_START_TO_STOP

Description: Running Windows Auto Service stopped

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
servicePath	Service Path	string	
serviceDesc	Service Description	string	

EventType: PH_DEV_MON_AUTO_SVC_STOP

Description: Windows Auto Service stopped

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
servicePath	Service Path	string	
serviceDesc	Service Description	string	

EventType: PH_DEV_MON_AUTO_SVC_STOP_TO_START

Description: Stopped Windows Auto Service started

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
servicePath	Service Path	string	
serviceDesc	Service Description	string	

EventType: PH_DEV_MON_BC_PROXY_METRIC

Description: Bluecoat Web-proxy metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
proxyCacheObjCount	Proxy Cache Object Count	uint32	
proxy2ServerHttpErr	Proxy-to-Server HTTP Error	uint32	
proxy2ServerHttpReq	Proxy-to-Server HTTP Requests	uint32	
server2ProxyHttpKBps	Server-to-Proxy HTTP Traffic KBps	double	
proxy2ServerHttpKBps	Proxy-to-Server HTTP Traffic KBps	double	
client2ProxyHttpReq	Client-to-Proxy HTTP Request	uint32	
client2ProxyHttpCacheHit	Client-to-Proxy HTTP Cache Hit	uint32	
client2ProxyHttpError	Client-to-Proxy HTTP Errors	uint32	
client2ProxyHttpKBps	Client-to-Proxy HTTP Traffic KBps	double	
proxy2ClientHttpKBps	Proxy-to-Client HTTP Traffic KBps	double	

EventType: PH_DEV_MON_BGP_NBR_STATUS**Description:** BGP neighbor status**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
srcASNum	Source Autonomous System Number	uint16	The Autonomous System Number (ASN) to which Source IP belongs. ASN is a unique identifier that is globally available and allows its autonomous system to exchange routing information with other systems. This attribute is generally present in Netflow.
destASNum	Destination Autonomous System Number	uint16	The Autonomous System Number (ASN) to which Destination IP belongs. ASN is a unique identifier that is globally available and allows its autonomous system to exchange routing information with other systems. This attribute is generally present in Netflow.
bgpState	BGP State	string	

EventType: PH_DEV_MON_BOX_FILE_CREATE

Description: Box.com file created

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
fileType	File Type	string	
targetName	Target Name	string	
fileSize64	File Size64 Bytes	uint64	
filePath	File Path	string	
fileOwner	File Owner	string	
fileDesc	File Description	string	
user	User	string	
userId	User Id	string	

Id	Display name	Type	Description
accessTime	Access Time	Date	
accountName	Account Name	string	
fileId	File Id	string	
fileVersion	File Version	string	
targetHashCode	Target Hash Code	string	

EventType: PH_DEV_MON_BOX_FILE_DELETE

Description: Box.com file deleted

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
fileType	File Type	string	
targetName	Target Name	string	
fileSize64	File Size64 Bytes	uint64	
filePath	File Path	string	
fileOwner	File Owner	string	
fileDesc	File Description	string	
user	User	string	
userId	User Id	string	
accessTime	Access Time	Date	
accountName	Account Name	string	
fileId	File Id	string	
fileVersion	File Version	string	
targetHashCode	Target Hash Code	string	

EventType: PH_DEV_MON_BOX_FILE_MODIFY**Description:** Box.com file modified**Severity:** 9 (High)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
fileType	File Type	string	
targetName	Target Name	string	
fileSize64	File Size64 Bytes	uint64	
filePath	File Path	string	
fileOwner	File Owner	string	
fileDesc	File Description	string	
user	User	string	
userId	User Id	string	
accessTime	Access Time	Date	
accountName	Account Name	string	
fileId	File Id	string	
fileVersion	File Version	string	
targetHashCode	Target Hash Code	string	

EventType: PH_DEV_MON_BOX_FILE_SHARE**Description:** Box.com file sharing properties**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

Id	Display name	Type	Description
fileType	File Type	string	
targetName	Target Name	string	
fileSize64	File Size64 Bytes	uint64	
filePath	File Path	string	
fileOwner	File Owner	string	
fileDesc	File Description	string	
accountName	Account Name	string	
fileId	File Id	string	
fileVersion	File Version	string	
infoURL	Informational URL	string	This field captures an URL if present in an event
downloadURL	Download URL	string	
filePasswordEnabled	File Password Enabled	string	
filePreviewEnabled	File Preview Enabled	string	
fileDownloadEnabled	File Download Enabled	string	
fileUnshareAtTime	File Unshare At Time	Date	
filePreviewCount	File Preview Count	uint64	
fileDownloadCount	File Download Count	uint64	

EventType: PH_DEV_MON_CBQOS_CMSTAT

Description: Cisco Class-Based QoS ClassMap related metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
qosPolicy	CBQoS Policy Name	string	Class Based QoS (CSQoS) Policy Name. This parameter is set by CBQoS monitoring.
qosClass	CBQoS Class Name	string	Class Based QoS (CSQoS) Class Name. This parameter is set by CBQoS monitoring.
qosPrePoliceRate	CBQoS PrePolice KBps	double	The rate (in KBytes/sec) of pre-policed Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosPostPoliceRate	CBQoS PostPolice KBps	double	The rate (in KBytes/sec) of post-policed Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosDropRate	CBQoS Drop KBps	double	The rate (in KBytes/sec) of dropped Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosDropPct	CBQoS Drop Pct	double	Dropped traffic percentage of Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.

EventType: PH_DEV_MON_CBQOS_POLICESTAT

Description: Cisco Class-Based QoS Police Action related metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.
qosPolicy	CBQoS Policy Name	string	Class Based QoS (CSQoS) Policy Name. This parameter is set by CBQoS monitoring.

Id	Display name	Type	Description
qosClass	CBQoS Class Name	string	Class Based QoS (CSQoS) Class Name. This parameter is set by CBQoS monitoring.
qosConformRate	CBQoS Conform KBps	double	The rate (in KBytes/sec) of conforming Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosExceedRate	CBQoS Exceeded KBps	double	The rate (in KBytes/sec) of exceeding Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosViolateRate	CBQoS Violated KBps	double	The rate (in KBytes/sec) of violating Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.

EventType: PH_DEV_MON_CBQOS_QUEUESTAT

Description: Cisco Class-Based QoS Queueing Action related metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.
qosPolicy	CBQoS Policy Name	string	Class Based QoS (CSQoS) Policy Name. This parameter is set by CBQoS monitoring.
qosClass	CBQoS Class Name	string	Class Based QoS (CSQoS) Class Name. This parameter is set by CBQoS monitoring.
qosCurrQueue	CBQoS Curr Queue Length	uint32	Current Queue length in Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosMaxQueue	CBQoS Max Queue Length	uint32	Maximum Queue length in Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosDiscardPkt	CBQoS Discarded Pkt	uint32	

EventType: PH_DEV_MON_CCM_CTI_STAT**Description:** Cisco Call Manager CTI device status**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	
ccmStatus	CCM Status	string	
errReason	Reason for Error	string	This is the reason for an error if given.
lastRegTime	Last Registered Time	Date	

EventType: PH_DEV_MON_CCM_CTI_STAT_CHANGE**Description:** Cisco Call Manager CTI device status changed**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
prevCCMStatus	Prev CCM Status	string	
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_DEL_CTI

Description: Cisco Call Manager CTI device deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_DEL_GW

Description: Cisco Call Manager Gateway deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_DEL_H323

Description: Cisco Call Manager H323 device deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_DEL_MEDIA

Description: Cisco Call Manager Media device deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_DEL_SIP_TRUNK

Description: Cisco Call Manager SIP Trunk Deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_DEL_VM

Description: Cisco Call Manager Voice mail device deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_GLOBAL_INFO

Description: Cisco Call Manager Global Device Info

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
regPhone	Registered Phones	uint32	
unregPhone	Unregistered Phones	uint32	
rejPhone	Rejected Phones	uint32	
regGw	Registered Gateways	uint32	
unregGw	Unregistered Gateways	uint32	
rejGw	Rejected Gateways	uint32	
regMedia	Registered Media	uint32	
unregMedia	Unregistered Media	uint32	
rejMedia	Rejected Media	uint32	
regVM	Registered VMail	uint32	
unregVM	Unregistered VMail	uint32	
rejVM	Rejected VMail	uint32	
sipTrunk	SIP Trunks	uint32	

EventType: PH_DEV_MON_CCM_GW_STAT**Description:** Cisco Call Manager Gateway Status**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	
ccmStatus	CCM Status	string	
errReason	Reason for Error	string	This is the reason for an error if given.
lastRegTime	Last Registered Time	Date	

EventType: PH_DEV_MON_CCM_GW_STAT_CHANGE**Description:** Cisco Call Manager Gateway Status Change**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
prevCCMStatus	Prev CCM Status	string	
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_H323_STAT

Description: Cisco Call Manager H323 Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	
ccmStatus	CCM Status	string	
lastRegTime	Last Registered Time	Date	

EventType: PH_DEV_MON_CCM_H323_STAT_CHANGE

Description: Cisco Call Manager H323 Status Change

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
prevCCMStatus	Prev CCM Status	string	
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_MEDIA_STAT

Description: Cisco Call Manager Media device Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	

Id	Display name	Type	Description
ccmStatus	CCM Status	string	
errReason	Reason for Error	string	This is the reason for an error if given.
lastRegTime	Last Registered Time	Date	

EventType: PH_DEV_MON_CCM_MEDIA_STAT_CHANGE

Description: Cisco Call Manager Media device status change

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
prevCCMStatus	Prev CCM Status	string	
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_NEW_CTI

Description: Cisco Call Manager CTI device added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_NEW_GW

Description: Cisco Call Manager Gateway added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_NEW_H323

Description: Cisco Call Manager H323 device added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_NEW_MEDIA

Description: Cisco Call Manager Media device added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_NEW_SIP_TRUNK

Description: Cisco Call Manager SIP Trunk Added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_NEW_VM

Description: Cisco Call Manager Voice Mail device added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_SIP_TRUNK_STAT

Description: Cisco Call Manager SIP Trunk Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	
srcProto	Source Application Protocol	string	
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destProto	Destination Application Protocol	string	
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_DEV_MON_CCM_VM_STAT

Description: Cisco Call Manager Voice Mail Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	
ccmStatus	CCM Status	string	
errReason	Reason for Error	string	This is the reason for an error if given.
lastRegTime	Last Registered Time	Date	

EventType: PH_DEV_MON_CCM_VM_STAT_CHANGE

Description: Cisco Call Manager Voice Mail Status Change

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
prevCCMStatus	Prev CCM Status	string	
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CHANGE_CUST_CONFIG

Description: Config Change detected by custom script

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oldSVNVersion	Old SVN Version	uint32	
newSVNVersion	New SVN Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_CHANGE_INST_SW

Description: New software (un)installed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oldSVNVersion	Old SVN Version	uint32	
newSVNVersion	New SVN Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_CHANGE_RUN_CONFIG**Description:** Running config changed**Severity:** 5 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oldSVNVersion	Old SVN Version	uint32	
newSVNVersion	New SVN Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_CHANGE_RUN_SW**Description:** Running apps changed**Severity:** 5 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_CHANGE_STARTUP_CONFIG**Description:** Startup config changed**Severity:** 5 (Medium)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oldSVNVersion	Old SVN Version	uint32	
newSVNVersion	New SVN Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_CISCO_NBAR_STAT

Description: Cisco NBAR statistics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.
appTransportProto	Application Protocol	string	
totFlows	Total Flows	uint32	Total number of Total (Sent plus Received) Flows. Used in Netflow.
recvFlows	Received Flows	uint32	Total number of Received Flows. Used in Netflow.
sentFlows	Sent Flows	uint32	Total number of Sent Flows. Used in Netflow.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.

Id	Display name	Type	Description
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
totBitsPerSec	Total Bit Rate	double	Total (Sent plus Received) bits/sec through an interface
recvBitsPerSec	Received Bit Rate	double	
sentBitsPerSec	Sent Bit Rate	double	

EventType: PH_DEV_MON_CISCO_RAS_VPN_MET

Description: Remote Access VPN metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
localVpnIpAddr	Local VPN Tunnel IP	IP	
ispVpnIpAddr	ISP VPN IP	IP	
user	User	string	
userGrp	User Group	string	
tunnelStatus	Tunnel Status	string	
tunnelUpTime	Tunnel Uptime	uint64	
rasSessProto	RAS Session Protocol	string	
authenMethod	Authentication Method	string	
authorMethod	Authorization Method	string	
encryptAlgo	Encryption Algorithm	string	

Id	Display name	Type	Description
authenAlgo	Authentication Algorithm	string	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.
sentPktDrop	Sent Packet Drop	uint64	
recvPktDrop	Recv Packet Drop	uint64	

EventType: PH_DEV_MON_CISCO_VPN_P1_TUNNEL_MET

Description: IPSec P1 Tunnel metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
localVpnIpAddr	Local VPN Tunnel IP	IP	
remoteVpnIpAddr	Remote VPN Tunnel IP	IP	
tunnelStatus	Tunnel Status	string	

Id	Display name	Type	Description
tunnelUpTime	Tunnel Uptime	uint64	
sentBitsPerSec	Sent Bit Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
recvBitsPerSec	Received Bit Rate	double	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPktDrop	Sent Packet Drop	uint64	
sentExchReject	Sent Exch Reject	uint64	
sentExchInvalid	Sent Exch Invalid	uint64	
recvPktDrop	Recv Packet Drop	uint64	
recvExchReject	Recv Exch Reject	uint64	
recvExchInvalid	Recv Exch Invalid	uint64	

EventType: PH_DEV_MON_CISCO_VPN_P2_TUNNEL_MET

Description: IPSec P2 Tunnel metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
localVpnIpAddr	Local VPN Tunnel IP	IP	

Id	Display name	Type	Description
remoteVpnIpAddr	Remote VPN Tunnel IP	IP	
tunnelStatus	Tunnel Status	string	
tunnelUpTime	Tunnel Uptime	uint64	
sentBitsPerSec	Sent Bit Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
recvBitsPerSec	Received Bit Rate	double	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPktDrop	Sent Packet Drop	uint64	
sentAuthFail	Sent Auth Fail	uint64	
sentEncryptFail	Sent Encrypt Fail	uint64	
recvPktDrop	Recv Packet Drop	uint64	
recvAuthFail	Recv Auth Fail	uint64	
recvDecryptFail	Recv Decrypt Fail	uint64	
recvReplayFail	Recv Replay Fail	uint64	

EventType: PH_DEV_MON_CISCO_WLAN_RADIO_METRIC

Description: WLAN Radio interface metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
devPort	Device Port	string	Name of the physical network port a device
wlanProtocol	WLAN Protocol	string	WLAN Protocol found in SNMP based WLAN monitoring
ifOperStatus	Interface Oper Status	string	
wlanUserCount	WLAN User count	uint32	WLAN User count found in SNMP based WLAN monitoring
wlanSuppChannels	WLAN Supported Channels	string	WLAN Supported Channels found in SNMP based WLAN monitoring
wlanChannelId	WLAN Channel Id	uint32	WLAN Channel Id found in SNMP based WLAN monitoring
wlanSendUtil	WLAN Transmit Util	uint32	WLAN Transmit Util found in SNMP based WLAN monitoring
wlanRecvUtil	WLAN Receive Util	uint32	WLAN Receive Util found in SNMP based WLAN monitoring
wlanChannelUtil	WLAN Channel Util	uint32	WLAN Channel Util found in SNMP based WLAN monitoring
wlanPoorSNRUserCount	WLAN Poor SNR User count	uint32	WLAN Poor SNR User count found in SNMP based WLAN monitoring
ifLoadProfile	WLAN Interface Load Profile	string	WLAN Interface Load Profile found in SNMP based WLAN monitoring
ifIntefProfile	WLAN Interface Intereference Profile	string	WLAN Interface Intereference Profile found in SNMP based WLAN monitoring
ifCoverageProfile	WLAN Interface Coverage Profile	string	WLAN Interface Coverage Profile found in SNMP based WLAN monitoring
ifNoiseProfile	WLAN Interface Noise Profile	string	WLAN Interface Noise Profile found in SNMP based WLAN monitoring

EventType: PH_DEV_MON_CITRIX_SDWAN_INTF

Description: Citrix SD-WAN Interface metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
ifInteflndx	WLAN Interface Intereference Index	uint32	WLAN Interface Intereference Index found in SNMP based WLAN monitoring
intfName	Host Interface Name	string	Name of a network interface in a host.
sentBytes	Sent Bytes	uint32	Number of bytes sent by a host. This has 32bit resolution.
sentPkts	Sent Packets	uint32	Number of packets sent by a host. This is 32bit version.
recvBytes	Received Bytes	uint32	Number of bytes received by a host. This has 32bit resolution.
recvPkts	Received Packets	uint32	Number of packets received by a host. This is 32bit version.
droppedBytes	Dropped Bytes	uint32	
totPktDrop	Dropped Packets	uint64	Packets dropped

EventType: PH_DEV_MON_CITRIX_SDWAN_LINK

Description: Citrix SD-WAN Link metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
wanLinkId	Wan link ID	uint32	
wanLinkName	Wan link Name	string	
wanLinkState	Wan link State	uint32	
sentBytes	Sent Bytes	uint32	Number of bytes sent by a host. This has 32bit resolution.

Id	Display name	Type	Description
sentPkts	Sent Packets	uint32	Number of packets sent by a host. This is 32bit version.
recvBytes	Received Bytes	uint32	Number of bytes received by a host. This has 32bit resolution.
recvPkts	Received Packets	uint32	Number of packets received by a host. This is 32bit version.
droppedBytes	Dropped Bytes	uint32	
totPktDrop	Dropped Packets	uint64	Packets dropped
addressType	Address Type	string	
serverIpAddr	Server IP	IP	
lanToWanRate	Lan To Wan Rate	uint64	
wanToLanRate	Wan To Lan Rate	uint64	
lanToWanAllowedRate	Lan To Wan Allowed Rate	uint64	
wanToLanAllowedRate	Wan To Lan Allowed Rate	uint64	

EventType: PH_DEV_MON_CLARION_ARRAY_UTIL

Description: Clarion/VNX Storage Array utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	

Id	Display name	Type	Description
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
availDiskMB	Available Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
hwHotSpareDiskCount	Hot Spare Disk Count	uint32	

EventType: PH_DEV_MON_CLARION_DISK_HEALTH

Description: Clarion/VNX Disk health

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
totDisk	Total Disk Count	uint32	Total number of Disks
totalDiskMB	Total Disk MB	uint32	
activeDisk	Active Disk Count	uint32	Total number of Active Disks
failedDisk	Failed Disk Count	uint32	Total number of Failed Disks
spareDisk	Spare Disk Count	uint32	Total number of Spare Disks

EventType: PH_DEV_MON_CLARION_HOST_CONN

Description: Host to Clarion/VNX Fiber channel Connections

Severity: 1 (Low)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcWWN	Source FiberChannel WWN Id	string	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
spPortName	SAN Storage Port Name	string	
fcLoginStatus	SAN FC Login Status	uint32	
fcRegStatus	SAN FC Registration Status	uint32	
lunNameList	SAN LUN Name List	string	
sgName	SAN Storage Group Name	string	

EventType: PH_DEV_MON_CLARION_LUN_UTIL**Description:** Clarion/VNX LUN utilization metric**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
lunName	LUN Name	string	
lunNumber	LUN Number	uint32	

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	

EventType: PH_DEV_MON_CLARION_PER_HOST_LUN_UTIL

Description: Per host Clarion/VNX LUN utilization metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
lunName	LUN Name	string	
lunNumber	LUN Number	uint32	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
pollIntv	Polling Interval	uint32	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	

EventType: PH_DEV_MON_CLARION_PORT_UTIL

Description: Clarion/VNX Storage Port utilization metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
spPortName	SAN Storage Port Name	string	

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	

EventType: PH_DEV_MON_CLARION_RG_UTIL

Description: Clarion/VNX RAID Group utilization metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
raidGrpId	RAID Group Id	uint32	
raidType	RAID Type	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	

Id	Display name	Type	Description
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	

EventType: PH_DEV_MON_CLARION_SP_UTIL

Description: Clarion/VNX Storage Processor utilization metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
spName	SAN Storage Processor Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
cpuUtil	CPU Util	double	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	

EventType: PH_DEV_MON_CLARION_STORAGE_USAGE**Description:** Clarion/VNX Storage space utilization**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
usageType	Usage Type	string	
diskUsage	Disk Used MB	uint64	

EventType: PH_DEV_MON_CLARION_STORE_POOL_UTIL**Description:** Clarion/VNX Storage pool utilization**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
spoolName	Storage Pool Name	string	
raidType	RAID Type	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
diskReadReqPerSec	Disk Read Rate req/sec	double	

Id	Display name	Type	Description
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	

EventType: PH_DEV_MON_CLARION_UNREG_HOST

Description: Logged in but not yet registered Host at EMC CLarion

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcWWN	Source FiberChannel WWN Id	string	
spPortName	SAN Storage Port Name	string	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DEV_MON_CLOUD_SERVICE_HEARTBEAT

Description: Cloud service heartbeat

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
reptVendor	Reporting Vendor	string	This field captures the vendor of the reported event
reptModel	Reporting Model	string	This field captures the model of the reported event
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
version	Version	string	
domain	Domain	string	

EventType: PH_DEV_MON_CMDB_DISK_PRUNE_FAILED

Description: CMDB free Disk fell below the low threshold and inspite of pruning older incidents and identity / location data, CMDB free Disk stays below high threshold. User need to reduce the number of months of incidents and identity / location data in CMDB.

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CMDB_DISK_PRUNE_SUCCESS

Description: CMDB free Disk fell below the low threshold and old incidents and identity / location data were pruned to bring the CMDB free Disk above high threshold

Severity: 4 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CUST_FILE_CHANGE_ATTRIB

Description: File or directory ownership or access permission changed

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CUST_FILE_CHANGE_CONTENT

Description: File or directory content hash changed

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CUST_FILE_CREATE

Description: New file or directory created

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CUST_FILE_DELETE

Description: New file or directory deleted

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CUST_FILE_SCAN

Description: Files scanned with hashes

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CUST_TARGET_FILE_CHANGE

Description: Target file content changed from gold standard

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_DATASTORE_UTIL

Description: Datastore utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_DC DIAG

Description: Windows Active Directory DC DIAG command output

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_DD NS_UPDATE_STAT

Description: InfoBlox DDNS Update performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
ddnsUpdateSuccess	DDNS Successful Updates	uint32	
ddnsUpdateFail	DDNS Failed Updates	uint32	
dynDnsUpdRej	Dynamic DNS Update Rejected	uint32	
ddnsUpdatePrereqRej	DDNS Prereq Rejected Updates	uint32	
ddnsUpdateLatency	DDNS Update latency	uint32	
dynDnsUpdTimeout	Dynamic DNS Update Timeout	uint32	

EventType: PH_DEV_MON_DELLFORCE10_EXT_INTF_UTIL

Description: Network Interface extended utilization stats for Dell Force10 device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
intfAlias	Host Interface Alias	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
inVlanPktsPerSec	Recv Valid VLAN Tagged Frame Rate	double	
inOverrunsPerSec	Recv Buffer Overrun Rate	double	
outVlanPktsPerSec	Sent Valid VLAN Tagged Frame rate	double	
outUnderrunsPerSec	Sent Buffer Underrun Rate	double	
outUnicastsPerSec	Sent Unicast Frames rate	double	
outCollisionsPerSec	Sent Frame Collision rate	double	
outWredDropsPerSec	Sent WRED Drop Rate	double	

EventType: PH_DEV_MON_DELL_BLADE_POWER_STATUS

Description: Dell Blade Server Chassis Power Utilization metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
maxSpecEnvPower	Max Spec Power Watt	double	
potentialEnvPower	Potential Power Watt	double	
idleEnvPower	Idle Power Watt	double	

Id	Display name	Type	Description
surplusEnvPower	Surplus Power Watt	double	
peakEnvPower	Peak Power Watt	double	
minEnvPower	Minimum Power Watt	double	
envPower	Power Watt	double	
envCurrentAmp	Current Amp	double	

EventType: PH_DEV_MON_DELL_BLADE_PSU_STATUS

Description: Dell Blade Server Power Supply Utilization metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorLoc	Sensor Location	string	
envPower	Power Watt	double	
envCurrentAmp	Current Amp	double	
envVoltage	Voltage	double	

EventType: PH_DEV_MON_DELTA_CONFIG

Description: Running config different than startup config

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
startUpConfVer	StartUp Config Version	uint32	
runningConfVer	Running Config Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_DGA_DETECTED

Description: FortiSIEM detected host names created via Domain Generation Algorithm

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
relayDevIpAddr	Relaying IP	IP	Relaying IP is most commonly used to specify the log relay appliance, usually a collector.
relayDevName	Relaying Device	string	This is the hostname of the relaying device, a log relay, which is most typically a FortiSIEM collector.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
domainEntropy	Domain Name Entropy	double	

EventType: PH_DEV_MON_DHCP_SUBNET_USAGE**Description:** InfoBlox DHCP subnet usage metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
dhcpSubnetAddr	DHCP Subnet Address	IP	
dhcpSubnetMask	DHCP Subnet Mask	IP	
dhcpSubnetUsed	DHCP Subnet Usage pct	uint32	

EventType: PH_DEV_MON_DISK_IO_UTIL**Description:** Disk IO Statistics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskIOUtil	Disk IO Util	double	
devDiskRWLatency	Disk Read/Write Latency	double	

Id	Display name	Type	Description
appDiskRWLatency	Disk Appl Read/Write Latency	double	
diskTfrKBytesPerSec	Disk Transfer Rate KBps	double	
diskNumofSeeksPerSec	Disk Number of Seeks	double	
diskType	Disk Type	string	
pollIntv	Polling Interval	uint32	
devDiskRdLatency	Disk Read Latency ms	double	
devDiskWrLatency	Disk Write Latency ms	double	
diskQLen	Disk Queue Length	uint32	

EventType: PH_DEV_MON_DISK_MON_SKIP

Description: Disk/Volume Monitoring skipped by policy

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	

EventType: PH_DEV_MON_DNS_CLUST_REPL_STAT

Description: InfoBlox DNS CLuster replication metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
dnsReplQueueStatus	DNS Replication Queue Status	string	
dnsSentQueueFromMaster	DNS Sent Queue From Master	uint32	
dnsLastSentTimeFromMaster	DNS Sent Time From Master	string	
dnsSentQueueToMaster	DNS Sent Queue To Master	uint32	
dnsLastSentTimeToMaster	DNS Sent Time To Master	string	

EventType: PH_DEV_MON_DNS_PERF_STAT

Description: InfoBlox DNS Performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
nonAuthDNSQueryCount	NonAuth DNS Query Count	uint32	
nonAuthDNSAvgLatency	Avg NonAuth DNS Latency ms	uint32	
authDNSQueryCount	Auth DNS Query Count	uint32	

Id	Display name	Type	Description
authDNSAvgLatency	Avg Auth DNS Latency ms	uint32	
dnsInvalidPort	Invalid DNS Port Response	uint32	
dnsInvalidTxId	Invalid DNS TXID Response	uint32	

EventType: PH_DEV_MON_DNS_ZONETX_MET

Description: InfoBlox DNS Zone Transfer metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
dnsZone	DNS Zone Name	string	
dnsRespSent	DNS Responses Sent	uint32	
dnsFailedQuery	DNS Failed Queries	uint32	
dnsReferral	DNS Referrals	uint32	
dnsQueryNxRecord	DNS Non-existent Record Queries	uint32	
dnsQueryNxDomain	DNS Non-existent Domain Queries	uint32	
dnsRecQueryRecv	Recursive DNS Query Recvd	uint32	

EventType: PH_DEV_MON_DST_AD_REPL_STAT

Description: Windows Active Directory Destination REPLSTAT command output

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_EBS_METRIC

Description: AWS EBS metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
volumeId	AWS Volume Id	string	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
ioReadsPerSec	Total Read I/Os Rate	double	
ioWritesPerSec	Total Write I/Os Rate	double	
diskQLen	Disk Queue Length	uint32	

EventType: PH_DEV_MON_EC2_INSTANCE_DOWN

Description: AWS EC2 instance went down

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
ec2InstanceId	EC2 Instance Id	string	
accountId	Account Id	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_EC2_INSTANCE_UP

Description: AWS EC2 instance came back up

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
ec2InstanceId	EC2 Instance Id	string	
accountId	Account Id	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_EC2_METRIC

Description: Amazon Web Services EC2 status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cpuUtil	CPU Util	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	

EventType: PH_DEV_MON EMC_DATADOMAIN_DISK_PERF

Description: EMC Data Domain disk performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
diskSectorsReadPerSec	Disk Sector Reads/sec	double	

Id	Display name	Type	Description
diskSectorsWrittenPerSec	Disk Sector Writes/sec	double	
diskTfrKBytesPerSec	Disk Transfer Rate KBps	double	
diskIOUtil	Disk IO Util	double	
hwDiskStatus	Hardware Disk Status	uint16	Hardware Disk Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)

EventType: PH_DEV_MON EMC_DATADOMAIN_OVERALL_PERF

Description: EMC Data Domain overall performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskIOUtil	Disk IO Util	double	
nvrReadKBytesPerSec	NVRAM Reads KBps	double	
nvrWriteKBytesPerSec	NVRAM Writes KBps	double	
replInKBytesPerSec	Replication Recvd KBps	double	
replOutKBytesPerSec	Replication Writes KBps	double	
nfsOpsPerSec	NFS Request Rate	double	
nfsProcPercentage	NFS Processing Pct	double	
nfsSendPercentage	NFS Send Pct	double	
nfsReceivePercentage	NFS Recv Pct	double	
cifsOpsPerSec	CIFS Request Rate	double	

EventType: PH_DEV_MON_EQL_CONN_MET

Description: EqualLogic connection performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
sanConnCount	SAN Connection Count	uint32	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
devDiskRdLatency	Disk Read Latency ms	double	
devDiskWrLatency	Disk Write Latency ms	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	

EventType: PH_DEV_MON_EQL_DISK_HEALTH

Description: EqualLogic disk status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
totDisk	Total Disk Count	uint32	Total number of Disks
activeDisk	Active Disk Count	uint32	Total number of Active Disks
failedDisk	Failed Disk Count	uint32	Total number of Failed Disks
spareDisk	Spare Disk Count	uint32	Total number of Spare Disks

EventType: PH_DEV_MON_EQL_DISK_MET

Description: EqualLogic disk level performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskIOUtil	Disk IO Util	double	
ioQueue	Disk IO Queue	uint32	
diskTransferRate	Disk Transfer Rate/sec	double	

EventType: PH_DEV_MON_EQL_GROUP_MET

Description: EqualLogic group level performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
totalStorageMB	Total Storage MB	uint32	
usedStorageMB	Used Storage MB	uint32	
resvStorageMB	Reserved Storage MB	uint32	
resvUsedStorageMB	Reserved Used Disk MB	uint32	
totalVolume	Total Volumes	uint32	
usedVolume	Used Volumes	uint32	
onlineVolume	Online Volumes	uint32	
totalSnapshot	Total Snapshots	uint32	
usedSnapshot	Used Snapshots	uint32	
onlineSnapshot	Online Snapshots	uint32	

EventType: PH_DEV_MON_ESX_DATASTORE_IO

Description: ESX Datastore IO stats

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_ESX_DISK_IO

Description: ESX Disk IO stats

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_ESX_DISK_UTIL

Description: ESX datastore utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_ESX_STATE

Description: Physical Machine State

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_ESX_UPTIME

Description: ESX server's up time

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_EUM_FAIL

Description: Synthetic transaction monitor failed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
appPort	Application Port	string	This field represents the port that an application uses.
appTransportProto	Application Protocol	string	
endUserMonitorName	Synthetic Transaction Monitor Name	string	This is the name of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI
endUserMonitorStep	Synthetic Transaction Monitor Step	string	This is the step of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI. An STM job can have many steps, and an event is generated for every step.

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
srcProto	Source Application Protocol	string	
srcUser	Source User	string	
destUser	Destination User	string	
mailSubject	Mail Subject	string	

EventType: PH_DEV_MON_EUM_INTERNAL_ERR

Description: Synthetic transaction monitoring failed because of internal error

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
appPort	Application Port	string	This field represents the port that an application uses.
appTransportProto	Application Protocol	string	
endUserMonitorName	Synthetic Transaction Monitor Name	string	This is the name of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
srcProto	Source Application Protocol	string	
srcUser	Source User	string	
destUser	Destination User	string	
mailSubject	Mail Subject	string	

EventType: PH_DEV_MON_EUM_STATUS

Description: Synthetic transaction monitor status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
appPort	Application Port	string	This field represents the port that an application uses.
appTransportProto	Application Protocol	string	
endUserMonitorName	Synthetic Transaction Monitor Name	string	This is the name of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI

Id	Display name	Type	Description
endUserMonitorStep	Synthetic Transaction Monitor Step	string	This is the step of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI. An STM job can have many steps, and an event is generated for every step.
newStatus	New Status	string	
sysDownTime	System Downtime	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_EUM_SUCCESS

Description: Synthetic transaction monitor succeeded

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
appPort	Application Port	string	This field represents the port that an application uses.
appTransportProto	Application Protocol	string	
endUserMonitorName	Synthetic Transaction Monitor Name	string	This is the name of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI
endUserMonitorStep	Synthetic Transaction Monitor Step	string	This is the step of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI. An STM job can have many steps, and an event is generated for every step.
appResponseTimeMSec	Application Response Time	uint32	

Id	Display name	Type	Description
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
srcProto	Source Application Protocol	string	
srcUser	Source User	string	
destUser	Destination User	string	
mailSubject	Mail Subject	string	

EventType: PH_DEV_MON_F5_ACTIVE_CONN

Description: F5 Active Connection Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
clientConns	Client Connections	uint64	
serverConns	Server Connections	uint64	
pvaClientConns	PVA Client Connections	uint32	
pvaServerConns	PVA Server Connections	uint32	
sslClientConns	SSL Client Connections	uint32	
sslServerConns	SSL Server Connections	uint32	

EventType: PH_DEV_MON_F5_LTM_NODE_STAT**Description:** F5 LTM Node Statistics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serverIpAddr	Server IP	IP	
statusDetailedReason	Status Detail Reason	string	
ratio	Ratio	double	
monitorState	Monitor State	string	
monitorStatus	Monitor Status	string	
sessionStatus	Session Status	string	
availState	Availability State	string	
enabledState	Enabled State	string	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
recvPktsPerSec	Received Packet Rate	double	Received Packet rate (packets/sec)
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
recvBytesPerSec	Received Byte Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
sentPktsPerSec	Sent Packet Rate	double	Sent Packet rate (packets/sec)
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
sentBytesPerSec	Sent Byte Rate	double	
peakConns	Peak Connections	uint64	
totConns	Total Connections	uint64	
totConnsPerSec	Total Connections/sec	double	

Id	Display name	Type	Description
activeConns	Active Connection	uint64	
pvaRecvPkts	Received PVA Packets	uint64	
pvaRecvPktsPerSec	Received PVA Pkts/sec	double	
pvaRecvBytes	Received PVA Bytes	uint64	
pvaRecvBytesPerSec	Received PVA Bps	double	
pvaSentPkts	Sent PVA Packets	uint64	
pvaSentPktsPerSec	Sent PVA Pkts/sec	double	
pvaSentBytes	Sent PVA Bytes	uint64	
pvaSentBytesPerSec	Sent PVA Bps	double	
pvaMaxConns	Max PVA Connections	uint64	
pvaTotConns	Total PVA Connections	uint64	
pvaTotConnsPerSec	PVA Connections/sec	double	
pvaCurrConns	Current PVA Connections	uint64	
totRequests	Total Requests	uint64	
totRequestsPerSec	Requests/sec	double	
pvaAssistTotConns	Total PVA Assisted Connections	uint64	
pvaAssistTotConnsPerSec	PVA Assisted Connections/sec	double	
pvaAssistCurrConns	Assisted PVA Connections	uint64	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_LTM_POOL_MEMBER_STAT

Description: F5 LTM Pool Member Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serverIpAddr	Server IP	IP	
poolName	Pool Name	string	
statusDetailedReason	Status Detail Reason	string	
memberPort	Member Port	uint16	
ratio	Ratio	double	
monitorState	Monitor State	string	
monitorStatus	Monitor Status	string	
sessionStatus	Session Status	string	
availState	Availability State	string	
enabledState	Enabled State	string	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
recvPktsPerSec	Received Packet Rate	double	Received Packet rate (packets/sec)
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
recvBytesPerSec	Received Byte Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
sentPktsPerSec	Sent Packet Rate	double	Sent Packet rate (packets/sec)
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
sentBytesPerSec	Sent Byte Rate	double	
peakConns	Peak Connections	uint64	
totConns	Total Connections	uint64	
totConnsPerSec	Total Connections/sec	double	
activeConns	Active Connection	uint64	
pvaRecvPkts	Received PVA Packets	uint64	
pvaRecvPktsPerSec	Received PVA Pkts/sec	double	

Id	Display name	Type	Description
pvaRecvBytes	Received PVA Bytes	uint64	
pvaRecvBytesPerSec	Received PVA Bps	double	
pvaSentPkts	Sent PVA Packets	uint64	
pvaSentPktsPerSec	Sent PVA Pkts/sec	double	
pvaSentBytes	Sent PVA Bytes	uint64	
pvaSentBytesPerSec	Sent PVA Bps	double	
pvaMaxConns	Max PVA Connections	uint64	
pvaTotConns	Total PVA Connections	uint64	
pvaTotConnsPerSec	PVA Connections/sec	double	
pvaCurrConns	Current PVA Connections	uint64	
totRequests	Total Requests	uint64	
totRequestsPerSec	Requests/sec	double	
pvaAssistTotConns	Total PVA Assisted Connections	uint64	
pvaAssistTotConnsPerSec	PVA Assisted Connections/sec	double	
pvaAssistCurrConns	Assisted PVA Connections	uint64	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_LTM_POOL_STAT

Description: F5 LTM Pool Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
poolName	Pool Name	string	
poolLbMode	Pool Loadbalance Mode	string	
poolMemberCount	Pool Member Count	uint64	
availState	Availability State	string	
enabledState	Enabled State	string	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
recvPktsPerSec	Received Packet Rate	double	Received Packet rate (packets/sec)
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
recvBytesPerSec	Received Byte Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
sentPktsPerSec	Sent Packet Rate	double	Sent Packet rate (packets/sec)
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
sentBytesPerSec	Sent Byte Rate	double	
peakConns	Peak Connections	uint64	
totConns	Total Connections	uint64	
totConnsPerSec	Total Connections/sec	double	
activeConns	Active Connection	uint64	
pvaRecvPkts	Received PVA Packets	uint64	
pvaRecvPktsPerSec	Received PVA Pkts/sec	double	
pvaRecvBytes	Received PVA Bytes	uint64	
pvaRecvBytesPerSec	Received PVA Bps	double	
pvaSentPkts	Sent PVA Packets	uint64	
pvaSentPktsPerSec	Sent PVA Pkts/sec	double	
pvaSentBytes	Sent PVA Bytes	uint64	
pvaSentBytesPerSec	Sent PVA Bps	double	
pvaMaxConns	Max PVA Connections	uint64	
pvaTotConns	Total PVA Connections	uint64	
pvaTotConnsPerSec	PVA Connections/sec	double	

Id	Display name	Type	Description
pvaCurrConns	Current PVA Connections	uint64	
pvaAssistTotConns	Total PVA Assisted Connections	uint64	
pvaAssistTotConnsPerSec	PVA Assisted Connections/sec	double	
pvaAssistCurrConns	Assisted PVA Connections	uint64	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_LTM_VIRT_ADDR_STAT

Description: F5 LTM Virtual Address Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serverIpAddr	Server IP	IP	
availState	Availability State	string	
enabledState	Enabled State	string	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
recvPktsPerSec	Received Packet Rate	double	Received Packet rate (packets/sec)
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
recvBytesPerSec	Received Byte Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
sentPktsPerSec	Sent Packet Rate	double	Sent Packet rate (packets/sec)

Id	Display name	Type	Description
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
sentBytesPerSec	Sent Byte Rate	double	
peakConns	Peak Connections	uint64	
totConns	Total Connections	uint64	
totConnsPerSec	Total Connections/sec	double	
activeConns	Active Connection	uint64	
pvaRecvPkts	Received PVA Packets	uint64	
pvaRecvPktsPerSec	Received PVA Pkts/sec	double	
pvaRecvBytes	Received PVA Bytes	uint64	
pvaRecvBytesPerSec	Received PVA Bps	double	
pvaSentPkts	Sent PVA Packets	uint64	
pvaSentPktsPerSec	Sent PVA Pkts/sec	double	
pvaSentBytes	Sent PVA Bytes	uint64	
pvaSentBytesPerSec	Sent PVA Bps	double	
pvaMaxConns	Max PVA Connections	uint64	
pvaTotConns	Total PVA Connections	uint64	
pvaTotConnsPerSec	PVA Connections/sec	double	
pvaCurrConns	Current PVA Connections	uint64	
pvaAssistTotConns	Total PVA Assisted Connections	uint64	
pvaAssistTotConnsPerSec	PVA Assisted Connections/sec	double	
pvaAssistCurrConns	Assisted PVA Connections	uint64	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_LTM_VIRT_SERVER_STAT

Description: F5 LTM Virtual Server Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
virtServerName	Virtual Server name	string	
statusDetailedReason	Status Detail Reason	string	
virtServerPort	Virtual Server Port	uint16	
availState	Availability State	string	
enabledState	Enabled State	string	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
recvPktsPerSec	Received Packet Rate	double	Received Packet rate (packets/sec)
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
recvBytesPerSec	Received Byte Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
sentPktsPerSec	Sent Packet Rate	double	Sent Packet rate (packets/sec)
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
sentBytesPerSec	Sent Byte Rate	double	
peakConns	Peak Connections	uint64	
totConns	Total Connections	uint64	
totConnsPerSec	Total Connections/sec	double	
activeConns	Active Connection	uint64	
pvaRecvPkts	Received PVA Packets	uint64	
pvaRecvPktsPerSec	Received PVA Pkts/sec	double	
pvaRecvBytes	Received PVA Bytes	uint64	
pvaRecvBytesPerSec	Received PVA Bps	double	
pvaSentPkts	Sent PVA Packets	uint64	
pvaSentPktsPerSec	Sent PVA Pkts/sec	double	
pvaSentBytes	Sent PVA Bytes	uint64	

Id	Display name	Type	Description
pvaSentBytesPerSec	Sent PVA Bps	double	
pvaMaxConns	Max PVA Connections	uint64	
pvaTotConns	Total PVA Connections	uint64	
pvaTotConnsPerSec	PVA Connections/sec	double	
pvaCurrConns	Current PVA Connections	uint64	
totRequests	Total Requests	uint64	
totRequestsPerSec	Requests/sec	double	
pvaAssistTotConns	Total PVA Assisted Connections	uint64	
pvaAssistTotConnsPerSec	PVA Assisted Connections/sec	double	
pvaAssistCurrConns	Assisted PVA Connections	uint64	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_NEW_CONN

Description: F5 New Connection Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
tcpClientAcceptsPerSec	TCP Client Connection Accept Rate	double	
tcpClientConnsPerSec	TCP Client Connection Rate	double	
serverConnsPerSec	Server Connection Rate	double	
clientConnsPerSec	Client Connection Rate	double	

Id	Display name	Type	Description
pvaClientConnsPerSec	PVA Client Connection Rate	double	
pvaServerConnsPerSec	PVA Server Connection Rate	double	
sslClientConnsPerSec	SSL Client Connection Rate	double	
sslServerConnsPerSec	SSL Server Connection Rate	double	
httpRequestsPerSec	HTTP Request Rate	double	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_RAM_CACHE

Description: F5 RAM Cache Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
httpRAMCacheHitRate	HTTP Cache Hit Rate	double	
httpRAMCacheHitByteRate	HTTP Cache Byte Hit Rate	double	
httpRAMCacheEvictionRate	HTTP cache Eviction Rate	double	

EventType: PH_DEV_MON_F5_THROUGHPUT

Description: F5 Throughput Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
clientTotBitsPerSec	Client Total bps	double	
serverTotBitsPerSec	Server Total bps	double	
httpCompressionBitsPerSec	HTTP Compression bps	double	
clientInBitsPerSec	Client Recv bps	double	
clientOutBitsPerSec	Client Sent bps	double	
serverInBitsPerSec	Server Recv bps	double	
serverOutBitsPerSec	Server Sent bps	double	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_TMM_MEM_UTIL

Description: F5 per TMM memory utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
tmmName	F5 TMM Name	string	
memUtil	Memory Util	double	
totalMemKB	Total Memory	uint32	
freeMemKB	Free Memory	uint32	
usedMemKB	Used Memory	uint32	

EventType: PH_DEV_MON_FGT_SEC_POSTURE_DETAILS

Description: FortiGate Security Posture - Per device audit details

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
type	Type	string	
subtype	Subtype	string	
eventSeverityCat	Event Severity Category	string	It takes 3 values - High, Medium and Low based on Event Severity. (1-4 : Low, 5-8 : Medium, 9-10 : High)
deviceType	Device Type	string	
serialNumber	Serial Number	string	
auditScore	Audit Score	double	
status	Status	string	

EventType: PH_DEV_MON_FGT_SEC_POSTURE_DETECTED_ENDPOINTS

Description: FortiGate Security Posture - Detected Endpoint Types

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
totGenericDevs	Total Generic Devices	uint32	
totFortigateDevs	Total FortiGates	uint32	
totFortimgrDevs	Total FortiManager	uint32	

Id	Display name	Type	Description
totFortisandboxDevs	Total FortiSandbox Devices	uint32	
totWindowsDevs	Total Windows Devices	uint32	
totLinuxDevs	Total Linux Devices	uint32	
totAppleDevs	Total Apple Devices	uint32	
totMobileDevs	Total Mobile Devices	uint32	

EventType: PH_DEV_MON_FGT_SEC_POSTURE_FABRIC_GRADE

Description: FortiGate Security Posture - Overall Fabric Grade

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
letterGrade	Letter Grade	string	

EventType: PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_GRADE

Description: FortiGate Security Posture - Per category grade

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
type	Type	string	
gradePercent	Grade Percentage	uint32	
letterGrade	Letter Grade	string	
eventSeverityCat	Event Severity Category	string	It takes 3 values - High, Medium and Low based on Event Severity. (1-4 : Low, 5-8 : Medium, 9-10 : High)
totalNum	Total Number of Items	uint32	

EventType: PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_STATS

Description: FortiGate Security Posture - Per category summary

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
type	Type	string	
totalChecks	Total Checks	uint32	
totalFailedChecks	Total Failed Checks	uint32	
totalExemptChecks	Total Exempt Checks	uint32	
totalPassedChecks	Total Passed Checks	uint32	
totalRecommendations	Total Recommendations	uint32	
auditScore	Audit Score	double	
lowSevCount	Low Severity Count	uint32	
mediumSevCount	Medium Severity Count	uint32	
highSevCount	High Severity Count	uint32	

Id	Display name	Type	Description
criticalSevCount	Critical Severity Count	uint32	

EventType: PH_DEV_MON_FGT_SEC_POSTURE_PER_DEVICE_STATS

Description: FortiGate Security Posture - Per device summary

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
serialNumber	Serial Number	string	
totalChecks	Total Checks	uint32	
totalFailedChecks	Total Failed Checks	uint32	
totalExemptChecks	Total Exempt Checks	uint32	
totalPassedChecks	Total Passed Checks	uint32	
totalRecommendations	Total Recommendations	uint32	
auditScore	Audit Score	double	
lowSevCount	Low Severity Count	uint32	
mediumSevCount	Medium Severity Count	uint32	
highSevCount	High Severity Count	uint32	
criticalSevCount	Critical Severity Count	uint32	

EventType: PH_DEV_MON_FGT_USER_INFO

Description: FortiGate User Device Informational Event

Severity: 4 (Low)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostVendor	Host Vendor	string	This field captures the vendor of the reported event
hostMACAddr	Host MAC	string	Host Layer 2 MAC Address in the log
vdom	Virtual Domain	string	
osName	Operating System Name	string	
osVersion	Operating System Version	string	
userFullName	User Full Name	string	
lastSeenTime	Last Seen Time	Date	
appName	Application Name	string	
user	User	string	
firstSeenTime	First Seen Time	Date	
tagName	Tag Name	string	
emsSerialNumber	FortiEMS Serial Number	string	
srcAppVersion	Source App Version	string	
discoveryDomain	Discovery Domain	string	
purdueLevel	Purdue Level	double	
vulnCount	Vulnerability Count	uint64	
vulnCountCritical	Vulnerability Count Critical	uint16	
vulnCountHigh	Vulnerability Count High	uint16	
vulnCountMedium	Vulnerability Count Medium	uint16	

Id	Display name	Type	Description
vulnCountLow	Vulnerability Count Low	uint16	
vulnCountInfo	Vulnerability Count Info	uint16	

EventType: PH_DEV_MON_FILE_CONTENT_CHANGE

Description: Monitored file modified

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
fileName	File Name	string	
hashCode	Hash Code	string	
oldSVNVersion	Old SVN Version	uint32	
newSVNVersion	New SVN Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	
user	User	string	
hashAlgo	Hash Algorithm	string	

EventType: PH_DEV_MON_FIREAMP_DISCOVERY_CLIENT_APP

Description: FireAMP Client App discovery event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
clientAppId	Client App Id	uint32	
appName	Application Name	string	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_DISCOVERY_NETWORK_PROTOCOL

Description: FireAMP Network App discovery event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_DISCOVERY_OS_FINGERPRINT

Description: FireAMP OS discovery event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
fingerprintId	Fingerprint	string	
osType	Operating System	string	
hostVendor	Host Vendor	string	This field captures the vendor of the reported event
osVersion	Operating System Version	string	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_DISCOVERY_SERVER

Description: FireAMP Server discovery event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
applicationId	Application Id	uint32	
appTransportProto	Application Protocol	string	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_FILE

Description: FireAMP File Analysis event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
envSensorId	Env Sensor Id	string	
deviceTime	Device Time	Date	This is the timestamp as seen in the raw log. This is converted and stored as epoch milliseconds. Note that the deviceTime, or event occur time, is different than the event receive time by the SIEM.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
fileName	File Name	string	
hashAlgo	Hash Algorithm	string	
hashCode	Hash Code	string	
fileSize64	File Size64 Bytes	uint64	
fileDirection	File Direction	uint16	
fireAmpDisposition	FireAmp Disposition	uint16	
fireAmpSperoDisposition	FireAmp Spero Disposition	uint16	
fireAmpFileStorageStatus	FireAmp File Storage Status	uint16	
fireAmpFileAnalysisStatus	FireAmp File Analysis Status	uint16	
threatScore	Threat Score	uint16	
fireAmpFileAction	FireAmp File Action	uint16	
fileType	File Type	string	
applicationId	Application Id	uint32	

Id	Display name	Type	Description
destUserId	Destination User Id	uint32	
infoURL	Informational URL	string	This field captures an URL if present in an event
signatureName	Signature Name	string	
accessCtlPolicyId	Access Control Policy Id	uint32	
srcGeoCountryCode	Source Country Number	uint32	
destGeoCountryCode	Destination Country Number	uint32	
webAppId	Web App Id	uint32	
clientAppId	Client App Id	uint32	
connCounter	Connection Counter	uint64	
connEventTime	Connection Event Time	Date	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_IMPACT_FLAG

Description: FireAMP Impact Flag event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
envSensorId	Env Sensor Id	string	
snortEventId	Snort Event ID	uint64	Event ID of a Snort IPS Device

Id	Display name	Type	Description
deviceTime	Device Time	Date	This is the timestamp as seen in the raw log. This is converted and stored as epoch milliseconds. Note that the deviceTime, or event occur time, is different than the event receive time by the SIEM.
eventType	Event Type	string	This is the unique log name, identifying the product and type of log. This is a key attribute for most queries.
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.
ipsGeneratorId	IPS Generator Id	uint64	
ipsSignatureId	Signature Id	uint64	
ipsClassificationId	IPS Classification Id	uint64	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
fireAmpImpactFlag	FireAmp Impact Flag	uint16	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_INTRUSION

Description: FireAMP Intrusion event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
envSensorId	Env Sensor Id	string	
snortEventId	Snort Event ID	uint64	Event ID of a Snort IPS Device
deviceTime	Device Time	Date	This is the timestamp as seen in the raw log. This is converted and stored as epoch milliseconds. Note that the deviceTime, or event occur time, is different than the event receive time by the SIEM.
eventType	Event Type	string	This is the unique log name, identifying the product and type of log. This is a key attribute for most queries.
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.
ipsGeneratorId	IPS Generator Id	uint64	
ipsSignatureId	Signature Id	uint64	
ipsClassificationId	IPS Classification Id	uint64	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
iocNum	IOC Number	uint32	
fireAmpImpactFlag	FireAmp Impact Flag	uint16	
fireAmpImpact	FireAmp Impact	uint16	
eventAction	Event Action	uint16	This is an unsigned integer boolean. 0 means permitted, 1 means blocked. It is used by various parsers to indicate success / failure or permit/deny.
mplsLabel	MPLS Label	uint32	
hostVLAN	Host VLAN	uint16	Host VLAN Number
userId	User Id	string	

Id	Display name	Type	Description
webAppId	Web App Id	uint32	
clientAppId	Client App Id	uint32	
appProtold	App Proto Id	uint32	
fwRule	Firewall Rule	string	Firewall Rule Name
policyName	Policy Name	string	
srcIntfName	Source Interface Name	string	Name of the network interface through which a packet enters a network device. This information is typically present in Firewall logs.
destIntfName	Destination Interface Name	string	Name of the network interface through which a packet exits a network device. This information is typically present in Firewall logs.
srcFwZone	Source Firewall Zone	string	Source Firewall Zone found in Firewall logs
destFwZone	Destination Firewall Zone	string	Destination Firewall Zone found in Firewall logs
connEventTime	Connection Event Time	Date	
connCounter	Connection Counter	uint64	
srcGeoCountryCode	Source Country Number	uint32	
destGeoCountryCode	Destination Country Number	uint32	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_MALWARE

Description: FireAMP Malware event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
envSensorId	Env Sensor Id	string	
deviceTime	Device Time	Date	This is the timestamp as seen in the raw log. This is converted and stored as epoch milliseconds. Note that the deviceTime, or event occur time, is different than the event receive time by the SIEM.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
fileName	File Name	string	
filePath	File Path	string	
fileSize64	File Size64 Bytes	uint64	
fileType	File Type	string	
fileTimestamp	File Timestamp	Date	
hashAlgo	Hash Algorithm	string	
hashCode	Hash Code	string	
fileDirection	File Direction	uint16	
fireAmpFileAction	FireAmp File Action	uint16	
parentFileName	Parent File Name	string	
parentFileHashCode	Parent File Hash Code	string	
infoURL	Informational URL	string	This field captures an URL if present in an event
threatScore	Threat Score	uint16	

Id	Display name	Type	Description
fireAmpDisposition	FireAmp Disposition	uint16	
fireAmpRetrospectiveDisposition	FireAmp Retrospective Disposition	uint16	
iocNum	IOC Number	uint32	
accessCtlPolicyId	Access Control Policy Id	uint32	
srcGeoCountryCode	Source Country Number	uint32	
destGeoCountryCode	Destination Country Number	uint32	
webAppId	Web App Id	uint32	
clientAppId	Client App Id	uint32	
applicationId	Application Id	uint32	
connEventTime	Connection Event Time	Date	
connCounter	Connection Counter	uint64	
cloudSecIntelId	Cloud Security Intel Id	uint32	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_USER_LOGIN

Description: FireAMP user login event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
deviceTime	Device Time	Date	This is the timestamp as seen in the raw log. This is converted and stored as epoch milliseconds. Note that the deviceTime, or event occur time, is different than the event receive time by the SIEM.
user	User	string	
userId	User Id	string	
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
emailId	Email Id	string	
loginType	Login Type	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FORTIAP_INTF_UTIL

Description: FortiAP interface performance

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_FORTIAP_PERF

Description: FortiAP performance

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_FORTIAP_STAT

Description: FortiAP Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
sysUpTime	System Uptime	uint32	
wtpDaemonUpTime	WLAN AP Daemon Uptime	uint32	WLAN AP Daemon Uptime found in SNMP based WLAN monitoring
wtpSessionUpTime	WLAN AP Session Uptime	uint32	WLAN AP Session Uptime found in SNMP based WLAN monitoring
numWlanClient	WLAN Station Count	uint32	WLAN Station Count found in SNMP based WLAN monitoring
ftntWtpSessionStatus	WLAN AP Session Status	uint32	WLAN AP Session Status found in SNMP based WLAN monitoring
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_FORTIGATE_INTF_UTIL

Description: Fortigate interface performance

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_FORTIGATE_PERF

Description: Fortigate performance

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_FORTIMAIL_SESSION_COUNT

Description: FortiMail session count

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_DEV_MON_FORTIMAIL_SYS_LOAD

Description: FortiMail system load

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
numJob	Average System Job	uint32	

EventType: PH_DEV_MON_FORTINET_PROCESSOR_USAGE

Description: FortiGate Firewall Processor Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cpuName	CPU Name	string	
sysCpuUtil	System CPU Util	double	
userCpuUtil	User CPU Util	double	
cpuUtil	CPU Util	double	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
recvPktsPerSec	Received Packet Rate	double	Received Packet rate (packets/sec)
sentPktsPerSec	Sent Packet Rate	double	Sent Packet rate (packets/sec)
totPktDrop	Dropped Packets	uint64	Packets dropped
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_FORTINET_QOS**Description:** Fortinet QoS metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.
qosClassId	QoS Class Id	uint32	
direction	Direction	string	
guaranteedBandwidth	Guaranteed Bandwidth	double	

Id	Display name	Type	Description
allocatedBandwidth	Allocated Bandwidth	double	
peakBandwidth	Peak Bandwidth	double	
currentBandwidth	Current Bandwidth	double	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.
totPktDrop	Dropped Packets	uint64	Packets dropped

EventType: PH_DEV_MON_FORTISWITCH_PERF

Description: FortiSwitch performance

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_FORTIWLC_QOS_STAT

Description: FortiWLC QoS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
qosSessionCount	QoS Session Count	uint32	
qosH323SessionCount	QoS H.323 Session Count	uint32	
qosSipSessionCount	QoS SIP Session Count	uint32	

Id	Display name	Type	Description
qosSccpSessionCount	QoS SCCP Session Count	uint32	
qosRejectedSessionCount	QoS Rejected Session Count	uint32	
qosRejectedH323SessionCount	QoS Rejected H.323 Session Count	uint32	
qosRejectedSipSessionCount	QoS Rejected SIP Session Count	uint32	
qosRejectedSccpSessionCount	QoS Rejected SCCP Session Count	uint32	
qosPendingSessionCount	QoS Pending Session Count	uint32	
qosH323PendingSessionCount	QoS H.323 Pending Session Count	uint32	
qoSsipPendingSessionCount	QoS SIP Pending Session Count	uint32	
qoSsccpPendingSessionCount	QoS SCCP Pending Session Count	uint32	
qosActiveFlowCount	QoS Active Flow Count	uint32	
qosPendingFlowCount	QoS Pending Flow Count	uint32	

EventType: PH_DEV_MON_FORTIWLC_STATIONS

Description: FortiWLC Station Count

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
station11a	802.11a Station Count	uint32	
station11b	802.11b Station Count	uint32	

Id	Display name	Type	Description
station11bg	802.11bg Station Count	uint32	
stationData	Data Station Copunt	uint32	
stationPhone	Phone Station Count	uint32	
stationWired	Wired Station Count	uint32	
stationUnknown	Unknown Station Count	uint32	

EventType: PH_DEV_MON_FORTIWLC_SYS_THRUPUT

Description: FortiWLC system throughput

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBitsPerSec	Received Bit Rate	double	
sentBitsPerSec	Sent Bit Rate	double	
wlanRecvBitsPerSec	WLAN Recv Rate bps	double	WLAN Recv Rate (in bits/sec)s found in SNMP based WLAN monitoring
wlanSentBitsPerSec	WLAN Sent Rate bps	double	WLAN Sent Rate (in bits/sec) found in SNMP based WLAN monitoring

EventType: PH_DEV_MON_FPC_LIEBERT_METRIC

Description: Liebert FPC metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
outputVoltageXNVolts	Output Voltage X-N	uint32	
outputVoltageYNVolts	Output Voltage Y-N	uint32	
outputVoltageZNVolts	Output Voltage Z-N	uint32	
outputCurrentXAmps	Output Current X Amps	uint32	
outputCurrentYAmps	Output Current Y Amps	uint32	
outputCurrentZAmps	Output Current Z Amps	uint32	
neutralCurrentAmps	Neutral Current Amps	uint32	
groundCurrentAmps	Ground Current Amps	double	
outputPowerWatts	Output Power Watts	uint32	
powerFactor	Power Factor	uint32	
outputFrequency	Output Frequency Hz	uint32	
outputVxTHD	Output Vx THD	double	
outputVyTHD	Output Vy THD	double	
outputVzTHD	Output Vz THD	double	
outputLxTHD	Output lx THD	double	
outputLyTHD	Output ly THD	double	
outputLzTHD	Output lz THD	double	
outputKWh	Output kWh	double	
outputLxCrestFactor	Output lx Crest Factor	double	
outputLyCrestFactor	Output ly Crest Factor	double	
outputLzCrestFactor	Output lz Crest Factor	double	
outputLxKFactor	Output lx K-Factor	double	
outputLyKFactor	Output ly K-Factor	double	
outputLzKFactor	Output lz K-Factor	double	
outputLxCapacity	Output lx Capacity	uint32	
outputLyCapacity	Output ly Capacity	uint32	

Id	Display name	Type	Description
outputLzCapacity	Output lz Capacity	uint32	

EventType: PH_DEV_MON_FW_CONN_UTIL

Description: Firewall connection count stats for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
fwConnCount	Firewall Session	uint32	Number of concurrent sessions, typically found in Stateful Firewall performance statistic log
fwConnPct	Firewall Session Utilization	double	Concurrent sessions utilization defined as the ratio of concurrent sessions and max allowed concurrent sessions, typically found in Stateful Firewall performance statistic log
pollIntv	Polling Interval	uint32	
fwConnMax	Max Firewall Conn	uint32	Maximum number of Firewall Connections reported by Firewalls.
tcpFwConnCount	TCP Connection	uint32	Total number of TCP Connections reported by Firewalls.
udpFwConnCount	UDP Connection	uint32	Total number of UDP Connections reported by Firewalls.
icmpFwConnCount	ICMP Connection	uint32	Total number of ICMP Connections reported by Firewalls.
fwConnRate	Firewall Session Rate	uint32	

EventType: PH_DEV_MON_GITHUB_BRANCH_EVENT

Description: GitHub Branch Create/Delete Event

Severity: 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
branchName	Branch Name	string	
actionName	Notification Action Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_COMMIT

Description: User committed code to a GitHub repository**Severity:** 1 (Low)**Event Category:** 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
comment	Comment	string	
srcFileName	Source File Name	string	
actionName	Notification Action Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_EVENT**Description:** GitHub event**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_FORK_REPOSITORY_EVENT

Description: GitHub Repository Fork Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
newRepoName	New Repository Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_ISSUE_EVENT

Description: GitHub Issue Action Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
title	Title	string	
issueBody	Issue Body	string	
status	Status	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_MEMBER_EVENT

Description: GitHub user membership and permission change event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
memberName	Member Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_ORG_EVENT

Description: GitHub Organization User Block/Unblock Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_PROJECT_EVENT

Description: GitHub Project Action Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
projectName	Project Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_PULL_REQUEST_EVENT

Description: GitHub Pull Request Action Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
title	Title	string	
requestBody	Request Body	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_PULL_REQUEST_REVIEW_EVENT

Description: GitHub Pull Request Review Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
title	Title	string	
requestBody	Request Body	string	
reviewBody	Review Body	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_REPOSITORY_EVENT

Description: GitHub Repository Create/Delete Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_TAG_EVENT

Description: GitHub Tag Create/Delete Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
tagName	Tag Name	string	
actionName	Notification Action Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GLASSFISH_APP

Description: Glassfish application server settings and metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_CONN_STAT

Description: Glassfish http connection statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_CPU

Description: Glassfish CPU usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_DB_POOL

Description: Glassfish database pool metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_EJB

Description: Glassfish EJB metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_JMS

Description: Glassfish JMS usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_MEMORY

Description: Glassfish memory usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_REQUEST_PROCESSOR

Description: Glassfish request processor metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_SERVLET

Description: Glassfish servlet metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_SESSION

Description: Glassfish session metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_THREAD_POOL

Description: Glassfish thread pool usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HARDWARE_STATUS

Description: Overall hardware Health status for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HOST_PERF_STATE**Description:** Host performance monitoring state**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
durationHostNormal	Duration Normal	uint32	
durationHostWarn	Duration Warning	uint32	
durationHostCrit	Duration Critical	uint32	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.

EventType: PH_DEV_MON_HVAC_LIEBERT_METRIC**Description:** Liebert HVAC metric**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envTempDegC	Temperature Celsius	uint32	

Id	Display name	Type	Description
envTempHighThreshDegC	High Temperature Threshold Celsius	uint32	
envTempLowThreshDegC	Low Temperature Threshold Celsius	uint32	
envTempOffHighDegC	Temp Offset High Celsius	uint32	
envTempOffLowDegC	Temp Offset Low Celsius	uint32	
envTempDegF	Temperature Fahrenheit	uint32	
envTempHighThreshDegF	High Temperature Threshold Fahrenheit	uint32	
envTempLowThreshDegF	Low Temperature Threshold Fahrenheit	uint32	
envTempOffHighDegF	Temp Offset High Fahrenheit	uint32	
envTempOffLowDegF	Temp Offset Low Fahrenheit	uint32	
envHumidityRel	Relative Humidity	uint32	
envHumidityRelHighThresh	High Relative Humidity Threshold	uint32	
envHumidityRelLowThresh	Low Relative Humidity Threshold	uint32	
envHumidityOffHigh	Humidity Offset High	uint32	
envHumidityOffLow	Humidity Offset Low	uint32	
lgpSystemState	Liebert HVAC System State	uint16	
lgpDehumidState	Liebert HVAC Dehumidifying State	uint16	

EventType: PH_DEV_MON_HW_AIRFLOW

Description: Airflow measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
envAirFlow	Air Flow 0.1meter/min	uint32	

EventType: PH_DEV_MON_HW_AMP

Description: Current measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
envCurrentAmp	Current Amp	double	

EventType: PH_DEV_MON_HW_AUDIO

Description: Audio sensor measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
envAudioLevel	Audio sensor level	uint32	

EventType: PH_DEV_MON_HW_CAMERA_MOTION

Description: Camera motion sensor measurement**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
cameraMotionSensorVal	Camera Motion Sensor Value	string	

EventType: PH_DEV_MON_HW_CHASSIS_COMP_STAT**Description:** Chassis component environmental measurement**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwCompAdminStateStr	Chassis Com Admin State	string	
hwCompOperStateStr	Chassis Comp Operational State	string	
hwCompSwStateStr	Chassis Comp Software State	string	
envTempDegF	Temperature Fahrenheit	uint32	
envTempHighThreshDegF	High Temperature Threshold Fahrenheit	uint32	

EventType: PH_DEV_MON_HW_CURRENT**Description:** Current measurement**Severity:** 1 (Low)**Event Category:** 3 (System Logs)

EventType: PH_DEV_MON_HW_DEWPT**Description:** Dew point measurement**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
envTempDegC	Temperature Celsius	uint32	
envTempDegF	Temperature Fahrenheit	uint32	

EventType: PH_DEV_MON_HW_DOOR_SWITCH**Description:** Door switch sensor measurement**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device

Id	Display name	Type	Description
doorSwitchSensorVal	Door Switch Sensor Value	string	

EventType: PH_DEV_MON_HW_DRY_CONTACT

Description: Dry contact sensor measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
dryContactSensorVal	Dry Contact Sensor Value	string	

EventType: PH_DEV_MON_HW_FAN_SPEED

Description: Fan Speed measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
fanSpeed	Fan Speed	double	

EventType: PH_DEV_MON_HW_HUMIDITY

Description: Relative humidity measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
envHumidityRel	Relative Humidity	uint32	
envSensorLoc	Sensor Location	string	
envHumidityRelHighThresh	High Relative Humidity Threshold	uint32	
envHumidityRelLowThresh	Low Relative Humidity Threshold	uint32	

EventType: PH_DEV_MON_HW_POWER

Description: Power measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HW_PS_STAT

Description: Power supply environmental measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envPSTrayId	Power Supply Tray Id	string	
hwPowerSupply1StatusStr	Power Supply 1 State	string	
hwPowerSupply2StatusStr	Power Supply 2 State	string	
hwTempSensorStatusStr	Power Supply Temp Sensor State	string	
envTempHighThreshDegF	High Temperature Threshold Fahrenheit	uint32	
envPSInputStateStr	Power Supply Input State	string	
envPSOutputStateStr	Power Supply Output State	string	
envPSACStateStr	Power Supply AC State	string	
envPSDCStateStr	Power Supply DC State	string	

EventType: PH_DEV_MON_HW_STACK_UNIT

Description: Stack unit status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
envTempDegF	Temperature Fahrenheit	uint32	
cpuUtil	CPU Util	double	
memUtil	Memory Util	double	

EventType: PH_DEV_MON_HW_STATUS

Description: Hardware health status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwBatteryStatus	Hardware Battery Status	uint16	Hardware Battery Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwDiskStatus	Hardware Disk Status	uint16	Hardware Disk Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwMemoryStatus	Hardware Memory Status	uint16	Hardware Memory Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)

Id	Display name	Type	Description
hwPowerSupplyStatus	Hardware Power Supply Status	uint16	Hardware Power Supply Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwTempSensorStatus	Hardware Temperature Sensor Status	uint16	Hardware Temperature Sensor Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwFanStatus	Hardware Fan Status	uint16	Hardware Fan Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwAmpStatus	Hardware Amp Status	uint16	Hardware Amp Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwVoltageStatus	Hardware Voltage Status	uint16	Hardware Voltage Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwFailedPowerSupplyCount	Failed Power Supply Count	uint16	Failed Power Supply Count from SNMP based hardware monitoring
hwFailedFanCount	Failed Fan Count	uint16	Failed Fan Count from SNMP based hardware monitoring
hwLCCStatus	Storage LCC Status	uint16	
hwLinkStatus	Storage Link Status	uint16	
hwPortStatus	Storage Port Status	uint16	
hwHotSpareDiskCount	Hot Spare Disk Count	uint32	
hwMiscCompStatus	Misc Component Status	uint16	
hwRaidStatus	Hardware Raid Status	uint16	Hardware Raid Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwRelHumidStatus	Relative Humidity Status	uint16	
hwDewPtStatus	Dew Point Status	uint16	

Id	Display name	Type	Description
hwAudioStatus	Audio Sensor Status	uint16	
hwAirFlowStatus	Air Flow Status	uint16	
hwGenNumericSensorStatus	Generic Numeric Sensor Status	uint16	
hwDryContactStatus	Dry Contact Status	uint16	
hwDoorSwitchStatus	Door Switch Status	uint16	
hwCameraMotionStatus	Camera Motion Status	uint16	
hwGenStateSensorStatus	Generic State Sensor Status	uint16	
hwPowerEnclosureStatus	Hardware Power Enclosure Status	uint16	Hardware Power Enclosure Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwChassisStatus	Hardware Chassis Status	uint16	Hardware Chassis Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwIOMStatus	Hardware IO Module Status	uint16	Hardware IO Module Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwKVMStatus	Hardware KVM Status	uint16	Hardware KVM Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwRedundantStatus	Hardware Redundancy Status	uint16	Hardware Redundancy Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwBladeStatus	Hardware Blade Status	uint16	Hardware Blade Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwDellCMCStatus	Hardware Dell CMC Status	uint16	Hardware Dell CMC Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwFileSystemStatus	File System Status	uint16	

Id	Display name	Type	Description
hwStackUnitStatus	Hardware Stack Unit Status	uint16	Hardware Stack Unit Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwProbeStatus	Hardware Probe Status	uint16	Hardware Probe Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwInputContactStatus	Hardware Input Contact Status	uint16	Hardware Input Contact Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwOutputRelayStatus	Hardware Output Relay Status	uint16	Hardware Output Relay Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwOutletStatus	Hardware Outlet Status	uint16	Hardware Outlet Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwAlarmDeviceStatus	Hardware Alarm Device Status	uint16	Hardware Alarm Device Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwMemSensorStatus	Hardware Mem Sensor Status	uint16	Hardware Mem Sensor Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwMemOutputStatus	Hardware Mem Output Status	uint16	Hardware Mem Output Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwMemOutletStatus	Hardware Outlet Status	uint16	Hardware Outlet Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwMemBeaconStatus	Hardware Mem Beacon Status	uint16	Hardware Mem Beacon Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwSlotStatus	Hardware Slot Status	uint16	Hardware Slot Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)

EventType: PH_DEV_MON_HW_STATUS_AIRFLOW_CRIT

Description: Airflow critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_AIRFLOW_WARN**Description:** Airflow warning**Severity:** 5 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_ALARMDEVICE_CRIT

Description: Alarm Device hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_ALARMDEVICE_WARN

Description: Alarm Device hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_AMP_CRIT

Description: Amp hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_AMP_WARN

Description: Amp hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_AUDIO_CRIT

Description: Audio sensor critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_AUDIO_WARN

Description: Audio sensor warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_BATTERY_CRIT

Description: Battery hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_BATTERY_WARN

Description: Battery hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_CAMERA_MOTION_CRIT

Description: Camera motion critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_CAMERA_MOTION_WARN

Description: Camera motion warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DEWPT_CRIT

Description: Dew Point temperature critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DEWPT_WARN

Description: Dew Point temperature warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DISK_CRIT

Description: Disk hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DISK_WARN

Description: Disk hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DOOR_SWITCH_CRIT

Description: Door switch critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DOOR_SWITCH_WARN

Description: Door switch warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DRY_CONTACT_CRIT

Description: Dry Contact sensor critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DRY_CONTACT_WARN

Description: Dry Contact Sensor warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_FAN_CRIT

Description: Fan hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_FAN_WARN

Description: Fan hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_FILESYSTEM_CRIT

Description: File system hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_FILESYSTEM_WARN

Description: File system hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_GEN_NUMERIC_SENSOR_CRIT

Description: Generic Numeric Sensor critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_GEN_NUMERIC_SENSOR_WARN

Description: Generic Numeric Sensor warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_GEN_STATE_SENSOR_CRIT

Description: Generic state sensor critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_GEN_STATE_SENSOR_WARN

Description: Generic state sensor warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_HUMIDITY_CRIT

Description: Relative humidity critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_HUMIDITY_WARN**Description:** Relative humidity warning**Severity:** 5 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_INPUTCONTACT_CRIT**Description:** Input Contact hardware health: Critical**Severity:** 10 (High)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_INPUTCONTACT_WARN

Description: Input Contact hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_LCC_CRIT

Description: SAN Link Control Card hardware critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_LCC_WARN

Description: SAN Link Control Card hardware warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_LINK_CRIT

Description: SAN host link critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_LINK_WARN

Description: SAN host link warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMBEACON_CRIT

Description: Memory Beacon hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMBEACON_WARN

Description: Memory Beacon hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMORY_CRIT

Description: Memory hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMORY_WARN

Description: Memory hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMOUTLET_CRIT

Description: Memory Outlet hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMOUTLET_WARN

Description: Memory Outlet hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMOUTPUT_CRIT

Description: Memory Output hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMOUTPUT_WARN

Description: Memory Output hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMSENSOR_CRIT

Description: Memory Sensor hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMSENSOR_WARN

Description: Memory Sensor hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MISC_CRIT

Description: Miscellaneous hardware critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MISC_WARN

Description: Miscellaneous hardware warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_OUTLET_CRIT

Description: Outlet hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_OUTLET_WARN

Description: Outlet hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_OUTPUTRELAY_CRIT

Description: Output relay hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_OUTPUTRELAY_WARN

Description: Output relay hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_PORT_CRIT

Description: SAN storage port hardware critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_PORT_WARN

Description: SAN storage port hardware warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_POWERSUPPLY_CRIT

Description: Power supply hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_POWERSUPPLY_WARN

Description: Power supply hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_POWER_ENCLOSURE_CRIT**Description:** Power enclosure health: Critical**Severity:** 10 (High)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_POWER_ENCLOSURE_WARN**Description:** Power enclosure health: Warning**Severity:** 5 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_PROBE_CRIT

Description: Probe hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_PROBE_WARN

Description: Probe hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_SLOT_CRIT

Description: Hardware Status Critical

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_SLOT_WARN

Description: Hardware Status Warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_STACKUNIT_CRIT**Description:** Stackunit critical**Severity:** 10 (High)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_STACKUNIT_WARN**Description:** Stackunit warning**Severity:** 5 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_TEMP_CRIT

Description: Temperature sensor hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_TEMP_WARN

Description: Temperature sensor hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_VOLTAGE_CRIT

Description: Voltage hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_VOLTAGE_WARN

Description: Voltage hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_TEMP**Description:** Temperature measurement**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
envTempDegC	Temperature Celsius	uint32	
envTempDegF	Temperature Fahrenheit	uint32	
envTempHighThreshDegC	High Temperature Threshold Celsius	uint32	
envTempOffHighDegC	Temp Offset High Celsius	uint32	
envTempHighThreshDegF	High Temperature Threshold Fahrenheit	uint32	
envTempOffHighDegF	Temp Offset High Fahrenheit	uint32	
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
envSensorLoc	Sensor Location	string	

Id	Display name	Type	Description
envTempLowThreshDegF	Low Temperature Threshold Fahrenheit	uint32	
envTempLowThreshDegC	Low Temperature Threshold Celsius	uint32	

EventType: PH_DEV_MON_HW_VOLTAGE

Description: Voltage measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
envVoltage	Voltage	double	

EventType: PH_DEV_MON_HYPERV_CPU_GUEST_VIRTUAL_PROC

Description: HyperV Guest Virtual Processor Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_CPU_LOGICAL_PROC

Description: HyperV Logical Processor Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_CPU_ROOT_VIRTUAL_PROC

Description: HyperV Root Virtual Processor Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_OVERALL

Description: HyperV Root Memory Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_PARTITION

Description: HyperV Memory Partition usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_PARTITION_PER_VM

Description: HyperV per-VM Memory Partition usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION

Description: HyperV Root Partition Total Memory Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION_ROOT

Description: HyperV Root Partition Root Memory Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_VID_PARTITION

Description: HyperV VID Partition Memory Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_VID_PARTITION_PER_VM

Description: HyperV per-VM VID Partition Memory Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_NET_LEGACY_ADAPTER

Description: HyperV Virtual Switch Per Adapter Network Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_NET_VIRTUAL_ADAPTER

Description: HyperV Virtual Switch Per Adapter Network Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_NET_VIRTUAL_SWITCH

Description: HyperV Virtual Switch Network Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_OVERALL_HEALTH

Description: HyperV Machine Health Summary

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_OVERALL_SYSINFO

Description: HyperV System Information

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_STORAGE_LOGICAL_DISK

Description: HyperV Logical Disk Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_IDE_CONTROLLER

Description: HyperV IDE Controller Storage Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_STORAGE

Description: HyperV Virtual Storage Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_INCOMING_EXCEED_GUARANTEED

Description: Incoming eps exceeded Guaranteed eps at a collector

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
collectorId	Collector ID	uint32	This field captures the ID of a FortiSIEM Collector
phCollectorName	Collector Name	string	Name of the FortiSIEM Collector. The name is set in GUI.
incomingEventsPerSec	Incoming Event Rate	double	This is a FortiSIEM event ingestion rate calculated every 3 minutes, divided by 180 to generate a rolling EPS (Events Per Second) interval.
guaranteedEventsPerSec	Guaranteed EPS	uint64	

EventType: PH_DEV_MON_INTF_ADMIN_DOWN_TO_UP

Description: Network Interface administratively came back up

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
intfAlias	Host Interface Alias	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_INTF_ADMIN_UP_TO_DOWN

Description: Network Interface administratively went down

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
intfAlias	Host Interface Alias	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_INTF_OPER_DOWN_TO_UP

Description: Network Interface operationally came back up

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
intfAlias	Host Interface Alias	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_INTF_OPER_UP_TO_DOWN

Description: Network Interface operationally went down

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
intfAlias	Host Interface Alias	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_INTF_USAGE_TOTAL**Description:** Aggregate Interface Usage**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
recvBitsPerSec	Received Bit Rate	double	
sentBitsPerSec	Sent Bit Rate	double	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.

EventType: PH_DEV_MON_IPSLA_HTTP_MET**Description:** IP SLA HTTP Performance metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipSLAProto	IP SLA Protocol	string	Name of the IP Service Level Agreement (SLA) protocol. This parameter is set during IPSLA monitoring
httpResponseTimeMs	HTTP Response Time ms	uint32	
dnsResponseTimeMs	DNS Response Time ms	uint32	
tcpConnectResponseTimeMs	TCP Connect Response Time ms	uint32	
httpTransactResponseTimeMs	HTTP Transaction Response Time ms	uint32	
ipslaHttpStatus	IPSLA HTTP Status	uint32	
ipslaHttpStatusDesc	IPSLA HTTP Status Description	string	
httpStatusCode	HTTP Status	string	

EventType: PH_DEV_MON_IPSLA_ICMP_MET

Description: ICMP performance metrics collected via IP SLA

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
ipslaTestName	IP SLA Test Name	string	
icmpResponseTimeMs	ICMP Response Time ms	uint32	

EventType: PH_DEV_MON_IPSLA_MET

Description: IP SLA performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

Id	Display name	Type	Description
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipSLAProto	IP SLA Protocol	string	Name of the IP Service Level Agreement (SLA) protocol. This parameter is set during IPSLA monitoring
tos	IP Type of Service	uchar	The type of service (ToS) field present in the IPv4 header. Typically present in Netflow.
dscp	DSCP	uchar	
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
avgJitterMs	Avg Jitter	uint32	Average Jitter (msec)
maxJitterMs	Max Jitter	uint32	Maximum Jitter (msec)
minJitterMs	Min Jitter	uint32	Minimum Jitter (msec)
avgJitterSDMs	Avg SD Jitter	uint32	Average Source to Destination Jitter (msec)
maxJitterSDMs	Max SD Jitter	uint32	Maximum Source to Destination Jitter (msec)
minJitterSDMs	Min SD Jitter	uint32	Minimum Source to Destination Jitter (msec)
avgJitterDSMs	Avg DS Jitter	uint32	Average Destination to Source Jitter (msec)
maxJitterDSMs	Max DS Jitter	uint32	Maximum Destination to Source Jitter (msec)
minJitterDSMs	Min DS Jitter	uint32	Minimum Destination to Source Jitter (msec)
pktLost	Packets Lost	uint32	Total Packets lost (includes Source to Destination and reverse)
pktLostSD	SD Packets Lost	uint32	Packets lost from Source to Destination
pktLostDS	DS Packets Lost	uint32	Packets lost from Destination to Source
pktMIA	Packets Missing	uint32	Packets missing
pktLate	Packets Late	uint32	Packets late

Id	Display name	Type	Description
pktOutSeq	Pkt Out-of-Seq	uint32	

EventType: PH_DEV_MON_IPSLA_UDP_MET

Description: IP SLA UDP Performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
udpResponseTimeMs	UDP Response Time ms	uint32	
ipslaUdpStatus	IPSLA UDP Status	uint32	
ipslaUdpStatusDesc	IPSLA UDP Status Description	string	

EventType: PH_DEV_MON_IPSLA_VOIP_MET**Description:** VOIP performance metrics collected via IP SLA**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipSLAProto	IP SLA Protocol	string	Name of the IP Service Level Agreement (SLA) protocol. This parameter is set during IPSLA monitoring
codec	VoIP Codec	string	
tos	IP Type of Service	uchar	The type of service (ToS) field present in the IPv4 header. Typically present in Netflow.
dscp	DSCP	uchar	
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
avgJitterMs	Avg Jitter	uint32	Average Jitter (msec)

Id	Display name	Type	Description
maxJitterMs	Max Jitter	uint32	Maximum Jitter (msec)
minJitterMs	Min Jitter	uint32	Minimum Jitter (msec)
avgJitterSDMs	Avg SD Jitter	uint32	Average Source to Destination Jitter (msec)
maxJitterSDMs	Max SD Jitter	uint32	Maximum Source to Destination Jitter (msec)
minJitterSDMs	Min SD Jitter	uint32	Minimum Source to Destination Jitter (msec)
avgJitterDSMs	Avg DS Jitter	uint32	Average Destination to Source Jitter (msec)
maxJitterDSMs	Max DS Jitter	uint32	Maximum Destination to Source Jitter (msec)
minJitterDSMs	Min DS Jitter	uint32	Minimum Destination to Source Jitter (msec)
pktLost	Packets Lost	uint32	Total Packets lost (includes Source to Destination and reverse)
pktLostSD	SD Packets Lost	uint32	Packets lost from Source to Destination
pktLostDS	DS Packets Lost	uint32	Packets lost from Destination to Source
pktMIA	Packets Missing	uint32	Packets missing
pktLate	Packets Late	uint32	Packets late
pktOutSeq	Pkt Out-of-Seq	uint32	
mosScore	MOS Score	double	MOS (Mean Opinion Score) measures the perceived quality of VoIP audio on a scale from 1 to 5, with 5 being the best possible score. A high MOS rate indicates that the audio quality is good, while a low MOS rate indicates poor audio quality.
icpifScore	ICPIF Score	uint32	ICPIF (Impairment/Calculated Planning Impairment Factor) quantifies the key impairments to voice quality that are encountered in the network. ICPIF values are expressed in a typical range of 5 (very low impairment) to 55 (very high impairment).

EventType: PH_DEV_MON_IRONPORT_MAIL_USAGE

Description: Cisco Ironport Mail Usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
workQueueMsgCount	Mail Work Queue Count	uint32	
diskIOUtil	Disk IO Util	double	
mailQueueUtil	Mail Queue Util	double	
msgAge	Oldest Message Age sec	uint32	
outstandingDNS	Outstanding DNS Req	uint32	
pendingDNS	Pending DNS Req	uint32	
openFile	Open File Count	uint32	
mtaThreadCount	MTA Thread Count	uint32	
queueAvailStatus	Mail Queue Avail Status	string	

EventType: PH_DEV_MON_ISILON_CLUSTER_HEALTH

Description: Isilon Cluster health and performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
svcStatus	Service Health	string	
clusterOnlineMember	Cluster Online Members	string	
clusterOfflineMember	Cluster Offline Members	string	

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
cpuUtil	CPU Util	double	
userCpuUtil	User CPU Util	double	
kernCpuUtil	Kernel CPU Util	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
netSentKBytesPerSec	Net Sent Rate KBps	double	
netRecvdKBytesPerSec	Net Received Rate KBps	double	

EventType: PH_DEV_MON_ISILON_CLUSTER_MEMBERSHIP_CHANGE

Description: Isilon cluster membership change

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
addedItem	Added Item	string	
deletedItem	Deleted Item	string	

EventType: PH_DEV_MON_ISILON_CLUSTER_QUOTA

Description: Isilon quota utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
quotaName	Quota Name	string	
quotaType	Quota Type	string	
quotaSoftThresholdBytes	Quota Soft Threshold Bytes	uint64	
quotaHardThresholdBytes	Quota Hard Threshold Bytes	uint64	
quotaAdvThresholdBytes	Quota Advisory Threshold Bytes	uint64	
quotaUsageBytes	Quota Usage Bytes	uint64	
quotaUsageWithOverheadBytes	Quota Usage With Overhead Bytes	uint64	
quotaInodeUsage	Quota Inode Usage	uint64	
gracePeriod	Quota Grace Period	uint64	

EventType: PH_DEV_MON_ISILON_CLUSTER_SNAPSHOT**Description:** Isilon snapshot usage**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
snapshotName	Snapshot Name	string	

Id	Display name	Type	Description
snapshotDescription	Snapshot Description	string	
snapshotPath	Snapshot Path	string	
snapshotCreateTime	Snapshot Create Time	Date	
snapshotExpiryTime	Snapshot Expiry Time	Date	
fileSize64	File Size64 Bytes	uint64	

EventType: PH_DEV_MON_ISILON_NODE_DISK_PERF

Description: Isilon disk performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
opsPerSec	Operations/sec	uint32	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	

EventType: PH_DEV_MON_ISILON_NODE_HEALTH

Description: Isilon node health and performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
svcStatus	Service Health	string	
cluster	Cluster	string	
cpuUtil	CPU Util	double	
userCpuUtil	User CPU Util	double	
kernCpuUtil	Kernel CPU Util	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
netSentKBytesPerSec	Net Sent Rate KBps	double	
netRecvdKBytesPerSec	Net Received Rate KBps	double	

EventType: PH_DEV_MON_ISILON_NODE_PROTO_PERF

Description: Isilon protocol performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appName	Application Name	string	
opsPerSec	Operations/sec	uint32	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
minSentBytes	Min Sent Bytes	uint64	Minimum of Sent Bytes over the report window. Used in Profile Reports only.
maxSentBytes	Max Sent Bytes	uint64	Maximum of Sent Bytes over the report window. Used in Profile Reports only.

Id	Display name	Type	Description
avgSentBytes	Avg Sent Bytes	double	Average of Sent Bytes over the report window. Used in Profile Reports only.
sdevSentBytes	Std Dev Sent Bytes	double	Standard Deviation of Sent Bytes over the report window. Used in Profile Reports only.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
minRecvBytes	Min Received Bytes	uint64	Minimum of Received Bytes over the report window. Used in Profile Reports only.
maxRecvBytes	Max Received Bytes	uint64	Maximum of Received Bytes over the report window. Used in Profile Reports only.
avgRecvBytes	Avg Received Bytes	double	Average of Received Bytes over the report window. Used in Profile Reports only.
sdevRecvBytes	Std Dev Received Bytes	double	Standard Deviation of Received Bytes over the report window. Used in Profile Reports only.
latency	Latency	double	
minLatency	Min Latency	double	
maxLatency	Max Latency	double	
avgLatency	Avg Latency	double	
sdevLatency	Std Dev Latency	double	
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	

EventType: PH_DEV_MON_JBOSS_APP

Description: JBOSS application server settings and metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_CPU

Description: JBOSS CPU metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_DB_POOL

Description: JBOSS database pool metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_EJB

Description: JBOSS EJB metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_MEMORY

Description: JBOSS memory usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_REQUEST_PROCESSOR

Description: Weblogic request processor metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_SERVLET

Description: JBOSS servlet metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_SESSION

Description: JBOSS session metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_THREAD_POOL

Description: JBOSS thread pool usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_LOG_ALL_DEVICE_DELAY_HIGH

Description: Log receipt delay for all devices from a collection point crossed high water mark

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_LOG_ALL_DEVICE_DELAY_LOW

Description: Log receipt delay for all devices from a collection point fell below low water mark

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_LOG_DEVICE_DELAY_HIGH

Description: Log receipt delay for a single device crossed high water mark

Notes: This event is generated by FortiSIEM Supervisor node when no events are received from a single source IP (Reporting IP) within a (high threshold) time window. The time period can be set in two ways:

- Global Setting: Set the EventRecvTimeGapHigh attribute in Admin > Device Support > Custom Properties. By default it is set to 10 minutes
- Per device Setting: Set the "Event Receive Time Gap High Threshold minutes" attribute in CMDB > Choose a Device > Edit > Device Properties

An event is generated for each jobType, e.g. Syslog, Windows Agent Log Collection, Linux Agent Log Collection, Cloud Service Log Collection etc.

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_LOG_DEVICE_DELAY_LOW

Description: Log receipt delay for a single device fell below water mark

Notes: This event is generated by FortiSIEM Supervisor node when no events are received from a single source IP (Reporting IP) within a (low threshold) time window. The time period can be set in two ways:

- Global Setting: Set the EventRecvTimeGapLow attribute in Admin > Device Support > Custom Properties. By default it is set to 5 minutes
- Per device Setting: Set the "Event Receive Time Gap Low Threshold minutes" attribute in CMDB > Choose a Device > Edit > Device Properties

An event is generated for each jobType, e.g. Syslog, Windows Agent Log Collection, Linux Agent Log Collection, Cloud Service Log Collection etc.

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_MANUAL_SVC_START_TO_STOP

Description: Running Windows Manual service stopped

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
servicePath	Service Path	string	
serviceDesc	Service Description	string	

EventType: PH_DEV_MON_MANUAL_SVC_STOP

Description: Windows Manual Windows Service stopped

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
servicePath	Service Path	string	
serviceDesc	Service Description	string	

EventType: PH_DEV_MON_MANUAL_SVC_STOP_TO_START

Description: Stopped Windows Manual Service started

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
servicePath	Service Path	string	
serviceDesc	Service Description	string	

EventType: PH_DEV_MON_NETAPP_AGGR_MET

Description: NETAPP aggregate performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
aggrName	NetApp Aggregate Name	string	
aggrReadOpsPerSec	Aggregate Read Request /sec	double	
aggrWriteOpsPerSec	Aggregate Write Request /sec	double	
aggrTxfrPerSec	Aggregate Transfer /sec	double	
aggrCpReadPerSec	Aggregate CP Read /sec	double	

EventType: PH_DEV_MON_NETAPP_CIFS_MET

Description: NETAPP CIFS performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cifsOpsPerSec	CIFS Request Rate	double	
cifsLatency	CIFS Latency ms	double	Overall Latency (ms) using CIFS storage protocol.

EventType: PH_DEV_MON_NETAPP_CP_MET

Description: NetApp consistency point metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cpFromTimer	Timer Consistency Point	uint32	
cpFromSnapshot	Snapshot Consistency Point	uint32	
cpFromLowWater	Low Water Consistency Point	uint32	
cpFromHiWater	High Water Consistency Point	uint32	
cpFromLogFull	Log Full Consistency Point	uint32	
backtobackCp	Back-to-back Consistency Point	uint32	
totalCp	Total Consistency Point	uint32	
deferredBacktobackCp	Deferred Back-to-back Consistency Point	uint32	

EventType: PH_DEV_MON_NETAPP_DISK_HEALTH

Description: NetApp disk status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
totDisk	Total Disk Count	uint32	Total number of Disks
activeDisk	Active Disk Count	uint32	Total number of Active Disks
failedDisk	Failed Disk Count	uint32	Total number of Failed Disks
spareDisk	Spare Disk Count	uint32	Total number of Spare Disks
reconstDisk	Reconstructing Disk Count	uint32	Total number of Reconstructing Disks
scrubbDisk	Scrubbing Disk Count	uint32	
addSpareDisk	Add Spare Disk Count	uint32	

EventType: PH_DEV_MON_NETAPP_DISK_MET**Description:** NETAPP disk level performance metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
diskUtil	Disk Capacity Util	double	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
devDiskRdLatency	Disk Read Latency ms	double	
devDiskWrLatency	Disk Write Latency ms	double	
diskTfrOpsPerSec	Disk Transfer Ops/s	double	

EventType: PH_DEV_MON_NETAPP_FCP_MET**Description:** NETAPP FCP performance metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
fcReadOpsPerSec	FCP Read Request /sec	double	Read Request Rate (operations/sec) using FCP storage protocol.
fcWriteOpsPerSec	FCP Write Request /sec	double	Write Request Rate (operations/sec) using FCP storage protocol.

Id	Display name	Type	Description
fcReadLatency	FCP Read Latency ms	double	Read Latency (ms) using FCP storage protocol.
fcWriteLatency	FCP Write Latency ms	double	Write Latency (ms) using FCP storage protocol.
fcReadKBytesPerSec	FCP Read Volume KBps	double	Read throughput (KBytes/sec) using FCP storage protocol.
fcWriteKBytesPerSec	FCP Write Volume KBps	double	Write throughput (KBytes/sec) using FCP storage protocol.

EventType: PH_DEV_MON_NETAPP_ISCSI_MET

Description: NETAPP ISCSI performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
iscsiReadOpsPerSec	ISCSI Read Request Rate	double	Read Request Rate (operations/sec) using ISCSI storage protocol.
iscsiWriteOpsPerSec	ISCSI Write Request Rate	double	Write Request Rate (operations/sec) using ISCSI storage protocol.
iscsiReadLatency	ISCSI Read Latency ms	double	Read Latency (ms) using ISCSI storage protocol.
iscsiWriteLatency	ISCSI Write Latency ms	double	Write Latency (ms) using ISCSI storage protocol.
iscsiReadKBytesPerSec	ISCSI Read Volume KBps	double	Read throughput (KBytes/sec) using ISCSI storage protocol.
iscsiWriteKBytesPerSec	ISCSI Write Volume KBps	double	Write throughput (KBytes/sec) using ISCSI storage protocol.

EventType: PH_DEV_MON_NETAPP_LUN_MET**Description:** NETAPP lun level performance metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
lunName	LUN Name	string	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
devDiskRWLatency	Disk Read/Write Latency	double	
diskQueueFull	Disk Queue Full /sec	double	

EventType: PH_DEV_MON_NETAPP_NFS3_MET**Description:** NETAPP detailed NFS V3 performance metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
nfsReadOpsPerSec	NFS Read Request Rate	double	Read Request Rate (operations/sec) using NFS storage protocol.

Id	Display name	Type	Description
nfsWriteOpsPerSec	NFS Write Request Rate	double	Write Request Rate (operations/sec) using NFS storage protocol.
nfsOpsPerSec	NFS Request Rate	double	
nfsReadLatency	NFS Read Latency	double	Read Latency (ms) using NFS storage protocol.
nfsWriteLatency	NFS Write Latency	double	Write Latency (ms) using NFS storage protocol.
nfsReadKBytesPerSec	NFS Read Volume KBps	double	Read throughput (KBytes/sec) using NFS storage protocol.
nfsWriteKBytesPerSec	NFS Write Volume KBps	double	Write throughput (KBytes/sec) using NFS storage protocol.

EventType: PH_DEV_MON_NETAPP_NFS4_MET

Description: NETAPP detailed NFS V4 performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
nfsReadOpsPerSec	NFS Read Request Rate	double	Read Request Rate (operations/sec) using NFS storage protocol.
nfsWriteOpsPerSec	NFS Write Request Rate	double	Write Request Rate (operations/sec) using NFS storage protocol.
nfsOpsPerSec	NFS Request Rate	double	
nfsReadLatency	NFS Read Latency	double	Read Latency (ms) using NFS storage protocol.
nfsWriteLatency	NFS Write Latency	double	Write Latency (ms) using NFS storage protocol.
nfsReadKBytesPerSec	NFS Read Volume KBps	double	Read throughput (KBytes/sec) using NFS storage protocol.
nfsWriteKBytesPerSec	NFS Write Volume KBps	double	Write throughput (KBytes/sec) using NFS storage protocol.

EventType: PH_DEV_MON_NETAPP_NFS_MET**Description:** NETAPP NFS performance metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cacheAgeMin	Cache Age Min	uint64	
cifsOpsPerSec	CIFS Request Rate	double	
nfsOpsPerSec	NFS Request Rate	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
netSentKBytesPerSec	Net Sent Rate KBps	double	
netRecvdKBytesPerSec	Net Received Rate KBps	double	
rpcBadCallsDelta	RPC Bad Calls	uint64	
nfsBadCallsDelta	NFS Bad Calls	uint64	
cifsBadCallsDelta	CIFS Bad Calls	uint64	

EventType: PH_DEV_MON_NETAPP_VOL_MET**Description:** NETAPP volume performance metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
volName	NetApp Volume Name	string	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
nfsWriteOpsPerSec	NFS Write Request Rate	double	Write Request Rate (operations/sec) using NFS storage protocol.
nfsReadLatency	NFS Read Latency	double	Read Latency (ms) using NFS storage protocol.
nfsWriteLatency	NFS Write Latency	double	Write Latency (ms) using NFS storage protocol.
cifsReadOpsPerSec	CIFS Read Request /sec	double	Read Request Rate (operations/sec) using CIFS storage protocol.
cifsWriteOpsPerSec	CIFS Write Request /sec	double	Write Request Rate (operations/sec) using CIFS storage protocol.
cifsReadLatency	CIFS Read Latency ms	double	Read Latency (ms) using CIFS storage protocol.
cifsWriteLatency	CIFS Write Latency ms	double	Write Latency (ms) using CIFS storage protocol.
sanReadOpsPerSec	SAN Read Request /sec	double	
sanWriteOpsPerSec	SAN Write Request /sec	double	
sanReadLatency	SAN Read Latency ms	double	
sanWriteLatency	SAN Write Latency ms	double	

EventType: PH_DEV_MON_NETBOTZ_HW_EMS_STATUS

Description: NetBotz EMS Hardware Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
emsHwStatus	EMS Hardware Status	uint16	EMS Hardware Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
phyMachConnectionStateCode	Physical Machine Connection State	uint16	
hwLogStatus	Hardware Log Status	uint16	Hardware Log Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)

EventType: PH_DEV_MON_NETBOTZ_HW_MODULE_SENSOR

Description: NetBotz Module Sensor Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
moduleNumber	Module Number	uint32	
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorLoc	Sensor Location	string	
envTempDegC	Temperature Celsius	uint32	

Id	Display name	Type	Description
envHumidityRel	Relative Humidity	uint32	
phyMachConnectionStateCode	Physical Machine Connection State	uint16	
hwAlarmDeviceStatus	Hardware Alarm Device Status	uint16	Hardware Alarm Device Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
envTempDegF	Temperature Fahrenheit	uint32	

EventType: PH_DEV_MON_NETBOTZ_HW_PROBE

Description: NetBotz Probe Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorLabel	Sensor Label	string	
envTempDegC	Temperature Celsius	uint32	
envTempHighThreshDegC	High Temperature Threshold Celsius	uint32	
envHumidityRel	Relative Humidity	uint32	
envHumidityRelHighThresh	High Relative Humidity Threshold	uint32	
envHumidityRelLowThresh	Low Relative Humidity Threshold	uint32	
serialNumber	Serial Number	string	

Id	Display name	Type	Description
phyMachConnectionStateCode	Physical Machine Connection State	uint16	
envTempDegF	Temperature Fahrenheit	uint32	
envTempHighThreshDegF	High Temperature Threshold Fahrenheit	uint32	

EventType: PH_DEV_MON_NETSCALER_APP_FW

Description: NetScaler Application Firewall metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
totalRequests	Total Requests	uint64	
totalResponses	Total Responses	uint64	
totalAborts	Total Aborts	uint64	
totalRedirects	Total Redirects	uint64	
startURLViol	Start URL Violations	uint32	
denyURLViol	Deny URL Violations	uint32	
bufOverflowViol	Buffer Overflow Violations	uint32	
cookieViol	Cookie Violations	uint32	
xssViol	XSS Violations	uint32	
sqlViol	SQL Violations	uint32	
fieldFormatViol	Field Format Violations	uint32	
fieldConsistViol	Field Consistency Violations	uint32	
creditCardViol	Credit Card Violations	uint32	

Id	Display name	Type	Description
safeObjViol	Safe Object Violations	uint32	
totViol	Total Violations	uint32	

EventType: PH_DEV_MON_NETSCALER_SERVICE

Description: NetScaler Service metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
serviceName	Service Name	string	
serverIpAddr	Server IP	IP	
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
appTransportProto	Application Protocol	string	
svcStatus	Service Health	string	
averageTransactionTime	Average Transaction Time ms	uint32	
createdConn	Created Connections	uint64	
activeConns	Active Connection	uint64	
surgeQueue	Surge Queue	uint32	
totalRequests	Total Requests	uint64	
totalResponses	Total Responses	uint64	
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.

Id	Display name	Type	Description
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.

EventType: PH_DEV_MON_NETSCALER_VIRT_SERVER

Description: NetScaler Virtual Server metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
serverName	Server Name	string	
serverIpAddr	Server IP	IP	
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
appTransportProto	Application Protocol	string	
svcStatus	Service Health	string	
clientConns	Client Connections	uint64	
serverConns	Server Connections	uint64	
surgeQueue	Surge Queue	uint32	
totalRequests	Total Requests	uint64	
totalResponses	Total Responses	uint64	
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.

Id	Display name	Type	Description
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
totHits	Total Hits	uint64	
serviceUp	Services Up	uint32	
serviceDown	Services Down	uint32	
serviceUnknown	Services Unknown	uint32	
serviceOOS	Services OutOfService	uint32	
serviceTransitOOS	Services Transit OutOfService	uint32	

EventType: PH_DEV_MON_NET_INTF_UTIL

Description: Network Interface utilization stats for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
intfAlias	Host Interface Alias	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
recvBitsPerSec	Received Bit Rate	double	
inIntfUtil	Recv Interface Util	double	Ratio of Received Bits per second (derived from recvBytes) to the received network interface speed

Id	Display name	Type	Description
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
sentBitsPerSec	Sent Bit Rate	double	
outIntfUtil	Sent Interface Util	double	Ratio of Sent Bits per second (derived from sentBytes) to the sent network interface speed
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
inIntfPktErr	Recv Packet Errors	uint32	Number of received packets that had errors. The networking stack discards these packets.
inIntfPktErrPct	Recv Packet Error Pct	double	Ratio of inIntfPktErr and the total number of received packets in an onterval
outIntfPktErr	Sent Packet Errors	uint32	Number of sent packets that had errors. he networking stack discards these packets.
outIntfPktErrPct	Sent Packet Error Pct	double	Ratio of outIntfPktErr and the total number of received packets in an onterval
outQLen64	Interface Sent Queue Length64	uint64	
intfInSpeed64	Recv Interface Speed bps	uint64	Received bits/sec through an interface
intfOutSpeed64	Sent Interface Speed bps	uint64	Sent bits/sec through an interface
intfAdminStatus	Interface Admin Status	string	
intfOperStatus	Interface Operational Status	string	
daysSinceLastUse	Days Since Last Use	uint32	
totIntfPktErr	Total Packet Errors	uint32	
totBitsPerSec	Total Bit Rate	double	Total (Sent plus Received) bits/sec through an interface
linkDuplexStatus	Link Duplex Status	string	
alignError	Frame Align Error	uint32	
fcsError	Frame FCS Error	uint32	
defTransmit	Frame Deferred Transmission	uint32	

Id	Display name	Type	Description
multiCollision	Frame Multi Collision	uint32	
lateCollision	Frame Late Collision	uint32	
excessCollisionAbort	Frame Excess Collision Abort	uint32	
macTxmitError	Frame MAC Transmit Error	uint32	
carrierSenseError	Frame Carrier Sense Error	uint32	
framesTooLong	Frame Too Long	uint32	
symbolError	Frame Symbol Error	uint32	
intMacRecvError	Frame Internal MAC Receive Error	uint32	
vdom	Virtual Domain	string	
latency	Latency	double	
jitterMs	Jitter	uint32	
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.
availSentBitsPerSec	Available Sent Rate	double	
availRecvBitsPerSec	Available Received Rate	double	
realtimeLinkCost	Real-time Link Cost	uint32	
transactionalLinkCost	Transactional Link Cost	uint32	
backgroundLinkCost	Background Link Cost	uint32	
relayDevIpAddr	Relaying IP	IP	Relaying IP is most commonly used to specify the log relay appliance, usually a collector.
relayDevName	Relaying Device	string	This is the hostname of the relaying device, a log relay, which is most typically a FortiSIEM collector.

EventType: PH_DEV_MON_NIMBLE_GLOBAL_STAT**Description:** Nimble Storage global stats**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
ioReadsPerSec	Total Read I/Os Rate	double	
ioSeqReadsPerSec	Total Sequential Read I/Os Rate	double	
ioWritesPerSec	Total Write I/Os Rate	double	
ioSeqWritesPerSec	Total Sequential Write I/Os Rate	double	
ioReadLatency	IO Read Latency	uint64	
ioWriteLatency	IO Write Latency	uint64	
ioReadKBytesPerSec	Total Read I/O Rate KBps	double	
ioSeqReadKBytesPerSec	Total Sequential Read I/O Rate KBps	double	
ioWriteKBytesPerSec	Total Write I/O Rate KBps	double	
ioSeqWriteKBytesPerSec	Total Sequential Write I/O Rate KBps	double	
usedVolMB	Used Volumes MB	uint64	
usedSnapMB	Used Snapshots MB	uint64	
ioNonSeqCacheHitRatio	Non-Sequential Read I/Os Hit Ratio	double	

EventType: PH_DEV_MON_NUTANIX_CLUSTER_STATUS**Description:** Nutanix Cluster Status**Severity:** 1 (Low)**Event Category:** 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
clusterVersion	Cluster Version	string	
clusterStatus	Cluster Status	string	
diskUtil	Disk Capacity Util	double	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
diskRWReqPerSec	Disk RW Rate req/sec	double	
devDiskRWLatency	Disk Read/Write Latency	double	

EventType: PH_DEV_MON_NUTANIX_CONTAINER_INFO**Description:** Nutanix Storage Container Info**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
ntxContainerId	Nutanix Container Id	uint64	
ntxContainerName	Nutanix Container Name	string	
diskUtil	Disk Capacity Util	double	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	

Id	Display name	Type	Description
diskRWReqPerSec	Disk RW Rate req/sec	double	
devDiskRWLatency	Disk Read/Write Latency	double	

EventType: PH_DEV_MON_NUTANIX_CTRLR_VM_RESOURCE

Description: Nutanix Controller VM Resource Info

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
ntxControllerVMId	Nutanix Controller VM Id	uint64	
memTotalIMB	Total Memory MB	uint32	
procCount	System Process Count	uint32	

EventType: PH_DEV_MON_NUTANIX_DISK_STATUS

Description: Nutanix Disk Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	

Id	Display name	Type	Description
diskId	Disk Id	uint64	
ntxControllerVMId	Nutanix Controller VM Id	uint64	
hwDiskSerial	Disk Serial	string	
diskUtil	Disk Capacity Util	double	
totalDiskMB	Total Disk MB	uint32	
freeDiskMBNonRoot	Free Disk MB NonRoot	uint32	
inodeUsedPct	Inode Util	double	
inodeMax	Max Inodes	uint32	
inodeFreeNonRoot	Free Inodes NonRoot	uint32	

EventType: PH_DEV_MON_NUTANIX_DISK_TEMP

Description: Nutanix Disk temperature event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskId	Disk Id	uint64	
ntxControllerVMId	Nutanix Controller VM Id	uint64	
hwDiskSerial	Disk Serial	string	
envTempdDegC	Temperature Celsius Detailed	double	

EventType: PH_DEV_MON_NUTANIX_SERVICE_STATUS

Description: Nutanix Service Status

Severity: 1 (Low)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
ntxControllerVMId	Nutanix Controller VM Id	uint64	
ntxClusterVMStatus	Cluster VM Status	string	
ntxZeusStatus	Nutanix Zeus Status	string	
ntxStargateStatus	Nutanix Stargate Status	string	

EventType: PH_DEV_MON_NUTANIX_STORAGE_POOL_INFO**Description:** Nutanix Storage Pool Info**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
spoolId	Storage Pool Id	uint64	
spoolName	Storage Pool Name	string	
diskUtil	Disk Capacity Util	double	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
diskRWReqPerSec	Disk RW Rate req/sec	double	
devDiskRWLatency	Disk Read/Write Latency	double	

EventType: PH_DEV_MON_OMI_PING_STAT**Description:** OMI Ping Statistics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.
sysDownTime	System Downtime	uint32	
sysDegradedTime	System Degraded Time	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_OSPF_NBR_STATUS**Description:** OSPF neighbor status**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
ospfAreaId	OSPF Area Id	uint32	
ospfState	OSPF State	string	

EventType: PH_DEV_MON_PANASONIC_AERO_LOG_MON_STATUS

Description: Panasonic Aero Log Monitoring Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
collectorId	Collector ID	uint32	This field captures the ID of a FortiSIEM Collector
phCollectorName	Collector Name	string	Name of the FortiSIEM Collector. The name is set in GUI.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
airlineName	Airline Name	string	
airlineTail	Airline Tail Number	string	
airlineDevName	Airline Device	string	
filePath	File Path	string	
scannedFiles	Scanned File Count	uint32	
totEventCount	Total Event Count	uint32	

EventType: PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_HIGH

Description: Performance monitoring delay for all devices from a collection point crossed high water mark

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_LOW

Description: Performance monitoring delay for all devices from a collection point fell below low water mark

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERFMON_DEVICE_DELAY_HIGH

Description: All performance metrics delay for a single device crossed high water mark

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERFMON_DEVICE_DELAY_LOW

Description: Some performance metric delay for a single device fell below water mark

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERFMON_JOB_DELAY_HIGH

Description: A performance metric delay for a single device crossed high water mark

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERFMON_JOB_DELAY_LOW

Description: A performance metric delay for a single device fell below water mark

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_BACKUP_INFO

Description: Last backup info on SQL Server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_BLOCKBY_INFO

Description: Blocked process in SQL Server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_CONFIG_INFO

Description: SQL Server configuration

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_ERROR_LOG_INFO

Description: SQL Server error log information

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_GEN_INFO

Description: SQL Server general information

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_LOCK_INFO

Description: SQL Server lock information

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_PERDB

Description: Metrics for per database in SQL Server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_SYS

Description: Metrics for the total SQL Server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_TOP_QUERIES

Description: Top queries against SQL Server database

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MYSQLDB

Description: MySQL database performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MYSQLDB_TABLESPACE

Description: MySQL tablespace metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_ORADB

Description: Oracle database performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_ORADB_CLUSTER

Description: Oracle Cluster performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_ORADB_TABLESPACE

Description: Oracle tablespace metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_ORADB_TOP_QUERIES

Description: Top queries against Oracle database

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PING_STAT

Description: Ping Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.
sysDownTime	System Downtime	uint32	
sysDegradedTime	System Degraded Time	uint32	
pollIntv	Polling Interval	uint32	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_DEV_MON_PING_STAT_SUPPRESSED

Description: Ping stat suppressed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.

Id	Display name	Type	Description
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.

EventType: PH_DEV_MON_PORT_CLOSE

Description: A port is closed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
ipPort	IP Port	uint16	IP port number
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_PORT_OPEN

Description: A new port is open

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs

Id	Display name	Type	Description
ipPort	IP Port	uint16	IP port number
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_PRINTER_OUTPUT_STATUS

Description: Printer Output Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
prtDevStatus	Printer Device Status	string	
prtPrintStatus	Printer Printing Status	string	
prtErrorState	Printer Error State	string	
prtPrintPageCount	Printed Page Count	uint32	

EventType: PH_DEV_MON_PRINTER_SUPPLY_STATUS

Description: Printer Supply Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
prtSupplyType	Printer Supply Type	string	
prtSupplyName	Printer Supply Name	string	

Id	Display name	Type	Description
prtMaxSupplyLevel	Printer Max Supply Level	int32	
prtCurrSupplyLevel	Printer Current Supply Level	int32	
prtSupplyUnit	Printer Supply Unit	string	
prtCurrSupplyUsedPct	Printer Pct Used Supply	double	

EventType: PH_DEV_MON_PROC_CPU_UTIL

Description: Process CPU Utilization stats

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PROC_MEM_UTIL

Description: Process Memory Utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PROC_RESOURCE_UTIL

Description: Process CPU and Memory Utilization stats

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
swProcName	Software Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
procOwner	Process Owner	string	

Id	Display name	Type	Description
memUtil	Memory Util	double	
cpuUtil	CPU Util	double	
appName	Application Name	string	
appGroupName	Application Group Name	string	
pollIntv	Polling Interval	uint32	
swParam	Software Param	string	
realMemPeakKBytes	Real Peak Memory KB	uint32	
virtMemKBytes	Virtual Memory KB	uint32	
peakVirtMemKBytes	Peak Virtual Memory KB	uint32	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
sysUpTime	System Uptime	uint32	

EventType: PH_DEV_MON_PROC_START

Description: Process Started

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
swProcName	Software Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
procOwner	Process Owner	string	
appName	Application Name	string	
appGroupName	Application Group Name	string	
pollIntv	Polling Interval	uint32	
swParam	Software Param	string	

EventType: PH_DEV_MON_PROC_STOP

Description: Process Stopped

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
swProcName	Software Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
procOwner	Process Owner	string	
appName	Application Name	string	
appGroupName	Application Group Name	string	
pollIntv	Polling Interval	uint32	
swParam	Software Param	string	

EventType: PH_DEV_MON_QUALYS_WEB_APP_FW

Description: Qualys Web Application Firewall Log

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventTime	Event Occur Time	Date	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
type	Type	string	
ipsConfidence	Attack Confidence	string	
policyName	Policy Name	string	
msg	Message	string	

EventType: PH_DEV_MON_RBD_BW

Description: Riverbed Steelhead appliance bandwidth metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
inLanBytes	Inbound Optimized Bytes LAN Side	uint32	
inWanBytes	Inbound Optimized Bytes WAN Side	uint32	
outLanBytes	Outbound Optimized Bytes LAN Side	uint32	
outWanBytes	Outbound Optimized Bytes WAN Side	uint32	

EventType: PH_DEV_MON_RBD_CONN

Description: Riverbed Steelhead appliance connection metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
optConn	Optimized Connections	uint32	
passthruOptConn	Passthrough Connections	uint32	
halfOpenOptConn	Half-open Optimized Connections	uint32	

Id	Display name	Type	Description
halfClosedOptConn	Half-closed Optimized Connections	uint32	
estOptConn	Established Optimized Connections	uint32	
activeOptConn	Active Optimized Connections	uint32	
totalOptConn	Total Opt Connections	uint32	

EventType: PH_DEV_MON_RBD_PEER_STAT

Description: Riverbed Steelhead appliance Peer metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
rbdState	Riverbed Steelhead State	string	
connFailure	Connection Failures	uint32	
reqTimeout	Request Timeout	uint32	
maxLatency	Max Latency	double	

EventType: PH_DEV_MON_RBD_PER_PORT_BW

Description: Riverbed Steelhead per port bandwidth metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
inLanBytes	Inbound Optimized Bytes LAN Side	uint32	
inWanBytes	Inbound Optimized Bytes WAN Side	uint32	
outLanBytes	Outbound Optimized Bytes LAN Side	uint32	
outWanBytes	Outbound Optimized Bytes WAN Side	uint32	

EventType: PH_DEV_MON_RBD_TOP_APP

Description: Riverbed Steelhead appliance top application metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_DEV_MON_RBD_TOP_DEST

Description: Riverbed Steelhead appliance top dest metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_DEV_MON_RBD_TOP_SRC

Description: Riverbed Steelhead appliance top src metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_DEV_MON_RBD_TOP_TALKER

Description: Riverbed Steelhead appliance top talker metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_DEV_MON_RDS_METRIC

Description: AWS RDS metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
instanceName	DB Instance Name	string	
type	Type	string	
dbCpuTimeRatio	DB CPU Time Ratio	double	
dbUserConn	DB User Connections	uint32	
diskQLen	Disk Queue Length	uint32	
freeMemKB	Free Memory	uint32	
freeDiskMB	Free Disk MB	uint32	
usedSwapMemKB	Used Swap Memory	uint32	
ioReadsPerSec	Total Read I/Os Rate	double	
ioWritesPerSec	Total Write I/Os Rate	double	

Id	Display name	Type	Description
devDiskRdLatency	Disk Read Latency ms	double	
devDiskWrLatency	Disk Write Latency ms	double	

EventType: PH_DEV_MON_RUCKUS_ACCESS_POINT_STAT

Description: Ruckus Access Point Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
description	Description	string	
numRadio	Radio Count	uint32	
numWlanClient	WLAN Station Count	uint32	WLAN Station Count found in SNMP based WLAN monitoring
knownRogueAP	Known Rogue APs	uint32	
connMode	Connection Mode	string	
firstJoinTime	First Join Time	Date	
lastBootTime	Last Boot Time	Date	
lastUpgradeTime	Last Upgrade Time	Date	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	

EventType: PH_DEV_MON_RUCKUS_CONTROLLER_STAT**Description:** Ruckus Controller Statistics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
numAp	AP Count	uint32	
numWlanClient	WLAN Station Count	uint32	WLAN Station Count found in SNMP based WLAN monitoring
newRogueAP	New Rogue APs	uint32	
knownRogueAP	Known Rogue APs	uint32	
wlanSentBytes	WLAN Sent Bytes	uint64	WLAN Sent Bytes found in SNMP based WLAN monitoring
wlanRecvBytes	WLAN Recv Bytes	uint64	WLAN Recv Bytes found in SNMP based WLAN monitoring
wlanSentBitsPerSec	WLAN Sent Rate bps	double	WLAN Sent Rate (in bits/sec) found in SNMP based WLAN monitoring
wlanRecvBitsPerSec	WLAN Recv Rate bps	double	WLAN Recv Rate (in bits/sec)s found in SNMP based WLAN monitoring
lanSentBytes	LAN Sent Bytes	uint64	
lanRecvBytes	LAN Recv Bytes	uint64	
lanSentBitsPerSec	LAN Sent Rate bps	double	

EventType: PH_DEV_MON_RUCKUS_SSID_PERF**Description:** Ruckus SSID Performance Metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
wlanSsid	WLAN SSID	string	WLAN Service Set Identifier (SSID) found in SNMP based WLAN monitoring
description	Description	string	
wlanName	WLAN Name	string	WLAN Name found in SNMP based WLAN monitoring
authenMethod	Authentication Method	string	
encryptAlgo	Encryption Algorithm	string	
isGuest	Guest VLAN	string	
srcVLAN	Source VLAN	uint16	The VLAN to which the Source Network Interface belongs. Source network interface through which a packet enters a network device.
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	
authSuccess	Auth Successes	uint32	
authFailure	Auth Failures	uint32	
assocSuccess	Assoc Success	uint32	
assocFailure	Assoc Failure	uint32	
assocDeny	Assoc Deny	uint32	
disassocAbnormal	Disassoc Abnormal	uint32	
disassocLeave	Disassoc Leave	uint32	
disassocMisc	Disassoc Misc	uint32	

EventType: PH_DEV_MON_SERVERIRON_REAL_SERVER_STAT

Description: Brocade ServerIron ADX Real Server Stat

Severity: 1 (Low)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
realServerIP	Real Server IP	IP	
realServerState	Real Server State	string	
failedPortExists	Failed Port Exists	uint16	
openConnectionsCount	Open Connections	uint64	
peakConns	Peak Connections	uint64	
activeSessions	Active Sessions	uint64	

EventType: PH_DEV_MON_SLB_METRIC**Description:** Cisco Server Load Balancing metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
lbOpenConn	LB Open Conn	uint32	
lbFailedConn	LB Failed Conn	uint32	
lbL4Conn	LB L4 Conn	uint32	
lbL7Conn	LB L7 Conn	uint32	
lbDroppedL4Conn	LB Dropped L4 Conn	uint32	
lbDroppedL7Conn	LB Dropped L7 Conn	uint32	
lbHttpRedirectConn	LB HTTP Redirect Conn	uint32	

Id	Display name	Type	Description
lbDroppedHttpRedirectConn	LB Dropped HTTP Redirect Conn	uint32	
lbAclDeniedConn	LB ACL Denied Conn	uint32	
lbTimedoutConn	LB Timed Out Conn	uint32	

EventType: PH_DEV_MON_SNMP_PING_STAT

Description: SNMP Ping Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.
sysDownTime	System Downtime	uint32	
sysDegradedTime	System Degraded Time	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_SRC_AD_REPL_STAT

Description: Windows Active Directory Source REPLSTAT command output

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_STATUS

Description: Status of devices monitored by FortiSIEM

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_STORAGE_PORT_DOWN_TO_UP

Description: Storage port came back up

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
spName	SAN Storage Processor Name	string	
spPortName	SAN Storage Port Name	string	
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.

EventType: PH_DEV_MON_STORAGE_PORT_UP_TO_DOWN

Description: Storage port went down

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
spName	SAN Storage Processor Name	string	
spPortName	SAN Storage Port Name	string	
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.

EventType: PH_DEV_MON_SYS_CPU_UTIL

Description: System CPU Utilization for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
cpuName	CPU Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cpuUtil	CPU Util	double	
pollIntv	Polling Interval	uint32	
sysCpuUtil	System CPU Util	double	
userCpuUtil	User CPU Util	double	
waitCpuUtil	Wait CPU Util	double	
kernCpuUtil	Kernel CPU Util	double	
contextSwitchPerSec	Context Switch Rate /sec	double	

Id	Display name	Type	Description
cpuInterruptPerSec	CPU Interrupt Rate /sec	double	
cpuCore	CPU Cores	uint16	
loadAvg1min	Load Average 1 min	double	Linux Server load average (calculated over 1min ntervals). Linux load average is a metric that shows the number of tasks currently executed by the CPU and tasks waiting in the queue.
loadAvg5min	Load Average 5 min	double	Linux Server load average (calculated over 5min ntervals). Linux load average is a metric that shows the number of tasks currently executed by the CPU and tasks waiting in the queue.
loadAvg15min	Load Average 15 min	double	Linux Server load average (calculated over 15min ntervals). Linux load average is a metric that shows the number of tasks currently executed by the CPU and tasks waiting in the queue.
relayDevIpAddr	Relaying IP	IP	Relaying IP is most commonly used to specify the log relay appliance, usually a collector.
relayDevName	Relaying Device	string	This is the hostname of the relaying device, a log relay, which is most typically a FortiSIEM collector.

EventType: PH_DEV_MON_SYS_DISK_FREE

Description: Free disk space stats for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_SYS_DISK_TREND_DAY

Description: Daily Disk growth trend

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
diskGrowthMBDaily	Current Daily Disk Growth	double	
avgDiskGrowthMBDaily	Avg Daily Disk Growth	double	
timeToDiskFull	Days To Disk Full	int32	

EventType: PH_DEV_MON_SYS_DISK_TREND_MONTH

Description: Monthly disk growth trend

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
diskGrowthMBMonthly	Current Monthly Disk Growth	double	
avgDiskGrowthMBMonthly	Avg Monthly Disk Growth	double	
timeToDiskFull	Days To Disk Full	int32	

EventType: PH_DEV_MON_SYS_DISK_TREND_WEEK**Description:** Weekly disk growth trend**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
diskGrowthMBWeekly	Current Weekly Disk Growth	double	
avgDiskGrowthMBWeekly	Avg Weekly Disk Growth	double	
timeToDiskFull	Days To Disk Full	int32	

EventType: PH_DEV_MON_SYS_DISK_UTIL**Description:** Disk Utilization stats for a device**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
diskName	Disk Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskUtil	Disk Capacity Util	double	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
pollIntv	Polling Interval	uint32	
inodeUsedPct	Inode Util	double	
inodeUsed	Used Inodes	uint32	
inodeFree	Free Inodes	uint32	
inodeMax	Max Inodes	uint32	
fileUsedPct	File Util	double	
fileUsed	Used Files	uint32	
fileFree	Free Files	uint32	
fileMax	Max Files	uint32	
maxDiskUtil	Max Disk Util	double	
maxInodeUsedPct	Max Inode Util	double	
maxFileUsedPct	Max File Util	double	
appTransportProto	Application Protocol	string	
resvDiskMB	Reserved Disk MB	uint32	
availDiskMB	Available Disk MB	uint32	

EventType: PH_DEV_MON_SYS_EXT_CMD

Description: Extensible commands status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appName	Application Name	string	
command	Command	string	
exitValue	Command exit value	int32	
usrMsg	User defined msg	string	
extCmdErrStatus	Extensible Command Error Status	string	
errFixCmd	Error Fix Command	string	

EventType: PH_DEV_MON_SYS_MEM_FREE

Description: Free system memory stats for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
memName	Memory Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
freeMemKB	Free Memory	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_SYS_MEM_UTIL

Description: System memory Utilization stats for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
memName	Memory Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
memUtil	Memory Util	double	
pollIntv	Polling Interval	uint32	
freeMemKB	Free Memory	uint32	
bufMemKB	Buffer Memory	uint32	
cacheMemKB	Cache Memory	uint32	
swapMemUtil	Swap Memory Util	double	
freeSwapMemKB	Free Swap Memory	uint32	
swapInRate	Swap Read Rate Pages/sec	double	
swapOutRate	Swap Write Rate Pages/sec	double	
swapRate	Total Swap Rate Pages/sec	double	
totalMemKB	Total Memory	uint32	
usedMemKB	Used Memory	uint32	
relayDevIpAddr	Relaying IP	IP	Relaying IP is most commonly used to specify the log relay appliance, usually a collector.
relayDevName	Relaying Device	string	This is the hostname of the relaying device, a log relay, which is most typically a FortiSIEM collector.

EventType: PH_DEV_MON_SYS_PAGEFILE_USAGE

Description: Pagefile usage for Windows systems

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pageFileUsage	PageFile Usage	double	
pageFilePeakUsage	PageFile Peak Usage	double	

EventType: PH_DEV_MON_SYS_PER_CPU_UTIL

Description: System per CPU Utilization for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
cpuName	CPU Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cpuUtil	CPU Util	double	
pollIntv	Polling Interval	uint32	
sysCpuUtil	System CPU Util	double	
userCpuUtil	User CPU Util	double	

EventType: PH_DEV_MON_SYS_PROC_COUNT

Description: System process count for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
procCount	System Process Count	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_SYS_RESTART

Description: A device restarted

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
restartTime	Restart Time	Date	

EventType: PH_DEV_MON_SYS_STAT

Description: HP-UNIX logged in users and average system jobs statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
numUser	System Logged In User	uint32	
numJob	Average System Job	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_SYS_STATUS

Description: Overall System ststus

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
overallStatusCode	Overall Health	uint16	
systemStatus	System Health	string	
svcStatus	Service Health	string	
envTempDegC	Temperature Celsius	uint32	

EventType: PH_DEV_MON_SYS_SWAP_MEM_ERROR_MSG

Description: Swap memory error

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
memName	Memory Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
swapMemUtil	Swap Memory Util	double	
freeSwapMemKB	Free Swap Memory	uint32	
memMinimumSwap	Minimum Swap Memory	uint32	
swapMemErrorString	Swap Memory Error	string	

EventType: PH_DEV_MON_SYS_UPTIME**Description:** System uptime for a device**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
sysUpTime	System Uptime	uint32	
sysUpTimePct	System Uptime Pct	double	
sysDownTime	System Downtime	uint32	
pollIntv	Polling Interval	uint32	
relayDevIpAddr	Relaying IP	IP	Relaying IP is most commonly used to specify the log relay appliance, usually a collector.
relayDevName	Relaying Device	string	This is the hostname of the relaying device, a log relay, which is most typically a FortiSIEM collector.

EventType: PH_DEV_MON_SYS_VIRT_MEM_UTIL**Description:** System virtual memory Utilization stats for a device**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
memName	Memory Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
virtMemUsedKB	Virtual Memory	uint32	
virtMemUtil	Virtual Memory Util	double	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_TARGET_FILE_CONTENT_CHANGE

Description: Target file hash changed from gold standard

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
fileName	File Name	string	
hashCode	Hash Code	string	
oldSVNVersion	Old SVN Version	uint32	
newSVNVersion	New SVN Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_TOMCAT_CPU

Description: Tomcat cpu usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TOMCAT_DB

Description: Tomcat database pool metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TOMCAT_MEMORY

Description: Tomcat memory usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TOMCAT_REQUEST_PROCESSOR

Description: Tomcat request processor metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TOMCAT_SERVLET

Description: Tomcat servlet metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TOMCAT_SESSION

Description: Tomcat session metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TOMCAT_THREAD_POOL

Description: Tomcat thread pool usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TRACEROUTE_STAT**Description:** Trace Route statistics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
eventTime	Event Occur Time	Date	
jobId	Job Id	string	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
hopNum	Hop Count	uint32	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.

EventType: PH_DEV_MON_UCS_HW_CHASSIS_STAT**Description:** Cisco UCS Chassis status**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
inputPowerWatt	Input Power Watt	double	
inputPowerAvgWatt	Avg Input Power Watt	double	
inputPowerMaxWatt	Max Input Power Watt	double	
inputPowerMinWatt	Min Input Power Watt	double	
outputPowerWatt	Output Power Watt	double	
outputPowerAvgWatt	Avg Output Power Watt	double	
outputPowerMaxWatt	Max Output Power Watt	double	
outputPowerMinWatt	Min Output Power Watt	double	

EventType: PH_DEV_MON_UCS_HW_FAN_STAT

Description: Cisco UCS fan status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
fanSpeed	Fan Speed	double	
fanSpeedAvg	Avg Fan Speed	double	
fanSpeedMax	Max Fan Speed	double	
fanSpeedMin	Min Fan Speed	double	

EventType: PH_DEV_MON_UCS_HW_MEMORY_STAT

Description: Cisco UCS memory status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
envTempdDegC	Temperature Celsius Detailed	double	
envTempAvgDegC	Avg Temperature Celsius	double	
envTempMaxDegC	Max Temperature Celsius	double	

Id	Display name	Type	Description
envTempMinDegC	Min Temperature Celsius	double	

EventType: PH_DEV_MON_UCS_HW_PROCESSOR_STAT

Description: Cisco UCS processor status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
inputCurrentAmp	Input Amp	double	
inputCurrentAvgAmp	Avg Input Amp	double	
inputCurrentMaxAmp	Max Input Amp	double	
inputCurrentMinAmp	Min Input Amp	double	
envTempdDegC	Temperature Celsius Detailed	double	
envTempAvgDegC	Avg Temperature Celsius	double	
envTempMaxDegC	Max Temperature Celsius	double	
envTempMinDegC	Min Temperature Celsius	double	

EventType: PH_DEV_MON_UCS_HW_PSU_STAT**Description:** Cisco UCS power supply status**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
envTempdDegC	Temperature Celsius Detailed	double	
envTempAvgDegC	Avg Temperature Celsius	double	
envTempMaxDegC	Max Temperature Celsius	double	
envTempMinDegC	Min Temperature Celsius	double	
input210Volt	Input 210 Volt	double	
input210AvgVolt	Avg Input 210 Volt	double	
input210MaxVolt	Max Input 210 Volt	double	
input210MinVolt	Min Input 210 Power Volt	double	
output12Volt	Output 12 Volt	double	
output12AvgVolt	Avg Output Volt	double	
output12MaxVolt	Max Output Volt	double	
output12MinVolt	Min Output Volt	double	

Id	Display name	Type	Description
output3V3Volt	Output 3V3 Volt	double	
output3V3AvgVolt	Avg Output 3V3 Volt	double	
output3V3MaxVolt	Max Output 3V3 Volt	double	
output3V3MinVolt	Min Output 3V3 Volt	double	
outputCurrentAmp	Output Amp	double	
outputCurrentAvgAmp	Avg Output Amp	double	
outputCurrentMaxAmp	Max Output Amp	double	
outputCurrentMinAmp	Min Output Amp	double	
outputPowerWatt	Output Power Watt	double	
outputPowerAvgWatt	Avg Output Power Watt	double	
outputPowerMaxWatt	Max Output Power Watt	double	
outputPowerMinWatt	Min Output Power Watt	double	

EventType: PH_DEV_MON_UPS_METRIC

Description: UPS metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
upsRemainBatteryChargePct	UPS Remaining Charge Pct	uint32	
upsBatteryStatus	UPS Battery Status	uint32	
upsReplaceBatteryIndicator	UPS Replace Battery Indicator	uint32	
upsTimeOnBattery	UPS Time on Battery sec	uint32	
upsBasicOutputStatus	UPS Output Status	uint32	
upsAdvOutputLoad	UPS Output Load	uint32	
upsAdvOutputVoltage	UPS Output Voltage V	uint32	
upsAdvOutputFreq	UPS Output Frequency Hz	uint32	
upsEstSecRemain	UPS Time Remaining sec	uint32	
upsBatteryVoltage	UPS Battery Voltage	double	
upsBatteryCurrent	UPS Battery Current Amp	double	
upsBatteryTempC	UPS Battery Temperature Celsius	uint32	
upsBatteryTempF	UPS Battery Temperature Fahrenheit	uint32	
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
upsAdvInputFreq	UPS Input FrequencyHz	uint32	
upsAdvInputVoltage	UPS Input Voltage	uint32	

Id	Display name	Type	Description
upsOutputCurrent	UPS Output Current	double	
upsOutputPower	UPS Output Power	double	

EventType: PH_DEV_MON_VMCLUSTER_CPU_UTIL

Description: Physical CPU usage for a VMware Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VMCLUSTER_DATASTORE_IO

Description: Datastore IO stats for a VMware Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VMCLUSTER_MEM_UTIL

Description: Physical memory usage for a VMware Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VMCLUSTER_STATUS

Description: VMware cluster status

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VMRESPOOL_CPU_UTIL

Description: Physical CPU usage for a VMware Resource Pool

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VMRESPOOL_MEM_UTIL

Description: Physical memory usage for a VMware Resource Pool

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_CPU_UTIL

Description: Physical CPU usage for a Virtual Machine

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_DATASTORE_IO

Description: Datastore IO stats for a Virtual Machine

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_DISK_IO

Description: Disk IO stats for a Virtual Machine

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_DISK_UTIL

Description: VM datastore utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_MEM_UTIL

Description: Physical memory usage for a Virtual Machine

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_NET_INTF_UTIL

Description: Network IO stats for a Virtual Machine

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_PER_CPU_UTIL

Description: Physical CPU utilization for a Virtual Machine's virtual CPU

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_SNAPSHOT

Description: Virtual Machine Snapshot

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_STATE

Description: Virtual Machine State

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_TOOLS_STATUS

Description: VMware tools status

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_UPTIME

Description: Virtual Machine's up time

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VPN_CONN

Description: VPN Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
vpnConnCount	VPN Conn Count	uint32	

EventType: PH_DEV_MON_VPN_STATUS

Description: VPN Performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
vpnStatus	VPN Status	string	
vpnConnCount	VPN Conn Count	uint32	
sslVpnStatus	SSL VPN Status	string	

Id	Display name	Type	Description
sslVpnConnCount	SSL VPN Conn Count	uint32	
vpnTunnelName	VPN Tunnel Name	string	
vpnConnType	VPN Conn Type	string	
remoteVpnIpAddr	Remote VPN Tunnel IP	IP	
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_WATCHGUARD_POLICY_STAT

Description: Watchguard Firebox Policy Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
policyName	Policy Name	string	
recvDecryptFail	Recv Decrypt Fail	uint64	
authFailure	Auth Failures	uint32	
failureCount	Failure Count	uint32	
activeSessions	Active Sessions	uint64	
totalNum	Total Number of Items	uint32	
totBytesPerSec	Total Byte Rate	double	
totPktsPerSec	Total Packet Rate	double	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_WEBLOGIC_APP

Description: Weblogic app server configuration and metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_DB_POOL

Description: Weblogic database pool metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_EJB

Description: Weblogic EJB metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_GEN

Description: Weblogic generic settings

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_MEMORY

Description: Weblogic memory usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_SERVLET

Description: Weblogic servlet metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_SESSION

Description: Weblogic session metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_THREAD_POOL

Description: Weblogic thread pool usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_APP

Description: Websphere app server configuration and metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_AUTHENTICATION

Description: Websphere app server authentication metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_CPU

Description: Websphere CPU usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_DB_POOL

Description: Websphere database pool metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_EJB

Description: Websphere EJB metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_MEMORY

Description: Websphere memory usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_SERVLET

Description: Websphere servlet metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_THREAD_POOL

Description: Websphere thread pool usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_TRANSACTION

Description: Websphere app server transaction metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WMI_PING_STAT

Description: WMI Ping Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.
sysDownTime	System Downtime	uint32	
sysDegradedTime	System Degraded Time	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_JOB_STAT

Description: Performance Monitor job status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobId	Job Id	string	

Id	Display name	Type	Description
jobType	Job Type	uint16	
jobDetail	Job Detail	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
jobName	Job Name	string	
jobDesc	Job Description	string	
jobStatus	Job Status	uint16	
pollIntv	Polling Interval	uint32	
eventTime	Event Occur Time	Date	

EventType: PH_JOB_STATUS_XML_SEND_ERROR

Description: Error in sending Performance Monitor job status to app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JOB_STATUS_XML_SENT

Description: Performance Monitor job status sent to app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_JOB_STAT_SUPPRESSED

Description: Performance monitor job status sending suppressed because of no change

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobId	Job Id	string	

Id	Display name	Type	Description
jobType	Job Type	uint16	
jobDetail	Job Detail	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
jobName	Job Name	string	
jobDesc	Job Description	string	
jobStatus	Job Status	uint16	
pollIntv	Polling Interval	uint32	
eventTime	Event Occur Time	Date	

EventType: PH_MONITOR_ARCHIVE_GET_WORKER_FAILURE

Description: phMonitor Failed to get worker list for archive change

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_ARCHIVE_UPDATE_WORKER_FAILURE

Description: phMonitor Failed to update worker archive

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_BEACONING_REGISTER_FAILURE

Description: Beaconing Registration Failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_CHECK_DEPENDENCY_FAILED**Description:** Failed to check dependency**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_CMD_FAILURE**Description:** phMonitor failed to run command**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
command	Command	string	
errorNoInt	Error Number Int	int32	

EventType: PH_MONITOR_CMD_SEND_FAILURE**Description:** FortiSIEM Monitor module failed to send command to other FortiSIEM modules**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
command	Command	string	
targetProcName	Target Process Name	string	

EventType: PH_MONITOR_COLLECTOR_REGISTER_FAILURE

Description: phMonitor failed to register collector

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_COLLECTOR_UPDATE_STATUS_FAILURE

Description: FortiSIEM Monitor module failed to update Collector status

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

EventType: PH_MONITOR_CONFIG_DOWNLOAD_FAILURE

Description: phMonitor failed to download config from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_DBCLUSTER_SEND_COMMAND_FAILED

Description: Send Reset Command to Super failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_DELETE_DR_FAILED

Description: Failed to delete DR

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_DELETE_SECONDARY_ON_WORKER_FAILED

Description: Failed to remove DR configuration on secondary worker

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_DELETE_SUPER_FOLLOWER_FAILED

Description: Failed to remove configuration of follower super

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_DISPATCH_CMD_MISMATCH

Description: phMonitor failed to dispatch wrong command to other processes

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_MONITOR_DOMAIN_CHANGE_XML_PARSE_FAILURE

Description: phMonitor failed to parse AppDefn object from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_ENT_OR_SP_MODE_MISSING

Description: phMonitor failed to identify Service Provider or Enterprise installation

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_EXCESSIVE_DB_LOGIN_FAILURE

Description: phMonitor failed to login to PostgreSQL

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_MONITOR_FAILED_CONN_QUERYMASTER

Description: Unable to send status query to QueryMaster

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_FILE_IO_ERROR

Description: phMonitor encountered empty or unreadable file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_MONITOR_FILE_PERMISSION_ERROR

Description: File Permssion error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_FILE_PERMISSION_WARNING

Description: File permission warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
details	Details	string	

EventType: PH_MONITOR_FLIP_PRIMARY_FAILURE

Description: phMonitor failed to flip primary server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_FSM_AGENT_UPDATE_PWD_ERROR

Description: phMonitor failed to update FortiSIEM Agent upload password

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_GET_REPLICATION_PROGRESS_FAILED

Description: Failed to get replication progress

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_GET_UPTIME_ERROR

Description: FortiSIEM Monitor module failed to get system uptime

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_HANDLE_TASK

Description: Monitor handles task

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_HARDWARE_SN_FORK_FAILURE

Description: phMonitor failed to fork to determine hardware Serial Number

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_HOST_UUID_READ_FAILURE

Description: phMonitor on Collector failed to read CSI

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_HTTP_PULL_ERROR

Description: phMonitor failed to pull information via HTTP from App Server

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_INIT_PROC_MODULE_NOT_FOUND

Description: phMonitor failed to initialize - Module not found

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	

EventType: PH_MONITOR_INIT_SECONDARY_ON_WORKER_FAILED

Description: Failed to update configuration on secondary worker

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_INIT_SUPER_FOLLOWER_FAILED

Description: Failed to update configuration of follower super

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_INIT_SYSTEM_XML_PARSE_FAILURE

Description: phMonitor failed to initialize - Wrong System Services XML in Config file

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_MONITOR_JDBC_POOL_NOT_EXIST

Description: JDBC Connection Pool exist

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_LIB_DEPENDENCY_WARNING

Description: Library dependency warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
details	Details	string	

EventType: PH_MONITOR_LOAD_CONF_FROM_APP_SERVER_FAILED

Description: Failed to load configure from app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_LOCAL_HOSTNAME_GET_FAILURE

Description: phMonitor cannot get local machine host name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_MEM_FILE_OPEN_FAILURE

Description: phMonitor failed on mem file open

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
userId	User Id	string	

EventType: PH_MONITOR_MISSING_MONITOR

Description: No running phMonitor process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_MMAP_FAILURE

Description: phMonitor encountered MMAP failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_MOTNIROR_REGISTER_FAILURE

Description: phMonitor failed to register other monitors

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_NOTIFICATION_CLIENT_CONTACT_FAILURE

Description: phMonitor Notification Client failed to contact another process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_MONITOR_NOTIFICATION_CMD_EMPTY

Description: phMonitor Notification client encountered invalid argument

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_NOTIFICATION_CMD_MISMATCH

Description: phMonitor Notification client encountered unknown command type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
notifEvtId	Notification Event Id	uint32	

EventType: PH_MONITOR_NOTIFICATION_RETURN_FAILURE

Description: phMonitor Notification client encountered returns failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
xmlBody	XML Body	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_MONITOR_PHOENIX_CONFIG_GLOBAL_MISSING

Description: phMonitor found GLOBAL phoenix_config section missing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_PHOENIX_CONFIG_INVALID

Description: phMonitor found Invalid phoenix config file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_PROCESS_OWNER_NOT_ADMIN_ERROR

Description: FortiSIEM Monitor module detected that a file owner is not admin

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
userId	User Id	string	
groupId	Group ID	string	

EventType: PH_MONITOR_RECVD_CONFIG_CHANGE

Description: Monitor received config change notification

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_RECVD_HEARTBEAT

Description: Monitor received heartbeat from module

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
usrMsg	User defined msg	string	

EventType: PH_MONITOR_REDIS_UPDATE_FAILED

Description: Failed to update redis cluster

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_REGISTER_MONITOR_GET_WORKER_FAILURE

Description: phMonitor failed to get workers

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REGISTER_NODE

Description: Register node

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REGISTER_SUPER_FOLLOWER

Description: Register follower super

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REGISTER_WORKER

Description: Register worker

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REMOVE_NODE

Description: Remove node

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REMOVE_SUPER_FOLLOWER

Description: Remove follower super

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REMOVE_WORKER

Description: Remove worker

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REPORTSERVER_NOTIFICATION_CLIENT_CONTACT_FAILURE

Description: phMonitor Notification client failed to contact report server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_MONITOR_REPORTSERVER_NOTIFICATION_CLIENT_INIT_FAILURE

Description: phMonitor Notification client failed to contact report server

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_MONITOR_REPORTSERVER_NOTIFICATION_SERVER_RETURN_FAILURE

Description: phMonitor Notification client encountered report server return failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_MONITOR_RESET_DB_SERVER_NAME_FAILED

Description: Failed to set phoenixPool.ServerName

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_RESET_JDBC_CONN_FAILED

Description: Failed to flush database connection pool

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_RESET_STORAGE_CONFIG_FAILED

Description: Failed to reset storage configuration

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
type	Type	string	

EventType: PH_MONITOR_RESTART_MODULES

Description: Monitor restarting all modules

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REST_CACHE_REQUEST_EMPTY

Description: phMonitor found empty REST Cache Request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REST_CACHE_REQUEST_FAILURE

Description: phMonitor failed to get response to Cache REST API request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
requestBody	Request Body	string	

EventType: PH_MONITOR_REST_CACHE_REQUEST_FORMAT_ILLEGAL

Description: phMonitor encountered Invalid REST Request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
requestBody	Request Body	string	

EventType: PH_MONITOR_REST_CACHE_SERVER_INIT_FAILURE

Description: phMonitor failed to initialize HTTP cache server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REST_CALL_FAILURE

Description: phMonitor REST API call failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
uriStem	URI Stem	string	

EventType: PH_MONITOR_ROLE_UNDEFINED

Description: phMonitor found undefined Monitor Role in phoenix_config.txt

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_SAVE_DR_CONFIG_FAILED

Description: Failed to write DR config in local file. The secondary DB Leader can't update DR config

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_SEND_CMD_TO_MODULE

Description: Monitor sending command to module

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_MONITOR_SEND_VG_UPDATE_CMD_TO_MODULE

Description: Monitor sending value group update command to module

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_MONITOR_SETUID_FAILURE

Description: phMonito failed to raise privilege via setuid()

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_START_MODULE

Description: Monitor starting a module

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	

EventType: PH_MONITOR_START_MODULES

Description: Monitor starting all modules

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STATFS_FAILURE

Description: phMonitor statfs() return failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_MONITOR_STATUS_PUSHER_SPAWN_FAILURE

Description: phMonitor encountered error in spawning statusPusher thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STOP_MODULES

Description: Monitor stopping all modules

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STOP_READER

Description: Deactivating shared store reader

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	

EventType: PH_MONITOR_STORAGE_ES_CUSTOMIZED_TEMPLATE_DEPLOYED

Description: Monitor deployed customized ES templated

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STORAGE_GET_WORKER_FAILURE

Description: phMonitor Failed to get worker list for storage change

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STORAGE_LOCAL_GET_FAILURE

Description: FortiSIEM Monitor module failed to get local disk configuration for event database storage

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STORAGE_NFS_GET_FAILURE

Description: phMonitor failed to get nfs

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_MONITOR_STORAGE_TYPE_GET_FAILURE

Description: phMonitor failed to get storage type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STORAGE_TYPE_UNKNOWN

Description: phMonitor encountered unknown storage type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
type	Type	string	

EventType: PH_MONITOR_STORAGE_UPDATE_WORKER_FAILURE

Description: phMonitor Failed to update worker storage

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_SVC_PASSWORD_DISTRIBUTION_ERROR

Description: phMonitor failed to contact one or more processes with changed svc passwd - so restarting all processes

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_SYSINFO_FAILURE

Description: phMonitor could not get system uptime via sysinfo - assuming uptime of 1 day

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_MONITOR_SYSTEM_DB_LOGIN_ERROR

Description: DB login failure

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_SYSTEM_HEALTH_CPU

Description: PH system health issue: high CPU usage

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	

EventType: PH_MONITOR_SYSTEM_HEALTH_ISSUE

Description: PH system health issue: high CPU and/or memory usage

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
reptProcName	Reported Process Name	string	

EventType: PH_MONITOR_SYSTEM_HEALTH_MEM

Description: PH system health issue: memory usage

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	

EventType: PH_MONITOR_SYSTEM_STATUS_SPAWN_FAILURE

Description: phMonitor encountered error in spawning systemStatus thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_THREAD_SPAWN_FAILED

Description: Failed to spawn thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_TUNNEL_ERROR

Description: phMonitor encountered Tunnel XML error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_UMOUNT_NFS_FAILURE

Description: phMonitor failed to umount nfs

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_UNABLE_CONTACT_APPSVR

Description: phMonitor unable to contact App Server - see response code

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
httpStatusCode	HTTP Status	string	

EventType: PH_MONITOR_UPDATE_DATA_FAILED

Description: Failed to update GeoDB Files

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_UPDATE_DR_FAILED

Description: Failed to update DR

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_UPDATE_WORKER_INFO_FAILED

Description: Failed to update worker info with app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_UPLOAD_LOG_SPAWN_FAILURE

Description: phMonitor encountered error in spawning logUploader thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_WINAGENT_DELETE_PWD_SPAWN_FAILURE

Description: phMonitor encountered error in spawning removeHttpdPassword thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_WINAGENT_UPDATE_PWD_ERROR

Description: phMonitor encountered failed to update windows agent upload password

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_WIN_LINUX_AGENT_PWD_UPDATE_SUCCESS

Description: Windows/Linux Agent password is update successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.

EventType: PH_MONITOR_WORKER_NODECONFIG_UPDATE_FAILED

Description: Failed to update nodejs config file with auth info on worker

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_WORKER_REDIS_ADDSLAVE_UPDATE_FAILED

Description: Failed to update redis config file with addslave info on worker

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_WORKER_REDIS_CONF_UPDATE_FAILED

Description: Failed to update redis config file with auth info on worker

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_COMMIT_FILE_FAILED

Description: Perf Monitoring module failed to commit file into svn - may due to race condition - will retry

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_CONFIG_SEND_FAILED

Description: Perf Monitoring module found unexpected http return code when sending config version to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_PERFMON_CONFIG_VERSION_ERROR

Description: Perf Monitoring module encountered wrong config version

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_CONFIG_VERSION_WARNING

Description: FortiSIEM Performance monitoring module detected Monitoring Config version out of sync with App server

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PERFMON_CUST_JOB_ADD_FAILED

Description: Perf Monitoring module failed to add custom monitoring job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_INIT_ERROR

Description: Perf Monitoring module failed to initialize

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PERFMON_INST_SW_MAP_EMPTY

Description: Perf Monitoring module found that downloaded Installed software map from App Server is empty

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_INST_SW_NO_NAME

Description: Perf Monitoring module found that downloaded Installed software from App Server has no name

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_JOB_ADD_FAILED

Description: Perf Monitoring module failed to add monitoring job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_MASS_PING_WARNING

Description: Perf Monitoring MassPing module found invalid IP

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_MONITEE_BAD

Description: Perf Monitoring module encountered bad monitee map entry

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_MONITEE_NOT_FOUND

Description: Perf Monitoring module failed to find a monitee

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_NO_DEV_TYPE

Description: Perf Monitoring module encountered internal error - devTypeToJobItemMap find failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_PERF_OBJ_PARSE_FAILURE

Description: Perf Monitoring module did not find performance object definition in XML received from App Server

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_PING_RESULT_OPEN_FAILED

Description: Perf Monitoring module failed to open Ping result file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_PROC_RUN_FAILED

Description: Perf Monitoring module failed to run process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_REAL_TIME_JOB_RUN_FAILED

Description: Perf Monitoring module failed to run real time job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PERFMON_ROUTE_LOAD_ERROR

Description: Perf Monitoring module failed to load network dependency from app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PERFMON_STATUS_REPORTER_INIT_FAILED

Description: Perf Monitoring module failed to initialize job status reporter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_STATUS_REPORT_FAILED

Description: Perf Monitoring module failed to report task status to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_SVN_CHECKOUT_FAILED

Description: Perf / Config Monitoring module failed to check out SVN directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_PERFMON_SVN_CONFIG_MISSING

Description: Perf / Config Monitoring module failed to find running or startup config

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_SVN_DIR_CREATE_FAILED

Description: Perf / Config Monitoring module failed to create svn root dir

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_PERFMON_SVN_DIR_UPDATE_FAILED

Description: Perf / Config Monitoring module failed to update dir

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_PERFMON_SVN_FILE_COPY_FAILED

Description: Perf / Config Monitoring module failed to copy file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	

EventType: PH_PERFMON_SVN_FILE_EMPTY

Description: Perf / Config Monitoring module config file is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_FILE_MARK_FAILED

Description: Perf / Config Monitoring module failed to mark file for add to svn

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_FILE_OPEN_FAILED

Description: Perf / Config Monitoring module cannot open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_PERFMON_SVN_FILE_PARSE_FAILED

Description: Perf / Config Monitoring module failed to parse file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_FILE_REMOVE_FAILED

Description: Perf / Config Monitoring module failed to remove file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_PERFMON_SVN_FILE_RENAME_FAILED

Description: Perf / Config Monitoring module cannot rename file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	

EventType: PH_PERFMON_SVN_FIM_FILE_MISSING

Description: Perf / Config Monitoring module failed to find FIM file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_SVN_FIRSTFILELINES_EMPTY

Description: Perf / Config Monitoring module found that FIRSTFILENAME is empty in file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_FIRSTFILELINES_NOT_IN_FILE

Description: Perf / Config Monitoring module found that FIRSTFILELINES is not in file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_GET_DEVICE_ID_FAILED

Description: Perf / Config Monitoring module failed to get device ID via hostname and IP from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_PERFMON_SVN_GET_DISCOV_TIME_FAILED

Description: Perf / Config Monitoring module failed to get discover time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PERFMON_SVN_INFO_GET_FAILED

Description: Perf / Config Monitoring module failed to get svn info on file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_INST_SW_BAD

Description: Perf / Config Monitoring module found that Installed Software xml is incorrectly formatted

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_SVN_INVALID_FILE_FORMAT

Description: Perf / Config Monitoring module found file format error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_INVALID_HEADER_IN_FILE

Description: Perf / Config Monitoring module found that file has incomplete header

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_INVALID_SECONDFILENAME

Description: Perf / Config Monitoring module found that SECONDFILENAME is invalid

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_LINE_MISMATCH

Description: Perf / Config Monitoring module found that line number not matched with the expected value

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_SVN_SECONDFILENAME_EMPTY

Description: Perf / Configuration Monitoring module found that SECONDFILENAME is empty in file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_SOFTWARE_MISSING

Description: Perf / Configuration Monitoring module found missing installed software

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_TOPO_CONFIG_ERROR

Description: Perf Monitoring module failed to parse topo xml from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PERFMON_TOPO_FILE_OPEN_FAILED

Description: Perf Monitoring module failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_PERFMON_TOPO_LOAD_ERROR

Description: Perf Monitoring module failed to load topology from app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_TRACERT_FILE_OPEN_FAILED

Description: Perf Monitoring module cannot open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_UNKNOWN_CUST_PERF_JOB_ID

Description: Perf Monitoring module encountered unknown custom performance monitoring job id from App Server

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_UNKNOWN_PERF_JOB_ID

Description: Perf Monitoring module encountered unknown performance monitoring job id from App Server

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_UNKNOWN_PROBE_JOB_ID

Description: Perf Monitoring module encountered unknown probe job id from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_UPDATE_CONFIG_ERROR

Description: Perf Monitoring module failed to update monitoring config from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PERFMON_UPDATE_FILTERS_ERROR

Description: Perf Monitoring module failed to update interface filter Perf Monitoring module

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PERFMON_UPDATE_ROUTE_DEPENDENCY_FAILED

Description: Perf Monitoring module failed to upload network dependency to app server - Unexpected http response code

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_PERFMON_USER_PWD_GET_FAILED

Description: Perf Monitoring module failed to get user and password

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PERFORM_MONITOR_ERROR

Description: FortiSIEM Performance Monitor generic error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_PER_MON_CONFIG_ERROR

Description: Config discover error occurred

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PER_MON_FETCH

Description: Performance Monitoring module doing SNMP fetch for an OID

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
comm	Community String	string	
oid	Object Identifier	string	

EventType: PH_PER_MON_FUNCTION

Description: Entering Performance Monitoring Debug Function

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_PER_MON_SNMP_DONE

Description: Performance Monitoring module successfully did SNMP fetch

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
comm	Community String	string	
oid	Object Identifier	string	

EventType: PH_PER_MON_WALK

Description: Performance Monitoring module starting SNMP walk for an OID

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
comm	Community String	string	
oid	Object Identifier	string	

EventType: PH_PER_MON_WALK_ERROR

Description: FortiSIEM Performance Monitor SNMP Walk error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
comm	Community String	string	
oid	Object Identifier	string	

EventType: PH_STM_ACCOUNT_UNMATCHED

Description: Perf / STM module encountered unmatched LOOP_EMAIL_42 account in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_AUTH_TYPE_UNKNOWN

Description: Perf / STM module encountered unknown auth type in monitor in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_BAD_ELEM

Description: Perf / STM module encountered bad element in monitor in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_BAD_ELEM_VALUE

Description: Perf / STM module encountered bad element values in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_BAD_PORT

Description: Perf / STM module encountered bad port in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_BAD_RTT_LINE

Description: Perf / STM module encountered bad RTT line in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_BAD_SSL

Description: Perf / STM module encountered bad SSL in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_BAD_TAG

Description: Perf / STM module encountered bad Tag in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_CMD_EXEC_FAILED

Description: Perf / STM module failed to execute command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
exitValue	Command exit value	int32	

EventType: PH_STM_CRED_INVALID

Description: Perf / STM module found that credential doesn't match with Custom Perf Object

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_CURL_ESCAPE_FAILED

Description: Perf / STM module found that curl_easy_escape() returned NULL

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_CURL_INIT_FAILED

Description: Perf / STM module failed to init curl - HTTP based communication will fail

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_STM_DNS_TYPE_UNSupport

Description: Perf / STM module found unsupported dns resource record type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_DUPLICATED

Description: Perf / STM module found duplicated svcMonitor name or id

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_ELEM_EMPTY

Description: Perf / STM module found empty XML element received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_ELEM_MISSING

Description: Perf / STM module found missing XML element received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_ELEM_NEGATIVE

Description: Perf / STM module found negative XML element received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_ERROR

Description: Perf / STM module encountered STM monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
ipPort	IP Port	uint16	IP port number
user	User	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_STM_FILE_OPEN_FAILED

Description: Perf / STM module failed to open file during STM operation

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_STM_GET_HOST_FAILED

Description: Perf / STM module failed to get outgoing host

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_STM_GUESS_TYPE_FAILED

Description: Perf / STM module could not guess resource record type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_HTTP_RESP_FAILED

Description: Perf / STM module did not find response time from command output

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_STM_METHOD_UNKNOWN

Description: Perf / STM module found unknown url method in monitor

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_MONITOR_MISSING_ACTION

Description: Perf / STM module found that No action is specified for monitor

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_MONITOR_RESULT_UPLOAD_FAILED

Description: Perf / STM module failed to upload test service monitor result xml to APP server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_NO_ORACLE_NAME

Description: Perf / STM module found missing instance name and service name for Oracle server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_STM_PORT_UNKNOWN

Description: Perf / STM module found unknown service monitor port

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_PROCESS_INVOKE_FAILED

Description: Perf / STM module failed to invoke SrvMonJobExec::execute

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_PROTO_UNKNOWN

Description: Perf / STM module encountered unknown proto in STM job definition

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_PROTO_UNSupport

Description: Perf / STM module encountered unsupported mail protocol in STM job definition

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_SERVER_ADDR_INVALID

Description: Perf / STM module encountered invalid server address in STM job definition

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_SPECIAL_LINE_NOT_FOUND

Description: Perf / STM module could not find either RTT line or packet loss line in ping response from device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_STM_GET_PROCESS_FAILED

Description: Perf / STM module cannot get process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_STM_GET_PROCESS_NAME_FAILED

Description: Perf / STM module cannot get process name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_TAG_MISSING

Description: Perf / STM module found missing tag XML element received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_TAG_NOT_FOUND

Description: Perf / STM module found missing tag XML element received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_TAG_UNKNOWN

Description: Perf / STM module found unknown tag XML element received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_TRACEROUTE_FAILED

Description: Perf / STM module failed to parse traceroute output

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_XML_PARSE_FAILED

Description: Perf / STM module failed to parse xml file received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_USER_MON_SUDDEN_LOC_CHANGE

Description: User location anomaly detected

Notes: FortiSIEM Identity and Location Module keeps track of (Source IP, Longitude, Latitude, User, Last Seen Time). For every new Identity and Location event (See docs on Dashboard identity location), the Haversine distance (https://en.wikipedia.org/wiki/Haversine_formula) between the new and existing Longitude and Latitudes is calculated. Then the speed required to attain this distance is calculated by dividing the Haversine distance by the elapsed time between current event and event stored in Identity and Location module. If this value exceeds 575 miles/hour, which is a reasonable limit on commercial Jetliners), then the event is generated.

This event can indicate the specific user credential is likely shared or stolen, which can be a security violation.

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
eventSource	Event Source	string	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
startTime	Start Time	Date	This is the start time of a given item or task, and is stored in epoch milliseconds
endTime	End Time	Date	This is the end time of a given item or task, stored in epoch milliseconds.
durationMSec	Duration	uint32	Duration of a connection (in msec)

EventType: PH_USER_MON_SUDDEN_LOGIN_DISTRIBUTION_CHANGE

Description: Change in user login distribution pattern

Severity: 5 (Medium)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
computer	Computer	string	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
oldDistrib	Old Distribution	string	Old Distribution is the profiled login distribution that is computed based on statistics from previous days. It is the probability mass function for the logins at various hours of the day and represented in a comma separated set of values, one for each hour. For each hour of the day (0 representing 12AM-1AM, 1 representing 1AM-2AM etc), the value represents the probability of login during that hour.
newDistrib	New Distribution	string	New Distribution is the login distribution for the current day. It is the probability mass function for the logins at various hours of the day and represented in a comma separated set of values, one for each hour. For each hour of the day (0 representing 12AM-1AM, 1 representing 1AM-2AM etc), the value represents the probability of login during that hour.

EventType: PH_USER_MON_SUDDEN_LOGIN_VOLUME_CHANGE

Description: Increase in User Login Volume**Severity:** 5 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	

Id	Display name	Type	Description
computer	Computer	string	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
oldValue	Old Value	uint64	
newValue	New Value	uint64	

Query Logs

This section provides logs related to querying events

- PH_JAVA_QUERYSERVER_ACTION_UNSUPPORTED_ERROR
- PH_JAVA_QUERYSERVER_ELASTIC_ERROR
- PH_JAVA_QUERYSERVER_ERROR
- PH_JAVA_QUERYSERVER_INFO
- PH_JAVA_QUERYSERVER_QUERYID_ERROR
- PH_JAVA_QUERYSERVER_QUERY_SYNTAX_ERROR
- PH_JAVA_QUERYSERVER_REDIS_ERROR
- PH_JAVA_QUERYSERVER_WARN
- PH_QUERYSRV_DUPLICATED_QUERYID
- PH_QUERYSRV_INVALID_QUERYXML
- PH_QUERY_AGGR_RESULTS_POST_PROCESS_FAILED
- PH_QUERY_ATTR_UNDEFINED
- PH_QUERY_BAD_RESULT_STATUS
- PH_QUERY_CACHE_GET_FAILED
- PH_QUERY_CACHE_RESULT_GET_FAILED
- PH_QUERY_CACHE_TRIGGER_EVENT_GET_FAILED
- PH_QUERY_CHAR_UNEXPECTED
- PH_QUERY_CH_PARSE_FAILED
- PH_QUERY_CH_POST_FAILED
- PH_QUERY_CLICKHOUSE_DATA_FAILED
- PH_QUERY_CLICKHOUSE_EXEC_FAILED
- PH_QUERY_CLICKHOUSE_STARTS
- PH_QUERY_CLICKHOUSE_STOP_FAILED
- PH_QUERY_CLICKHOUSE_WAITING_QUEUE_FULL
- PH_QUERY_COMMAND_BAD
- PH_QUERY_COMPLETION_NOTIFICATION_SEND_FAILED
- PH_QUERY_CONFIG_UNDEFINED
- PH_QUERY_CONVERT_FAILED
- PH_QUERY_DATA_ENUM_FAILED
- PH_QUERY_DATA_MANAGER_NODES_GET_FAILED
- PH_QUERY_DATA_SEND_FAILED
- PH_QUERY_DATA_SIZE_MISMATCH
- PH_QUERY_DATA_SIZE_UNEXPECTED
- PH_QUERY_DATA_TYPE_UNEXPECTED
- PH_QUERY_DB_SERVER_HOST_UNDEFINED
- PH_QUERY_DIR_CREATE_FAILED
- PH_QUERY_DIR_RENAME_FAILED

- PH_QUERY_DISTRIBUTION
- PH_QUERY_DURATION
- PH_QUERY_ES_PARSE_FAILED
- PH_QUERY_ES_POST_FAILED
- PH_QUERY_ES_SCROLL_FAILED
- PH_QUERY_EVENT_COLLECTOR_UNAVAILABLE
- PH_QUERY_EVENT_ID_GET_FAILED
- PH_QUERY_EVENT_PARSE_FAILED
- PH_QUERY_EVENT_PAYLOAD_READ_FAILED
- PH_QUERY_EXCEPTION_CAUGHT
- PH_QUERY_EXPORT_TASK_CREAT_FAILED
- PH_QUERY_EXPORT_TASK_INSERT_FAILED
- PH_QUERY_EXPR_INCOMPLETE
- PH_QUERY_FILE_CONTENT_BAD
- PH_QUERY_FILE_CONTENT_MISSING
- PH_QUERY_FILE_COPY_FAILED
- PH_QUERY_FILE_CORRUPT
- PH_QUERY_FILE_CREATE_FAILED
- PH_QUERY_FILE_EMPTY
- PH_QUERY_FILE_HEADER_GET_FAILED
- PH_QUERY_FILE_LINK_FAILED
- PH_QUERY_FILE_MAGIC_BAD
- PH_QUERY_FILE_MMAP_FAILED
- PH_QUERY_FILE_NAME_BAD
- PH_QUERY_FILE_OPEN_FAILED
- PH_QUERY_FILE_READ_FAILED
- PH_QUERY_FILE_REMOVE_FAILED
- PH_QUERY_FILE_SEEK_FAILED
- PH_QUERY_FILE_STAT_FAILED
- PH_QUERY_FORMAT_UNSUPPORTED
- PH_QUERY_FUNC_ERROR
- PH_QUERY_ID_DUPLICATE
- PH_QUERY_ID_INACTIVE
- PH_QUERY_ID_NOT_FOUND
- PH_QUERY_ID_REMOVE_FAILED
- PH_QUERY_ID_UNSUPPORTED
- PH_QUERY_INLINEREQUEST_BAD
- PH_QUERY_IPC_EVENT_SEND_FAILED
- PH_QUERY_IP_GET_FAILED
- PH_QUERY_IP_INVALID
- PH_QUERY_IP_TYPE_INVALID
- PH_QUERY_LOGINTEGRITYEXPORT_TASK_CREAT_FAILED
- PH_QUERY_LOGINTEGRITYEXPORT_TASK_INSERT_FAILED

- PH_QUERY_LOG_INTEGRITY_EXPORT_DIR_UNCONFIGURED
- PH_QUERY_LOG_INTEGRITY_EXPORT_FAILED
- PH_QUERY_LONG_RUNNING_STOPPED
- PH_QUERY_MEM_ALLOC_FAILED
- PH_QUERY_MESSAGE_SEND_FAILED
- PH_QUERY_MODULE_INIT_FAILED
- PH_QUERY_MODULE_UNCONFIGURED
- PH_QUERY_ONLINE_WORKER_CHANGED
- PH_QUERY_PARSED_EVENT_LOAD_FAILED
- PH_QUERY_PARTIAL_WORKER_FAILURE
- PH_QUERY_PCAP_FINALIZE_FAILED
- PH_QUERY_PCAP_LOAD_FAILED
- PH_QUERY_PCAP_RENAME_FAILED
- PH_QUERY_PCAP_TRANSFER_FAILED
- PH_QUERY_PGDB_EXEC_SQL_FAILED
- PH_QUERY_PGDB_RECONNECT_FAILED
- PH_QUERY_PGDB_SQL_GET_VAL_FAILED
- PH_QUERY_POST_FILTER_PARSE_FAILED
- PH_QUERY_PQ_ERROR
- PH_QUERY_PROCESS_GET_FAILED
- PH_QUERY_PROFILE_ATTR_UNSPECIFIED
- PH_QUERY_PROFILE_EVENT_TYPE_ERROR
- PH_QUERY_PROFILE_FUNCTION_ERROR
- PH_QUERY_PROFILE_NOT_MARKED_AS_BASELINE
- PH_QUERY_PROGRESS_REJECTED
- PH_QUERY_REPORTEXPORT_TASK_CREAT_FAILED
- PH_QUERY_REPORTEXPORT_TASK_INSERT_FAILED
- PH_QUERY_REPORT_RESULTS_LOAD_FAILED
- PH_QUERY_REPORT_RESULTS_POST_FILTER_FAILED
- PH_QUERY_REPORT_RESULT_FILE_NOT_EXIST
- PH_QUERY_REQUEST_BAD
- PH_QUERY_RESULT_FILES_MERGE_FAILED
- PH_QUERY_RESULT_GET_FAILED
- PH_QUERY_RESULT_NOT_READY
- PH_QUERY_RESULT_PARSE_FAILED
- PH_QUERY_RESULT_REJECTED
- PH_QUERY_RESULT_SAVE_FAILED
- PH_QUERY_RESULT_UPLOAD_FAILED
- PH_QUERY_RT_ERROR
- PH_QUERY_SORT_SPEC_GET_FAILED
- PH_QUERY_START_FAILED
- PH_QUERY_STATE_BAD
- PH_QUERY_STATUS_LOAD_FAILED

- PH_QUERY_STATUS_SAVE_FAILED
- PH_QUERY_SUMM_ATTR_BAD
- PH_QUERY_SUMM_ATTR_MISSING
- PH_QUERY_SUMM_ATTR_UPDATE_FAILED
- PH_QUERY_SUMM_COLUMN_UNSUPPORTED
- PH_QUERY_SUMM_EVENT_SKIPPED
- PH_QUERY_SUMM_PARSE_FAILED
- PH_QUERY_SUMM_PERF_ETINFO_UNSUPPORTED
- PH_QUERY_TASK_INVALID
- PH_QUERY_TASK_REROUTED
- PH_QUERY_TASK_REROUTE_FAILED
- PH_QUERY_VALUE_TYPE_UNSUPPORTED
- PH_QUERY_WORKERS_GET_FAILED
- PH_QUERY_WORKERS_SPLIT_AMONG_FAILED
- PH_QUERY_WORKER_CHANGED_TO_OFFLINE
- PH_QUERY_WORKER_CHANGED_TO_ONLINE
- PH_QUERY_XML_PARSE_FAILED

EventType: PH_JAVA_QUERYSERVER_ACTION_UNSUPPORTED_ERROR

Description: Java Query Server unsupported action

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_ELASTIC_ERROR

Description: Java Query Server Elasticsearch error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_ERROR

Description: Java Query Server error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_INFO

Description: Java Query Server Query informational log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_QUERYID_ERROR

Description: Java Query Server unknown or expired Query ID error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_QUERY_SYNTAX_ERROR

Description: Java Query Server Query syntax error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_REDIS_ERROR

Description: Java Query Server Redis error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_WARN

Description: Java Query Server Query warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_QUERYSRV_DUPLICATED_QUERYID

Description: Duplicated query id

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERYSRV_INVALID_QUERYXML

Description: Invalid query xml

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_AGGR_RESULTS_POST_PROCESS_FAILED

Description: Query Master failed to post-process aggregate query results - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_ATTR_UNDEFINED

Description: Query Master/Worker found undefined attribute in Query XML - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_BAD_RESULT_STATUS

Description: Bad Query Result Status

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_CACHE_GET_FAILED

Description: FortiSIEM Query Master failed to get cache results

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_CACHE_RESULT_GET_FAILED

Description: Query Master failed to get query results from its own cache - query will be resubmitted

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_CACHE_TRIGGER_EVENT_GET_FAILED

Description: Query Master failed to get trigger event query from Data Manager - Query Master will attempt to get trigger events from event database

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_CHAR_UNEXPECTED

Description: Query Master/Worker found unexpected character in expression in a Query XML - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_QUERY_CH_PARSE_FAILED

Description: Query Master failed to parse CLICKHOUSE query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_CH_POST_FAILED

Description: Query Master failed to post query to CLICKHOUSE

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
statusCode	HTTP Status	string	

EventType: PH_QUERY_CLICKHOUSE_DATA_FAILED

Description: FortiSIEM ClickHouse DATA failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_CLICKHOUSE_EXEC_FAILED

Description: Failed to exec query from ClickHouse

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_CLICKHOUSE_STARTS

Description: ClickHouse query starts

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_CLICKHOUSE_STOP_FAILED

Description: Failed to stop ClickHouse query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_CLICKHOUSE_WAITING_QUEUE_FULL

Description: ClickHouse query waiting queue is full

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_COMMAND_BAD

Description: Internal error - unsupported query control command - expected Stop, pause and resume

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_COMPLETION_NOTIFICATION_SEND_FAILED

Description: Query Master failed to send query completion notification to App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_CONFIG_UNDEFINED

Description: Query Master/Worker found undefined phoenix_config item

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configName	Config Name	string	

EventType: PH_QUERY_CONVERT_FAILED

Description: Query Master/Worker failed to convert a particular query to certain format - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_DATA_ENUM_FAILED

Description: Query Master failed to enumerate inline report results for a particular report - inline report will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_DATA_MANAGER_NODES_GET_FAILED

Description: Query Master failed to get Data Manager IP addresses - queries will be done by Query Master until the next attempt to get this list of IP addresses

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_DATA_SEND_FAILED

Description: Query Master failed to send query-related data to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_DATA_SIZE_MISMATCH

Description: Query Master found size mismatch between two data entries while loading a particular inline query - this inline report will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_DATA_SIZE_UNEXPECTED

Description: Query Master found unexpected data size while returning results to App server - inline report will not have results

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_DATA_TYPE_UNEXPECTED

Description: Query Master found unexpected data types while returning results to App server - inline report will not have results

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_DB_SERVER_HOST_UNDEFINED

Description: Database server host not defined for query master

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configName	Config Name	string	

EventType: PH_QUERY_DIR_CREATE_FAILED

Description: Query Master/Worker/Data Manager failed to create directory

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_DIR_RENAME_FAILED

Description: Query Master/Worker/Data Manager failed to rename directory

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_DISTRIBUTION

Description: Query distribution (Worker IP: Workload)

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
oldDistrib	Old Distribution	string	Old Distribution is the profiled login distribution that is computed based on statistics from previous days. It is the probability mass function for the logins at various hours of the day and represented in a comma separated set of values, one for each hour. For each hour of the day (0 representing 12AM-1AM, 1 representing 1AM-2AM etc), the value represents the probability of login during that hour.
newDistrib	New Distribution	string	New Distribution is the login distribution for the current day. It is the probability mass function for the logins at various hours of the day and represented in a comma separated set of values, one for each hour. For each hour of the day (0 representing 12AM-1AM, 1 representing 1AM-2AM etc), the value represents the probability of login during that hour.

EventType: PH_QUERY_DURATION**Description:** Query statistics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
reportName	Report Name	string	FortiSIEM report name.

EventType: PH_QUERY_ES_PARSE_FAILED**Description:** Query Master failed to parse Elastic Search Summary query result - query will fail**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)

EventType: PH_QUERY_ES_POST_FAILED

Description: Query Master failed to provide Elastic Search Summary query results to App Server - query results will not be available

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
httpStatusCode	HTTP Status	string	

EventType: PH_QUERY_ES_SCROLL_FAILED

Description: ES Query scroll failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_EVENT_COLLECTOR_UNAVAILABLE

Description: Query Master/Worker failed to get event collector for a particular query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_EVENT_ID_GET_FAILED

Description: Query Master failed to get triggered event ID for a particular triggered event query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventId	Event ID	uint64	This is a globally unique ID assigned to every raw event ingested into the SIEM. This is used by the system for tying events to incidents, and is typically not needed by end users.
queryId	Query Id	string	

EventType: PH_QUERY_EVENT_PARSE_FAILED

Description: Query Master failed to parse events from Data Manager - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.
queryId	Query Id	string	

EventType: PH_QUERY_EVENT_PAYLOAD_READ_FAILED

Description: Query Master failed to read events - some real time events may be missed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_EXCEPTION_CAUGHT

Description: Query Worker encountered corrupt event index or data - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_EXPORT_TASK_CREAT_FAILED

Description: FortiSIEM Query Engine failed to export query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_QUERY_EXPORT_TASK_INSERT_FAILED

Description: FortiSIEM Query Engine failed to start query result export task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_QUERY_EXPR_INCOMPLETE

Description: Query Master failed to handle Query XML during internal processing- Incomplete expression

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_QUERY_FILE_CONTENT_BAD

Description: Query Master / Worker found invalid content in Query XML file - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_FILE_CONTENT_MISSING

Description: Query Master / Worker found certain content missing in Query XML file - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_FILE_COPY_FAILED

Description: Query Master failed to copy query XML file from completed/active to eventdb directory - XXX

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_CORRUPT

Description: Query Master found corrupt query status file for a particular query - query will not be completed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_FILE_CREATE_FAILED

Description: Query Master / Worker failed to create query result file - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_EMPTY

Description: Query Master/Worker found empty query status backup file - system loses redundancy for this query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_FILE_HEADER_GET_FAILED

Description: Query Master failed to read query related file header from query result file - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_FILE_LINK_FAILED

Description: Query Master / Worker failed to hard link query result file - query cache will not be used

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_MAGIC_BAD

Description: Query Master found bad query-related file magic inside query status or result file - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_FILE_MMAP_FAILED

Description: Query Master failed to memory-map summary event cache file - summary event query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_NAME_BAD

Description: Query Master found invalidly formatted summary event cache file - summary event query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_FILE_OPEN_FAILED

Description: Query Master / Worker/ Data Manager failed to open query related file - related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_READ_FAILED

Description: Query Master / Worker/ Data Manager failed to read query related file - related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_REMOVE_FAILED

Description: Query Master failed to remove cached query result file - disk may eventually get full

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_SEEK_FAILED

Description: Query Master failed to seek trend file to offset for a specific inline report - that inline report will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.

EventType: PH_QUERY_FILE_STAT_FAILED

Description: Query Master / Worker/ Data Manager failed to stat query related file - related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FORMAT_UNSUPPORTED

Description: Query Master received unsupported report export file format from App Server - export will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_FUNC_ERROR

Description: Query Master / Worker encountered internal function error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_ID_DUPLICATE

Description: Query Master / Worker encountered duplicate query ID assigned by App server - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_ID_INACTIVE

Description: Query Master / Worker failed to retrieve supposedly active query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_ID_NOT_FOUND

Description: Query Master / Worker failed to find Query ID not found in task queue - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_ID_REMOVE_FAILED

Description: Query Master failed to remove trigger event query ID from task queue - partial results will be returned

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_ID_UNSUPPORTED

Description: Query Master found unsupported query type hint from App Server - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_INLINEREQUEST_BAD

Description: Query Master received bad inline query request via TCP socket - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_IPC_EVENT_SEND_FAILED

Description: Query Master failed to send IPC event (containing heartbeat data) to Data Manager - trigger event queries may be slow

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_QUERY_IP_GET_FAILED

Description: Query Master failed to get Supervisor IP - Query Master will not be able to communicate with Super data Manager

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_QUERY_IP_INVALID

Description: Query Worker got invalid Query Master IP - queries will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_QUERY_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_LOGINTEGRITYEXPORT_TASK_CREAT_FAILED

Description: Data Manager failed to create task for exporting log integrity check request from App Server - request will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_LOGINTEGRITYEXPORT_TASK_INSERT_FAILED

Description: Data Manager failed to insert task for exporting log integrity check request from App Server into internal task queue - request will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_LOG_INTEGRITY_EXPORT_DIR_UNCONFIGURED

Description: Query Master failed to obtain log integrity export directory - particular request will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_LOG_INTEGRITY_EXPORT_FAILED

Description: Query Master failed to export bad event blocks from file - log integrity query from App server will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_LONG_RUNNING_STOPPED

Description: Long running query stopped

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
reportName	Report Name	string	FortiSIEM report name.

EventType: PH_QUERY_MEM_ALLOC_FAILED

Description: Query Master / Worker failed to allocate memory during event / rule processing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_QUERY_MESSAGE_SEND_FAILED

Description: FortiSIEM Query Engine failed to send message

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
type	Type	string	
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_QUERY_MODULE_INIT_FAILED

Description: Query Master / Worker module failed to initialize

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_MODULE_UNCONFIGURED

Description: Query Master / Worker module failed to obtain some parameters during phoenix_config.txt during initialization - module likely will not start

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	

EventType: PH_QUERY_ONLINE_WORKER_CHANGED

Description: FortiSIEM Online Query Worker number changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_QUERY_PARSED_EVENT_LOAD_FAILED

Description: Query Worker failed to load parsed event from shared buffer during real time query which may not show events from this Query Worker node

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_PARTIAL_WORKER_FAILURE

Description: Partial query results due to worker failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
reportName	Report Name	string	FortiSIEM report name.

EventType: PH_QUERY_PCAP_FINALIZE_FAILED

Description: Query Master failed to finalize pcap export - export will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_PCAP_LOAD_FAILED

Description: Query Master failed to load query results in pcap format - results will not be complete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.

EventType: PH_QUERY_PCAP_RENAME_FAILED

Description: Query Master failed to rename pcap file - export will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_PCAP_TRANSFER_FAILED

Description: Query Master failed to transfer event to pcap packet - results will not be complete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.

EventType: PH_QUERY_PGDB_EXEC_SQL_FAILED

Description: Query Master failed to execute SQL statement against Supervisor Postgres DB for Incident Query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbQuery	Database Query	string	

EventType: PH_QUERY_PGDB_RECONNECT_FAILED

Description: Query Master failed to reconnect to Supervisor Postgres DB - Query Master will remain disconnected and all incident queries will fail

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_QUERY_PGDB_SQL_GET_VAL_FAILED

Description: Query Master failed to get column value from SQL result - incident query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_POST_FILTER_PARSE_FAILED

Description: Query Master failed to parse post-filter inline query results - no post-filtering is going to occur

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_QUERY_PQ_ERROR

Description: FortiSIEM Postgres DB connection or execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_PROCESS_GET_FAILED

Description: Query Master failed to get its own parent process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_PROFILE_ATTR_UNSPECIFIED

Description: Query Master failed to find specified attribute in Profile Query XML from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_PROFILE_EVENT_TYPE_ERROR

Description: Query Master encountered unexpected event type in a Profile Query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_PROFILE_FUNCTION_ERROR

Description: Query Master hit Function error while executing Profile Query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_PROFILE_NOT_MARKED_AS_BASELINE

Description: Query Master will not execute a profile query since it is not marked as baseline

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_PROGRESS_REJECTED

Description: Query Worker fails to upload query progress to Query Master - some progress reporting will be skipped

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
httpStatusCode	HTTP Status	string	

EventType: PH_QUERY_REPORTEXPORT_TASK_CREAT_FAILED

Description: Query Master failed to create task for exporting CSV/PCAP formatted Query request from App Server - export will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_REPORTEXPORT_TASK_INSERT_FAILED

Description: Query Master failed to insert task for exporting CSV/PCAP formatted Query request from App Server into internal task queue - export will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_REPORT_RESULTS_LOAD_FAILED

Description: Query Master failed to load inline query report results from file - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_REPORT_RESULTS_POST_FILTER_FAILED

Description: Query Master failed to post-filter inline query report results - no post-filtering is going to occur

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_REPORT_RESULT_FILE_NOT_EXIST

Description: Query report result file not exist

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_REQUEST_BAD

Description: FortiSIEM Query Engine received bad request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
queryId	Query Id	string	

EventType: PH_QUERY_RESULT_FILES_MERGE_FAILED

Description: Query Master failed to merge inline query result files - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_RESULT_GET_FAILED

Description: Query Master failed to produce inline query result / CSV export - operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.

EventType: PH_QUERY_RESULT_NOT_READY

Description: Query Master failed to find Query result directory for CSV export

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_RESULT_PARSE_FAILED

Description: Query Master failed to parse trigger event query result from Data Manager

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.
queryId	Query Id	string	

EventType: PH_QUERY_RESULT_REJECTED

Description: Query Master rejected query result upload from Query Worker

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
httpStatusCode	HTTP Status	string	

EventType: PH_QUERY_RESULT_SAVE_FAILED

Description: FortiSIEM Query Engine failed to save query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.

EventType: PH_QUERY_RESULT_UPLOAD_FAILED

Description: Query Worker failed to upload query result to Query Master - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
queryId	Query Id	string	
filePath	File Path	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_RT_ERROR

Description: Query Worker spawned excessive threads to handle real time search and will exit (delete)

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_SORT_SPEC_GET_FAILED

Description: Query Master failed to get sort specification for cached query result - query will automatically rerun

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_START_FAILED

Description: Query Worker failed to start a query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
queryId	Query Id	string	
reportName	Report Name	string	FortiSIEM report name.

EventType: PH_QUERY_STATE_BAD

Description: Query Master encounters invalid query state - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_STATUS_LOAD_FAILED

Description: Query Master failed to load query status from disk - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_STATUS_SAVE_FAILED

Description: Query Master failed to save query status to disk - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_SUMM_ATTR_BAD

Description: Query Master encountered bad attribute in Summary Dashboard data cache - cache will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_SUMM_ATTR_MISSING

Description: Query Master failed to locate an attribute in Summary Dashboard data cache - cache will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_SUMM_ATTR_UPDATE_FAILED

Description: Query Master failed to update certain host attribute in Summary Dashboard data cache - cache will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_QUERY_SUMM_COLUMN_UNSUPPORTED

Description: Query Master encountered unsupported attribute in Summary Dashboard data cache - cache will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_SUMM_EVENT_SKIPPED

Description: Query Master skipped a bad event for Summary Dashboard data cache - performance metrics will be partially updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_SUMM_PARSE_FAILED

Description: Query Master failed to parse Summary Dashboard Query XML - one query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_QUERY_SUMM_PERF_ETINFO_UNSUPPORTED

Description: Query Master encountered unsupported perfETInfo in Summary Dashboard Query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_TASK_INVALID

Description: FortiSIEM Query task and worker IP are not matched

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
clientIpAddr	Client IP	IP	

EventType: PH_QUERY_TASK_REROUTED

Description: FortiSIEM Query task is rerouted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_QUERY_TASK_REROUTE_FAILED

Description: FortiSIEM Query Task Reroute failed

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_VALUE_TYPE_UNSUPPORTED

Description: FortiSIEM Query Engine encountered bad value type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_WORKERS_GET_FAILED

Description: Query Master failed to get the list of query workers - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_WORKERS_SPLIT_AMONG_FAILED

Description: Query Master failed to split query among workers - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_WORKER_CHANGED_TO_OFFLINE

Description: FortiSIEM Query Worker Status Changed from online to offline

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_QUERY_WORKER_CHANGED_TO_ONLINE

Description: FortiSIEM Query Worker Status Changed from offline to online

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_QUERY_XML_PARSE_FAILED

Description: Query Master / Worker failed to parse query XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

Report Logs

This section provides logs related to generating reports for dashboards in EventDB/Elasticsearch and for Profile/baselining

- PH_REPORT_ACTION_STATUS
- PH_REPORT_ACT_FAILED
- PH_REPORT_AGGR_FIELDS_EMPTY
- PH_REPORT_AGGR_FIELD_NOT_ADDED
- PH_REPORT_AGGR_FUNC_EMPTY
- PH_REPORT_AGGR_TYPE_ERROR
- PH_REPORT_AGGR_TYPE_UNDEFINED
- PH_REPORT_ATTR_ID_UNSUPPORTED
- PH_REPORT_ATTR_MISSING
- PH_REPORT_ATTR_UNDEFINED
- PH_REPORT_BUFFER_OVERFLOW
- PH_REPORT_CHECKSUM_MISMATCH
- PH_REPORT_CONFIG_UPDATE_NULL
- PH_REPORT_CONVERT_FAILED
- PH_REPORT_DATA_INIT_FAILED
- PH_REPORT_DATA_SIZE_MISMATCH
- PH_REPORT_DATA_SIZE_OVERFLOW
- PH_REPORT_DATA_SIZE_UNEXPECTED
- PH_REPORT_DATA_SIZE_UNKNOWN
- PH_REPORT_DATA_TYPE_UNEXPECTED
- PH_REPORT_DIR_CREATE_FAILED
- PH_REPORT_DIR_OPEN_FAILED
- PH_REPORT_DIR_REMOVE_FAILED
- PH_REPORT_ES_BUCKETS_EMPTY
- PH_REPORT_ES_POST_FAILED
- PH_REPORT_ES_PROFILE_EMPTY
- PH_REPORT_ES_PROFILE_TIMEOUT
- PH_REPORT_ES_PURGE_INDEX_FAILED
- PH_REPORT_ES_TIME_RANGE_INVALID
- PH_REPORT_EXPR_PARSE_FAILED
- PH_REPORT_FILE_CONTENT_MISSING
- PH_REPORT_FILE_COPY_FAILED
- PH_REPORT_FILE_HEADER_BAD
- PH_REPORT_FILE_INIT_FAILED
- PH_REPORT_FILE_LINK_FAILED
- PH_REPORT_FILE_MAGIC_BAD

- PH_REPORT_FILE_MMAP_FAILED
- PH_REPORT_FILE_NAME_BAD
- PH_REPORT_FILE_OPEN_FAILED
- PH_REPORT_FILE_PARSE_FAILED
- PH_REPORT_FILE_READ_FAILED
- PH_REPORT_FILE_REMOVE_FAILED
- PH_REPORT_FILE_RENAME_FAILED
- PH_REPORT_FILE_RSYNC_FAILED
- PH_REPORT_FILE_STAT_FAILED
- PH_REPORT_FILE_TYPE_UNKNOWN
- PH_REPORT_FILE_UNSPECIFIED
- PH_REPORT_FILE_WRITE_FAILED
- PH_REPORT_FUNC_OBJ_DEF_ERROR
- PH_REPORT_FUNC_OBJ_DEF_GET_FAILED
- PH_REPORT_FUNC_OBJ_DEF_UNKNOWN
- PH_REPORT_ID_LOC_DEVICE_EXCLUDED_INVALID
- PH_REPORT_ID_LOC_EVENT_SEND_FAILED
- PH_REPORT_ID_LOC_RESULT_UPLOAD_FAILED
- PH_REPORT_ID_LOC_SYNCH_DATA_UPLOAD_FAILED
- PH_REPORT_ID_LOC_USER_ALREADY_EXCLUDED
- PH_REPORT_ID_LOC_USER_EXCLUDE_FAILED
- PH_REPORT_INDEX_OVERFLOW
- PH_REPORT_IP_GET_FAILED
- PH_REPORT_IP_TYPE_INVALID
- PH_REPORT_KEY_LOAD_FAILED
- PH_REPORT_MODULE_INIT_FAILED
- PH_REPORT_MODULE_UNCONFIGURED
- PH_REPORT_OLD_REPORT_DATA
- PH_REPORT_OP_UNEXPECTED
- PH_REPORT_ORDER_BY_ATTR_EMPTY
- PH_REPORT_ORDER_BY_INVALID
- PH_REPORT_PACK_FAILED
- PH_REPORT_PACK_FAILED_COUNT
- PH_REPORT_PARSED_EVENT_LOAD_FAILED
- PH_REPORT_PGDB_CONNECT_FAILED
- PH_REPORT_PGDB_EXEC_FAILED
- PH_REPORT_PGDB_NOT_CONNECTED
- PH_REPORT_PGDB_NOT_INIT
- PH_REPORT_POINTER_NULL
- PH_REPORT_POINTER_NULL_WARNING
- PH_REPORT_POSITIVE_INTEGER_EXPECTED
- PH_REPORT_PQ_ERROR
- PH_REPORT_PROFILE_TYPE_BAD

- PH_REPORT_PROFILE_TYPE_WRONG_FORMAT
- PH_REPORT_PROFILE_UPDATE_FAILED
- PH_REPORT_ROW_LENGTH_ZERO
- PH_REPORT_RULE_ATTR_MISSING
- PH_REPORT_SCHEMA_INCOMPATIBLE
- PH_REPORT_SCHEMA_INVALID
- PH_REPORT_SCHEMA_LOAD_FAILED
- PH_REPORT_SQLITE3_BATCH_BEGIN_FAILED
- PH_REPORT_SQLITE3_BATCH_COMMIT_FAILED
- PH_REPORT_SQLITE3_BIND_VALUE_FAILED
- PH_REPORT_SQLITE3_BUSY
- PH_REPORT_SQLITE3_BUSY_TIMEOUT_ERROR
- PH_REPORT_SQLITE3_CHECKPOINT_FAILED
- PH_REPORT_SQLITE3_COMMIT_ERROR
- PH_REPORT_SQLITE3_CONFIG_FAILED
- PH_REPORT_SQLITE3_ENABLE_SHARED_CACHE_FAILED
- PH_REPORT_SQLITE3_EXEC_FAILED
- PH_REPORT_SQLITE3_EXTENDED_RESULT_CODES_ERROR
- PH_REPORT_SQLITE3_OPEN_FAILED
- PH_REPORT_SQLITE3_PREPARE_ERROR
- PH_REPORT_SQLITE3_PROFILE_ENTRY_DELETE_FAILED
- PH_REPORT_SQLITE3_PROFILE_NOT_FOUND
- PH_REPORT_SQLITE3_STEP_ERROR
- PH_REPORT_UNPACK_FAILED
- PH_REPORT_VALUE_TYPE_LOOKUP_BY_ID_FAILED
- PH_REPORT_VALUE_TYPE_LOOKUP_BY_NAME_FAILED
- PH_REPORT_VALUE_TYPE_OF_ID_UNEXPECTED
- PH_REPORT_VALUE_TYPE_OF_NAME_UNEXPECTED
- PH_REPORT_VALUE_TYPE_OF_STAT_UNEXPECTED
- PH_REPORT_VALUE_TYPE_UNSUPPORTED
- PH_REPORT_WORKER_UPLOAD_FAILED
- PH_REPORT_XML_ELEMENT_DUPLICATE
- PH_REPORT_XML_ELEMENT_MISSING
- PH_REPORT_XML_ELEMENT_PARSE_FAILED
- PH_REPORT_XML_PARSE_FAILED
- PH_REPORT_ZLIB_COMPRESSION_TYPE_UNKNOWN
- PH_REPORT_ZLIB_UNCOMPRESS_FAILED

EventType: PH_REPORT_ACTION_STATUS

Description: Record action result for report notification

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ACT_FAILED

Description: Query Master/Query Worker/Report Worker/Report Loader failed to perform requested ACTION from App Server, i.e. UPDATE, REMOVE. Event Role will not be updated.

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
roleId	Role ID	uint32	

EventType: PH_REPORT_AGGR_FIELDS_EMPTY

Description: Report Master/Report Worker encountered empty aggregate fields. Report file will be incomplete

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_REPORT_AGGR_FIELD_NOT_ADDED

Description: Query Master/Report Master/Report Worker failed to add certain aggregate field to report schema. The schema will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_AGGR_FUNC_EMPTY

Description: Report Master/Report Worker encountered empty aggregate function. Report file will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_AGGR_TYPE_ERROR

Description: Report Master/Report Worker encountered aggregate type error. Report file will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_AGGR_TYPE_UNDEFINED

Description: Report Master/Report Worker encountered undefined aggregate type. Report file will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ATTR_ID_UNSUPPORTED

Description: Report Master/Report Worker encountered unsupported attribute ID. Report file will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ATTR_MISSING

Description: Report Master/Report Worker failed to locate certain attribute. Report file will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ATTR_UNDEFINED

Description: Report Master/Report Worker encountered undefined attribute. Report file will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_BUFFER_OVERFLOW

Description: Report buffer overflow

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
size	Size	uint32	

EventType: PH_REPORT_CHECKSUM_MISMATCH

Description: Query Master encountered checksum mismatch in report results. The inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_CONFIG_UPDATE_NULL

Description: Report Worker/Report Loader encountered NULL object in config update. Config update will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_CONVERT_FAILED

Description: FortiSIEM internal error used for testing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_REPORT_DATA_INIT_FAILED

Description: Query Master/Report Master failed to initialize report results block data. This inline query or report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_DATA_SIZE_MISMATCH

Description: Query Master/Report Master/Report Worker/Report Loader encountered size mismatch between two pieces of data. The affected operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_DATA_SIZE_OVERFLOW

Description: Query Master/Report Master/Report Worker/Report Loader encountered data size overflow. The affected operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_DATA_SIZE_UNEXPECTED

Description: Query Master/Report Master/Report Worker/Report Loader encountered unexpected data type. The affected operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_DATA_SIZE_UNKNOWN

Description: Query Master/Report Master/Report Worker/Report Loader encountered unknown data size. The affected operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_DATA_TYPE_UNEXPECTED

Description: Query Master/Report Master/Report Worker/Report Loader encountered unexpected data type. The affected operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_DIR_CREATE_FAILED

Description: FortiSIEM Report Engine failed to create directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_DIR_OPEN_FAILED

Description: FortiSIEM Report Engine failed to open directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_DIR_REMOVE_FAILED

Description: FortiSIEM Report Engine failed to remove directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_ES_BUCKETS_EMPTY

Description: Data Manager encountered empty Elastic Search buckets. Report data will not be written to disk

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ES_POST_FAILED

Description: Report Master/Report Worker failed to POST Elastic Search data to App Server. Report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

Id	Display name	Type	Description
httpStatusCode	HTTP Status	string	

EventType: PH_REPORT_ES_PROFILE_EMPTY

Description: Report Master encountered empty Elastic Search profile. Report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_REPORT_ES_PROFILE_TIMEOUT

Description: Report Master encountered timeout in Elastic Search profile response. This profile will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_ES_PURGE_INDEX_FAILED

Description: Elastic Search Purge Inline Report Index Failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ES_TIME_RANGE_INVALID

Description: Report Master encountered invalid time range in Elastic Search profile query. This query will failed to be built

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_EXPR_PARSE_FAILED

Description: Query Master failed to parse schema expression. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_REPORT_FILE_CONTENT_MISSING

Description: Report Master failed to locate certain content in report file. Report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_COPY_FAILED

Description: Report Master/Report Worker failed to copy report file. Report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_HEADER_BAD

Description: Query Master/Report Master/Report Worker encountered bad report file header. This inline query or report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_INIT_FAILED

Description: Report Master/Report Worker failed to initialize report file. Report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_LINK_FAILED

Description: Report Master failed to link report file. Report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_MAGIC_BAD

Description: Query Master/Report Master/Report Worker encountered bad report file magic. Inline query or report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_MMAP_FAILED

Description: Query Master/Report Master failed to memory-map report file. This inline query or report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_NAME_BAD

Description: Report Master/Report Loader encountered bad report file name. This report rolling or loading will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_OPEN_FAILED

Description: Query Master/Report Master/Report Worker/Report Loader failed to open report file. Related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_PARSE_FAILED

Description: FortiSIEM Report Engine failed to parse file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_READ_FAILED

Description: Identity Master/Identity Worker failed to read entry IDs file. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_REMOVE_FAILED

Description: Report Master failed to remove report file. Disk will eventually be full

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_RENAME_FAILED

Description: Report Master failed to rename report file. This report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_RSYNC_FAILED

Description: Report Master failed to rsync report file to remote super

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
targetHostName	Target Host Name	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_STAT_FAILED

Description: Report Worker/Report Loader failed to stat report file. This report writing or loading will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_TYPE_UNKNOWN

Description: Report Worker/Report Loader encountered unknown report file type. This report writing or loading will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_UNSPECIFIED

Description: Report Master/Report Worker encountered unspecified report file. Report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_FILE_WRITE_FAILED

Description: Identity Master/Identity Worker failed to write entry IDs to file. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FUNC_OBJ_DEF_ERROR

Description: Internal error and highly generic. Refer to [procName] and [phLogDetail] tags in the actual log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_FUNC_OBJ_DEF_GET_FAILED

Description: Internal error and highly generic. Refer to [procName] and [phLogDetail] tags in the actual log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_FUNC_OBJ_DEF_UNKNOWN

Description: Internal error and highly generic. Refer to [procName] and [phLogDetail] tags in the actual log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ID_LOC_DEVICE_EXCLUDED_INVALID

Description: FortiSIEM Identity and location module encountered invalid excluded device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ID_LOC_EVENT_SEND_FAILED

Description: FortiSIEM Identity and location module failed to upload events

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_REPORT_ID_LOC_RESULT_UPLOAD_FAILED

Description: FortiSIEM Identity and location module failed to upload results to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
httpStatusCode	HTTP Status	string	

EventType: PH_REPORT_ID_LOC_SYNCH_DATA_UPLOAD_FAILED

Description: FortiSIEM Identity and location module failed to upload Synch Data (Worker to Master)

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_REPORT_ID_LOC_USER_ALREADY_EXCLUDED

Description: FortiSIEM Identity and location module found already excluded user

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	

EventType: PH_REPORT_ID_LOC_USER_EXCLUDE_FAILED

Description: FortiSIEM Identity and location module failed to exclude user

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_REPORT_INDEX_OVERFLOW

Description: Query Master/phRuleMaster/Report Master/Report Worker/Report Loader/Data Manager/Identity Master/Identity Worker encountered index out of bound. Related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.
size	Size	uint32	

EventType: PH_REPORT_IP_GET_FAILED

Description: Failed to get host IP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_REPORT_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_KEY_LOAD_FAILED

Description: FortiSIEM Report module failed to load event attribute keys

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_REPORT_MODULE_INIT_FAILED

Description: Report Master/Report Worker/Report Loader/Identity Master/Identity Worker failed to initialize certain module. Related operation will fail

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_REPORT_MODULE_UNCONFIGURED

Description: Report Worker encountered unconfigured item. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	

EventType: PH_REPORT_OLD_REPORT_DATA

Description: Report Master encountered older report data from Worker, might enlarge block_collection_window

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_REPORT_OP_UNEXPECTED

Description: Query Master/Report Master/Report Worker encountered unexpected operator type. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ORDER_BY_ATTR_EMPTY

Description: Query Master/phRuleMaster/Report Master encountered empty order-by attributes in report. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_ORDER_BY_INVALID

Description: Query Master/phRuleMaster/Report Master encountered invalid order-by attributes in report. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_PACK_FAILED

Description: Failed to pack data

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_REPORT_PACK_FAILED_COUNT

Description: Failed to pack or unpack data

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_REPORT_PARSED_EVENT_LOAD_FAILED

Description: FortiSIEM Report module failed to load event

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_PGDB_CONNECT_FAILED

Description: Report Loader failed to connect to Postgres DB. Report loading will fail

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_REPORT_PGDB_EXEC_FAILED

Description: Report Loader failed to execute SQL statement in Postgres DB. This report loading will fail

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbQuery	Database Query	string	

EventType: PH_REPORT_PGDB_NOT_CONNECTED

Description: Query Master/Report Loader encountered disconnected Postgres DB while executing SQL statement. This incident query or report loading will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbQuery	Database Query	string	

EventType: PH_REPORT_PGDB_NOT_INIT

Description: Query Master/Report Loader encountered uninitialized Postgres DB connection manager. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_REPORT_POINTER_NULL

Description: Query Master/phRuleMaster/Report Master/Report Worker/Report Loader/Data Manager/Identity Master/Identity Worker encountered NULL pointer. Related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_POINTER_NULL_WARNING

Description: NULL pointer detected

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_POSITIVE_INTEGER_EXPECTED

Description: Query Master/Data Manager expected positive integer in performance data but got other value. Default value will be set instead

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.

EventType: PH_REPORT_PQ_ERROR

Description: Query Master/Report Loader encountered PQ function error in Postgres DB. This incident query or report loading will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_PROFILE_TYPE_BAD

Description: FortiSIEM Report module encountered bad profile

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_PROFILE_TYPE_WRONG_FORMAT

Description: Query Master encountered wrong format of profile. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_PROFILE_UPDATE_FAILED

Description: FortiSIEM Report module failed to upload profile

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	

EventType: PH_REPORT_ROW_LENGTH_ZERO

Description: Query Master encountered empty row for given report ID. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_RULE_ATTR_MISSING

Description: Query Master failed to locate certain rule attribute in profile. This profile query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_REPORT_SCHEMA_INCOMPATIBLE

Description: Query Master/Report Master encountered incompatible report schema. This inline query or report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_SCHEMA_INVALID

Description: Query Master/Report Master encountered invalid report schema. This inline query or report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_SCHEMA_LOAD_FAILED

Description: Query Master/Report Master failed to load report schema. This inline query or report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_SQLITE3_BATCH_BEGIN_FAILED

Description: Report Master failed to begin SQLite3 batch transaction. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
profDateType	Profile Date Type	uchar	
hourOfDay	Hour Of Day	uint16	This attribute is not used

EventType: PH_REPORT_SQLITE3_BATCH_COMMIT_FAILED

Description: Report Master failed to commit SQLite3 batch transaction. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
profDateType	Profile Date Type	uchar	
hourOfDay	Hour Of Day	uint16	This attribute is not used

EventType: PH_REPORT_SQLITE3_BIND_VALUE_FAILED

Description: Report Master failed to bind certain value to SQLite3. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
tableName	DB Tablespace Name	string	
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_SQLITE3_BUSY

Description: Report Master encountered SQLite3 busy state. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_SQLITE3_BUSY_TIMEOUT_ERROR

Description: Report Master encountered SQLite3 busy timeout. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbRetCode	DB Return Code	uint32	

EventType: PH_REPORT_SQLITE3_CHECKPOINT_FAILED

Description: FortiSIEM Report module failed to checkpoint profile

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_SQLITE3_COMMIT_ERROR

Description: Report Master encountered commit error in SQLite3. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
tablespaceName	DB Tablespace Name	string	

EventType: PH_REPORT_SQLITE3_CONFIG_FAILED

Description: Report Master failed to configurate SQLite3 with multi-thread mode. Performance will degrade

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_SQLITE3_ENABLE_SHARED_CACHE_FAILED

Description: Report Master failed to enable shared cache for SQLite3. Performance will degrade

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbRetCode	DB Return Code	uint32	

EventType: PH_REPORT_SQLITE3_EXEC_FAILED

Description: Report Master failed to execute SQLite3 statement. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbQuery	Database Query	string	
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
tableName	DB Tablespace Name	string	

EventType: PH_REPORT_SQLITE3_EXTENDED_RESULT_CODES_ERROR

Description: Report Master failed to enable extended result codes for SQLite3. Maintainability will degrade

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbRetCode	DB Return Code	uint32	

EventType: PH_REPORT_SQLITE3_OPEN_FAILED

Description: Report Master failed to open SQLite3. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_SQLITE3_PREPARE_ERROR

Description: Report Master failed to prepare SQLite3 statement. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
tableName	DB Tablespace Name	string	
dbQuery	Database Query	string	
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_SQLITE3_PROFILE_ENTRY_DELETE_FAILED

Description: Report Master failed to delete profile entry from SQLite3. Profile or Daily DB will contain redundant data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
reportId	Report ID	uint32	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
profDateType	Profile Date Type	uchar	
hourOfDay	Hour Of Day	uint16	This attribute is not used

EventType: PH_REPORT_SQLITE3_PROFILE_NOT_FOUND

Description: Report Master failed to find profile ID in SQLite3. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id				Display name				Type				Description			
dbName				DB Name				string							
reportId				Report ID				uint32							

EventType: PH_REPORT_SQLITE3_STEP_ERROR

Description: Report Master failed to step SQLite3 statement. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id				Display name				Type				Description			
tableName				DB Tablespace Name				string							
dbRetCode				DB Return Code				uint32							
errorString				Error String				string				This is the error message, synonymous to attribute errReason			

EventType: PH_REPORT_UNPACK_FAILED

Description: Rule Master failed to unpack rule data from Rule Workers, causing potential incident loss.

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_REPORT_VALUE_TYPE_LOOKUP_BY_ID_FAILED

Description: Report-related process failed to lookup value type by attribute ID. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_VALUE_TYPE_LOOKUP_BY_NAME_FAILED

Description: Report-related process failed to lookup value type by attribute name. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_VALUE_TYPE_OF_ID_UNEXPECTED

Description: Report-related process encountered unexpected value type of certain attribute ID. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_VALUE_TYPE_OF_NAME_UNEXPECTED

Description: Report-related process encountered unexpected value type of certain attribute name. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_VALUE_TYPE_OF_STAT_UNEXPECTED

Description: Report-related process encountered unexpected value type of stat item. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_VALUE_TYPE_UNSUPPORTED

Description: Report-related process encountered unsupported value type. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_WORKER_UPLOAD_FAILED

Description: Failed to upload a data block buffer

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_REPORT_XML_ELEMENT_DUPLICATE

Description: Query Master encountered duplicate XML element. This performance metrics update will not be complete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.

EventType: PH_REPORT_XML_ELEMENT_MISSING

Description: Report Master failed to locate certain XML element. This report rolling will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_REPORT_XML_ELEMENT_PARSE_FAILED

Description: Query Master failed to parse certain XML element. This performance metrics update will not be complete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.

EventType: PH_REPORT_XML_PARSE_FAILED

Description: Report-related process failed to parse certain XML. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_REPORT_ZLIB_COMPRESSION_TYPE_UNKNOWN

Description: Query Master encountered unknown Zlib compression type for report results file. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ZLIB_UNCOMPRESS_FAILED

Description: Query Master failed to uncompress Zlib report results file. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

Rule Logs

This section provides logs related to rule processing and incident generation

- PH_ANOMALY_CONFIG
- PH_ANOMALY_LATERAL_MOVEMENT_ANALYZE
- PH_ANOMALY_LATERAL_MOVEMENT_DETECT
- PH_ANOMALY_LATERAL_MOVEMENT_TRAIN
- PH_ANOMALY_SYSTEM
- PH_ANOMALY_TIMER
- PH_DROP_EVENT_FROM_SHARED_BUFFER
- PH_DROP_INCIDENT
- PH_DROP_INCIDENT_COUNT
- PH_JMS_QUEUE_SIZE_WARNING
- PH_ML_ANOMALY_DETECTED
- PH_RULEMASTER_TEST_RULES_CHECK_SYNTAX
- PH_RULEMASTER_TEST_RULES_FINALIZE_STATE
- PH_RULEMASTER_TEST_RULES_UPDATE_STATE
- PH_RULEMOD_AGGREGATOR_EMPTY
- PH_RULEMOD_ARITH_OP_ILLEGAL
- PH_RULEMOD_ATTR_ALREADY_ASSOCIATED
- PH_RULEMOD_ATTR_ID_LOOKUP_BY_NAME_FAILED
- PH_RULEMOD_ATTR_ID_UNDEFINED
- PH_RULEMOD_ATTR_MISSING
- PH_RULEMOD_ATTR_NAME_LOOKUP_BY_ID_FAILED
- PH_RULEMOD_ATTR_UNDEFINED
- PH_RULEMOD_BUFFER_EMPTY
- PH_RULEMOD_CLEAR_CONDITION_INVALID
- PH_RULEMOD_CLEAR_CONDITION_SET_FAILED
- PH_RULEMOD_CONFIG_UNDEFINED
- PH_RULEMOD_CONSTRUCTOR_ERROR
- PH_RULEMOD_CUST_ID_LIST_INVALID
- PH_RULEMOD_DATA_REQUEST_PARSE_FAILED
- PH_RULEMOD_DATA_SIZE_OVERFLOW
- PH_RULEMOD_DATA_UNSUPPORTED
- PH_RULEMOD_DB_SERVER_HOST_UNDEFINED
- PH_RULEMOD_DIR_OPEN_FAILED
- PH_RULEMOD_ENCODE_FAILED
- PH_RULEMOD_ENTITY_VERSION_MISSING
- PH_RULEMOD_EVENT_TYPE_GROUP_INVALID
- PH_RULEMOD_EVENT_TYPE_NOT_FOUND

- PH_RULEMOD_EXCEPTION_ELEMENT_INVALID
- PH_RULEMOD_EXPR_EVAL_UNKNOWN
- PH_RULEMOD_EXPR_PARSE_FAILED
- PH_RULEMOD_EXPR_UNSUPPORTED
- PH_RULEMOD_FILE_OPEN_FAILED
- PH_RULEMOD_FILE_UNSPECIFIED
- PH_RULEMOD_FORMAT_ERROR
- PH_RULEMOD_FUNC_NOT_FOUND
- PH_RULEMOD_FUNC_PARSE_FAILED
- PH_RULEMOD_GLOBAL_CONSTRAINT_INVALID
- PH_RULEMOD_GROUPBY_LIST_INVALID
- PH_RULEMOD_GROUPBY_LIST_NOT_FOUND
- PH_RULEMOD_GROUP_EVENT_CONSTRAINT_INVALID
- PH_RULEMOD_ID_LOOKUP_BY_INCIDENT_FAILED
- PH_RULEMOD_INCIDENT_ARG_INVALID
- PH_RULEMOD_INCIDENT_CACHE_NOT_FOUND
- PH_RULEMOD_INCIDENT_DEF_INVALID
- PH_RULEMOD_INCIDENT_NOT_FOUND
- PH_RULEMOD_INCIDENT_REPORT_SEND_FAILED
- PH_RULEMOD_INDEX_OVERFLOW
- PH_RULEMOD_INFO_GET_FAILED
- PH_RULEMOD_IP_GET_FAILED
- PH_RULEMOD_IP_INVALID
- PH_RULEMOD_IP_TYPE_INVALID
- PH_RULEMOD_LOAD_METHOD_UNDEFINED
- PH_RULEMOD_MEM_ALLOC_FAILED
- PH_RULEMOD_MODULE_INIT_FAILED
- PH_RULEMOD_MUTEX_ACQUIRE_FAILED
- PH_RULEMOD_NOTIF_CONNECTION_FAILED
- PH_RULEMOD_OBJ_GET_FROM_SUBPATTERN_FAILED
- PH_RULEMOD_OBJ_LOAD_FAILED
- PH_RULEMOD_OP_NOT_FUNC
- PH_RULEMOD_OP_UNKNOWN
- PH_RULEMOD_PARSED_EVENT_LOAD_FAILED
- PH_RULEMOD_PQ_ERROR
- PH_RULEMOD_PROFILE
- PH_RULEMOD_REM_BY_ZERO
- PH_RULEMOD_REM_BY_ZEROD
- PH_RULEMOD_SELECT_ATTR_PARSE_FAILED
- PH_RULEMOD_SELECT_SPEC_PARSE_FAILED
- PH_RULEMOD_SINGLE_EVENT_CONSTRAINT_INVALID
- PH_RULEMOD_SUBPATTERN_INVALID
- PH_RULEMOD_SUBPATTERN_MISSING

- PH_RULEMOD_SUBPATTERN_MORE_THAN_ONE
- PH_RULEMOD_SUBPATTERN_UNDEFINED
- PH_RULEMOD_SUMMARY_UPLOAD_FAILED
- PH_RULEMOD_THREAD_SPAWN_FAILED
- PH_RULEMOD_TOKEN_UNDEFINED
- PH_RULEMOD_TOKEN_UNEXPECTED
- PH_RULEMOD_UNPACK_FAILED
- PH_RULEMOD_VALUE_TYPE_UNEXPECTED
- PH_RULEMOD_XML_ELEMENT_EMPTY
- PH_RULEMOD_XML_ELEMENT_MISSING
- PH_RULEMOD_XML_ELEMENT_PARSE_FAILED
- PH_RULEMOD_XML_ELEMENT_UNEXPECTED
- PH_RULEMOD_XML_ELEMENT_UNKNOWN
- PH_RULEMOD_XML_LOAD_FAILED
- PH_RULEMOD_XML_PARSE_FAILED
- PH_RULEMOD_XML_POINTER_NULL
- PH_RULEWORKER_TEST_RULES_CHECK_SYNTAX
- PH_RULEWORKER_TEST_RULES_EVENT_MATCH_STATUS
- PH_SCHEDULED_RULE_QUERY_FAILED
- PH_TEST_RULES_PARSE_STATUS
- PH_UPDATE_RULE_SUCCEED

EventType: PH_ANOMALY_CONFIG

Description: Anomaly Detection System Config Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_ANOMALY_LATERAL_MOVEMENT_ANALYZE

Description: FSM Anomaly engine: Lateral Movement Module in analyze mode

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
startTime	Start Time	Date	This is the start time of a given item or task, and is stored in epoch milliseconds
endTime	End Time	Date	This is the end time of a given item or task, stored in epoch milliseconds.

EventType: PH_ANOMALY_LATERAL_MOVEMENT_DETECT

Description: FSM Anomaly engine detected Lateral Movement

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcIpAddrList	Source IP List	string	Comma separated list of source IP addresses as identified in a log message
destIpAddrList	Destination IP List	string	Comma separated list of destination IP addresses as identified in a log message
endTime	End Time	Date	This is the end time of a given item or task, stored in epoch milliseconds.

EventType: PH_ANOMALY_LATERAL_MOVEMENT_TRAIN

Description: FSM Anomaly engine: Lateral Movement Module in training mode

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
startTime	Start Time	Date	This is the start time of a given item or task, and is stored in epoch milliseconds
endTime	End Time	Date	This is the end time of a given item or task, stored in epoch milliseconds.

EventType: PH_ANOMALY_SYSTEM

Description: Anomaly Detection System Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_ANOMALY_TIMER

Description: Anomaly Detection System Timer Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_DROP_EVENT_FROM_SHARED_BUFFER

Description: Event dropped from shared buffer

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
collectorId	Collector ID	uint32	This field captures the ID of a FortiSIEM Collector
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_DROP_INCIDENT

Description: Incident dropped

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.
incidentId	Incident ID	uint64	Unique ID of a FortiSIEM Incident
details	Details	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DROP_INCIDENT_COUNT

Description: Dropped incident count

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
incidentCount	Triggered Event Count	uint32	This field represents the number of Triggering events in an Incident.
policyName	Policy Name	string	

EventType: PH_JMS_QUEUE_SIZE_WARNING

Description: JMS Queue large

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ML_ANOMALY_DETECTED

Description: Machine Learning Anomaly Detected

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMASTER_TEST_RULES_CHECK_SYNTAX

Description: Rule master starts to check syntax

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_RULEMASTER_TEST_RULES_FINALIZE_STATE

Description: Rule master finalizes state report summary

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_RULEMASTER_TEST_RULES_UPDATE_STATE

Description: Rule master updates state report summary

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_RULEMOD_AGGREGATOR_EMPTY

Description: Rule Master/Rule Worker encountered empty aggregator. This rule definition will be incomplete

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_ARITH_OP_ILLEGAL

Description: Rule Master/Rule Worker encountered illegal arithmetic operation. This rule evaluation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_ATTR_ALREADY_ASSOCIATED

Description: Rule Master/Rule Worker encountered attribute already associated with given event type in '/opt/phoenix/bin/evtTypeAttrMapForSimpleRule.xml'. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.

EventType: PH_RULEMOD_ATTR_ID_LOOKUP_BY_NAME_FAILED

Description: Rule Master/Rule Worker failed to lookup attribute ID by name in '/opt/phoenix/bin/evtTypeAttrMapForSimpleRule.xml'. The process could terminate depending on the attribute type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_ATTR_ID_UNDEFINED

Description: Rule Master/Rule Worker encountered undefined attribute ID. This rule evaluation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_ATTR_MISSING

Description: Rule Master/Rule Worker failed to locate certain attribute in '/opt/phoenix/bin/evtTypeAttrMapForSimpleRule.xml'. This attribute will be skipped

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_ATTR_NAME_LOOKUP_BY_ID_FAILED

Description: Query Master/Rule Master/Rule Worker failed to lookup attribute name by ID. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_ATTR_UNDEFINED

Description: Query Master/Rule Master/Rule Worker encountered undefined event attribute. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_BUFFER_EMPTY

Description: Rule Master/Rule Worker encountered empty buffer in loading '/opt/phoenix/bin/evtTypeAttrMapForSimpleRule.xml'. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_CLEAR_CONDITION_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid clear condition in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_CLEAR_CONDITION_SET_FAILED

Description: Query Master/Rule Master/Rule Worker failed to set clear condition in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_CONFIG_UNDEFINED

Description: Rule Master encountered undefined config item of db_server_host. Incident processing will not work

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configName	Config Name	string	

EventType: PH_RULEMOD_CONSTRUCTOR_ERROR

Description: Rule Master/Rule Worker encountered error in constructor of given module. This rule evaluation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	

EventType: PH_RULEMOD_CUST_ID_LIST_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid customer ID list in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_RULEMOD_DATA_REQUEST_PARSE_FAILED

Description: Query Master failed to parse data request from App Server. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_RULEMOD_DATA_SIZE_OVERFLOW

Description: Rule Master/Rule Worker encountered data size exceeding its capacity. This rule parsing or evaluation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_DATA_UNSUPPORTED

Description: Rule Master/Rule Worker encountered unsupported data. This rule parsing or evaluation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_DB_SERVER_HOST_UNDEFINED

Description: Database server host not defined for rule master

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configName	Config Name	string	

EventType: PH_RULEMOD_DIR_OPEN_FAILED

Description: Rule Master/Rule Worker failed to open rule XML directory. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_RULEMOD_ENCODE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to encode given data. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_ENTITY_VERSION_MISSING

Description: Query Master/Rule Master/Rule Worker failed to identify entity version of rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_EVENT_TYPE_GROUP_INVALID

Description: Rule Worker failed to parse certain event type group in rules. Affected rule evaluation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventTypeGrp	Event Type Group	string	This field is not used

EventType: PH_RULEMOD_EVENT_TYPE_NOT_FOUND

Description: Query Master/Rule Master/Rule Worker failed to find certain event type in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_EXCEPTION_ELEMENT_INVALID

Description: Rule Master encountered invalid element in rule exception. This rule exception parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
description	Description	string	

EventType: PH_RULEMOD_EXPR_EVAL_UNKNOWN

Description: Query Master encountered unknown expression evaluation of given operator type. This incident query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_EXPR_PARSE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to parse certain expression. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_RULEMOD_EXPR_UNSUPPORTED

Description: Query Master/Rule Master/Rule Worker encountered unsupported expression in aggregate function. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_RULEMOD_FILE_OPEN_FAILED

Description: Rule Master/Rule Worker failed to open rule-related file. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_RULEMOD_FILE_UNSPECIFIED

Description: Rule Master/Rule Worker encountered unspecified rule XML file. This rule update will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_RULEMOD_FORMAT_ERROR

Description: Query Master/Rule Master/Rule Worker encountered format error in given expression. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_FUNC_NOT_FOUND

Description: Query Master/Rule Master/Rule Worker failed to locate certain function in given expression. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_RULEMOD_FUNC_PARSE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to parse certain function in given expression. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_RULEMOD_GLOBAL_CONSTRAINT_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid global constraint in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.
task	Task	string	

EventType: PH_RULEMOD_GROUPBY_LIST_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid group-by list in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_RULEMOD_GROUPBY_LIST_NOT_FOUND

Description: Query Master/Rule Master/Rule Worker failed to find group-by list in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_GROUP_EVENT_CONSTRAINT_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid group event constraint in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_RULEMOD_ID_LOOKUP_BY_INCIDENT_FAILED

Description: Rule Master failed to lookup rule ID by incident ID. This incident firing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
incidentId	Incident ID	uint64	Unique ID of a FortiSIEM Incident
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_RULEMOD_INCIDENT_ARG_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid incident argument in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_RULEMOD_INCIDENT_CACHE_NOT_FOUND

Description: Rule Master failed to find incident cache for given incident ID. This incident will not be cleared

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
incidentId	Incident ID	uint64	Unique ID of a FortiSIEM Incident
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_INCIDENT_DEF_INVALID

Description: Query Master/Rule Master encountered invalid incident definition in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_INCIDENT_NOT_FOUND

Description: Rule Master failed to find given incident ID. This incident will not be cleared

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
incidentId	Incident ID	uint64	Unique ID of a FortiSIEM Incident

EventType: PH_RULEMOD_INCIDENT_REPORT_SEND_FAILED

Description: Rule Master failed to send incident report to phParser. This incident will be missing in eventdb

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_RULEMOD_INDEX_OVERFLOW

Description: Query Master encountered out-of-bound index in certain data. This incident query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.
size	Size	uint32	

EventType: PH_RULEMOD_INFO_GET_FAILED

Description: FortiSIEM Report module failed to get statistics

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_IP_GET_FAILED

Description: Rule Worker failed to get host IP of Supervisor. Incident firing will not work

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_RULEMOD_IP_INVALID

Description: Query Master/Rule Master/Rule Worker found invalid IP in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_RULEMOD_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_LOAD_METHOD_UNDEFINED

Description: Rule Master/Rule Worker encountered undefined rule load method. Rule loading will fail

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_MEM_ALLOC_FAILED

Description: Query Master/Rule Master/Rule Worker failed to allocate memory. The related operation will fail

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_MODULE_INIT_FAILED

Description: Rule Master/Rule Worker failed to be initialized. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_MUTEX_ACQUIRE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to acquire mutex. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	

EventType: PH_RULEMOD_NOTIF_CONNECTION_FAILED

Description: Rule Master failed to establish notification connection to phParser. This incident will be missing in eventdb

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_RULEMOD_OBJ_GET_FROM_SUBPATTERN_FAILED

Description: Rule Master failed to get certain object from subpattern. This incident cache update will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_OBJ_LOAD_FAILED

Description: Query Master/Rule Master/Rule Worker failed to load certain object in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_OP_NOT_FUNC

Description: Rule Master encountered an operator of non-function type. This incident initialization will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_OP_UNKNOWN

Description: Query Master/Rule Master/Rule Worker encountered unknown operator. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_PARSED_EVENT_LOAD_FAILED

Description: Rule Worker failed to load and skipped a parsed event, causing potential incident loss.

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_PQ_ERROR

Description: Rule Master encountered PQ function error in Postgres DB. Incident processing will not work

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_RULEMOD_PROFILE

Description: FortiSIEM Rule resource usage profile

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleName	Rule Name	string	FortiSIEM rule name.
usedMemKB	Used Memory	uint32	
updateQueueSize	Update Queue Size	uint32	

EventType: PH_RULEMOD_REM_BY_ZERO

Description: Rule Master/Rule Worker caught remainder-by-zero exception. Default value will be set instead

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_REM_BY_ZEROD

Description: FortiSIEM Report module failed to produce statistics

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_SELECT_ATTR_PARSE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to parse and skipped certain select attribute. This rule parsing will be incomplete

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_SELECT_SPEC_PARSE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to parse at least one select spec field. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_SINGLE_EVENT_CONSTRAINT_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid single event constraint in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_RULEMOD_SUBPATTERN_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid subpattern in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

Id	Display name	Type	Description
ruleName	Rule Name	string	FortiSIEM rule name.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_SUBPATTERN_MISSING

Description: Query Master/Rule Master/Rule Worker failed to locate certain subpattern in XML. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_SUBPATTERN_MORE_THAN_ONE

Description: Query Master/Rule Master/Rule Worker encountered more than one subpattern in simple rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_SUBPATTERN_UNDEFINED

Description: Query Master/Rule Master/Rule Worker encountered undefined subpattern in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_SUMMARY_UPLOAD_FAILED

Description: Rule Worker failed to upload rule summary to Rule Master, causing potential incident loss.

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_THREAD_SPAWN_FAILED

Description: Rule Master/Rule Worker failed to spawn thread during initialization. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_RULEMOD_TOKEN_UNDEFINED

Description: Query Master/Rule Master/Rule Worker encountered undefined token of given type in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_TOKEN_UNEXPECTED

Description: Query Master/Rule Master/Rule Worker encountered unexpected token of given type in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_UNPACK_FAILED

Description: Rule Master failed to unpack rule data from Rule Workers, causing potential incident loss.

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_VALUE_TYPE_UNEXPECTED

Description: Query Master encountered unexpected value type of certain attribute. This incident query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_XML_ELEMENT_EMPTY

Description: Query Master/Rule Master/Rule Worker encountered empty XML element. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_XML_ELEMENT_MISSING

Description: Query Master/Rule Master/Rule Worker encountered missing XML element. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_XML_ELEMENT_PARSE_FAILED

Description: Query Master failed to parse certain XML element. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_XML_ELEMENT_UNEXPECTED

Description: Query Master/Rule Master/Rule Worker encountered unexpected XML element. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_XML_ELEMENT_UNKNOWN

Description: Query Master/Rule Master/Rule Worker encountered unknown XML element. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_XML_LOAD_FAILED

Description: Rule Master/Rule Worker failed to load rule XML from file. This rule loading will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_RULEMOD_XML_PARSE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to parse rule XML. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_RULEMOD_XML_POINTER_NULL

Description: NULL pointer in XML detected

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEWORKER_TEST_RULES_CHECK_SYNTAX

Description: Rule worker starts to check syntax

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_RULEWORKER_TEST_RULES_EVENT_MATCH_STATUS

Description: Rule worker event test status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventId	Event ID	uint64	This is a globally unique ID assigned to every raw event ingested into the SIEM. This is used by the system for tying events to incidents, and is typically not needed by end users.

EventType: PH_SCHEDULED_RULE_QUERY_FAILED

Description: Failed to run query for scheduled rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_TEST_RULES_PARSE_STATUS

Description: Syntax check status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_UPDATE_RULE_SUCCEED

Description: Rule update succeeded

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
opName	Operation Name	string	
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

System Logs

This section provides logs related phMonitor module.

- PH_BAD_ROUTE_OUTPUT
- PH_BASE_PROC_BASE_AGENT_JOB_NO_THREAD_NUM_ASSIGNED
- PH_BASE_PROC_DUMP_STACK_TRACE_FAILURE
- PH_BASE_PROC_GET_PID_FILE_FAILED
- PH_BASE_PROC_HANDLE_NOTIFICATION_ERROR
- PH_BASE_PROC_KILL_PROC_ERROR
- PH_BASE_PROC_NOTIFICATION_HANDLE_CONN_ERROR
- PH_BASE_PROC_NO_CONN_TO_HEARTBEAT_SERVER
- PH_BASE_PROC_RENAME_MINI_DUMP_FILE_FAILURE
- PH_BASE_PROC_REST_CACHE_CHECKOUT_STATUS_WARNING
- PH_BASE_PROC_SEND_HEARTBEAT_FAILURE
- PH_BASE_PROC_SEND_USER_DEFINED_SIG_FAILED
- PH_BASE_PROC_SET_PID_FILE_FAILED
- PH_BASE_PROC_STACK_TRACE
- PH_BASE_PROC_STACK_TRACK_TOO_LONG
- PH_BASE_PROC_SYS_INFO_CALC_CPU_ERROR
- PH_BASE_PROC_SYS_PROC_INFO_GET_FAILURE
- PH_BASE_PROC_SYS_PROC_INFO_INIT_ERROR
- PH_BASE_PROC_SYS_PROC_INFO_UNABLE_OPEN_PROC_PID_FILE
- PH_BASE_PROC_SYS_PROC_INFO_UNABLE_OPEN_PROC_STAT_FILE
- PH_BASE_PROC_THREAD_SPAWN_FAILED
- PH_BASE_PROC_THREAD_WRONG_PARAM
- PH_BASE_PROC_UPLOAD_FILE_FAILURE
- PH_BASE_PROC_VALUE_GROUP_UPDATE_FAILURE
- PH_BASE_PRO_AQUIRE_SHARED_STORE_FAILED
- PH_CLIHOUSE_BUILD_QUERY_DIST_SQL_COMMAND_FAILURE
- PH_CLI_ERROR
- PH_CREATE_TEMP_FILE_FAILURE
- PH_DISC_DATA_PROCESS_ERROR
- PH_DIVIDE_BY_ZERO
- PH_FAILED_TO_EXEC
- PH_FILE_NOT_FOUND
- PH_GCS_BUCKET_ACCESS_FAILURE
- PH_GENERIC_CRITICAL
- PH_GENERIC_DEBUG
- PH_GENERIC_ERROR
- PH_GENERIC_INFO

- PH_GENERIC_WARNING
- PH_GET_CURL_HANDLE_FAILED
- PH_GET_SUPER_LEADER_FAILURE
- PH_GRPC_CERT_CREATE_SUCCESS
- PH_GRPC_CERT_ERROR
- PH_GRPC_CERT_LOADED_FAILED
- PH_GRPC_CERT_UPDATE_FAILED
- PH_GRPC_CERT_UPDATE_SUCCESS
- PH_GRPC_FORTMAT_JSON_FAILED
- PH_GRPC_INIT_SSL_CONTEXT
- PH_GRPC_TASK_DATA_EMPTY
- PH_HTTP_CLIENT_COMPRESS_FAILED
- PH_HTTP_CLIENT_CURL_ERROR
- PH_HTTP_CLIENT_GET_CACHE_FROM_MONITOR_FAILED
- PH_HTTP_CLIENT_GET_DATA_FROM_CACHE_FAILED
- PH_HTTP_CLIENT_GET_INIT_RESPONSE_FAILED
- PH_HTTP_CLIENT_GET_INIT_RESPONSE_WARNING
- PH_HTTP_CLIENT_GET_RESPONSE_WARNING
- PH_HTTP_CLIENT_HOST_IS_NULL
- PH_HTTP_CLIENT_INIT_FAILURE
- PH_HTTP_CLIENT_INIT_WARNING
- PH_HTTP_CLIENT_INVALID_FILE_SIZE
- PH_HTTP_CLIENT_MKSTEMP_FAILED
- PH_HTTP_CLIENT_NO_FILE_PARAM
- PH_HTTP_CLIENT_PICK_SUPER_FAILED
- PH_HTTP_CLIENT_PREP_REQUEST_ERROR
- PH_HTTP_CLIENT_PUT_REDIRECT_FAILURE
- PH_HTTP_CLIENT_SETOPT_FAILED
- PH_HTTP_CLIENT_SET_HOST_WARNING
- PH_HTTP_CLIENT_UPLOAD_FILE_FAILED
- PH_HTTP_CLIENT_WRITE_CACHE_NULL
- PH_HTTP_INIT_FAILURE
- PH_HTTP_RESPONSE_FAILURE
- PH_INCIDENT_ACTION_STATUS
- PH_INVALID_IP_ADDR
- PH_INVALID_PARAM
- PH_INVALID_PARAM_CNT
- PH_INVALID_PARAM_VAL_EMPTY
- PH_LOAD_CONFIG_CHANGE_FAILED
- PH_LOOKUP_TABLE_CANNOT_LOAD_DATA
- PH_MODULE_ABORT
- PH_MODULE_ABORT_FOUND
- PH_MODULE_ACCEPTED_CONN

- PH_MODULE_ACE_ACCEPTOR_FAILED
- PH_MODULE_ACE_HANDLE_EVENT_ERROR
- PH_MODULE_COMM_ERROR
- PH_MODULE_COMM_HANDLER_REG
- PH_MODULE_COMM_PORTS_OPENED
- PH_MODULE_DB_CONFIG_LOADED
- PH_MODULE_DIODE_CONFIG_ERROR
- PH_MODULE_EXCEPTION_NOT_CAUGHT
- PH_MODULE_EXITING
- PH_MODULE_EXIT_OK
- PH_MODULE_HEARTBEAT_INIT
- PH_MODULE_INITIALIZING
- PH_MODULE_INIT_COMPLETE
- PH_MODULE_INIT_FAILURE
- PH_MODULE_LOADED_NEW_CONFIG
- PH_MODULE_LOAD_DIODE_CRED_ERROR
- PH_MODULE_LOCAL_CONFIG_LOADED
- PH_MODULE_LOCAL_CONFIG_SECTION_ERROR
- PH_MODULE_LOCAL_CONFIG_VALUE_ERROR
- PH_MODULE_LOG_LEVEL_CHANGE
- PH_MODULE_RECVD_EXIT_EXT
- PH_MODULE_RECVD_EXIT_MONITOR
- PH_MODULE_RECVD_NEW_CONFIG
- PH_MODULE_RECVD_START
- PH_MODULE_SETPIDFILE_ERR
- PH_MODULE_UNABLE_INIT_SHARED_STORE
- PH_MODULE_UNABLE_OPEN_COMM_PORT
- PH_NOTIFICATION_ACCEPT_FAILURE
- PH_NOTIFICATION_CALLBACK_ERROR
- PH_NOTIFICATION_CONN_FAILED
- PH_NOTIFICATION_INIT_FAILED
- PH_NOTIFICATION_NO_RESPONSE
- PH_NOTIFICATION_RETURN_FAILURE
- PH_NOTIFICATION_SEND_FAILURE
- PH_NOTIFICATION_SEND_FILE_FAILURE
- PH_OBJECT_NOT_FOUND
- PH_PDF_BUILDER_ERROR
- PH_READER_BLOCK_WRITE
- PH_Rule_AbuseCH_Botnetc2_MalwareIP_Inbound
- PH_Rule_AbuseCH_Botnetc2_MalwareIP_Outbound
- PH_Rule_Blocklist_MalwareIP_Inbound
- PH_Rule_Blocklist_MalwareIP_Outbound
- PH_Rule_C2_Tracker_MalwareIP_Inbound

- PH_Rule_C2_Tracker_MalwareIP_Outbound
- PH_Rule_CINSScore_MalwareIP_Inbound
- PH_Rule_CINSScore_MalwareIP_Outbound
- PH_Rule_CertPL_MalwareDomain_Inbound
- PH_Rule_CertPL_MalwareDomain_Outbound
- PH_Rule_Cisco_Talos_MalwareIP_Inbound
- PH_Rule_Cisco_Talos_MalwareIP_Outbound
- PH_Rule_Cluster_DBLeader_Changed
- PH_Rule_Cluster_REPL_Leader_Changed
- PH_Rule_DigitalSide_MalwareDomain_Inbound
- PH_Rule_DigitalSide_MalwareDomain_Outbound
- PH_Rule_DigitalSide_MalwareIP_Inbound
- PH_Rule_DigitalSide_MalwareIP_Outbound
- PH_Rule_DigitalSide_MalwareURL_Outbound
- PH_Rule_FML_Antispam_Malicious_File
- PH_Rule_FML_Antispam_Malicious_Url
- PH_Rule_FireHol_MalwareIP_Inbound
- PH_Rule_FireHol_MalwareIP_Outbound
- PH_Rule_FortiRecon_MalwareDomain_Inbound
- PH_Rule_FortiRecon_MalwareDomain_Outbound
- PH_Rule_FortiRecon_MalwareIP_Inbound
- PH_Rule_FortiRecon_MalwareIP_Outbound
- PH_Rule_FortiRecon_MalwareURL_Outbound
- PH_Rule_FortiSOAR_MalwareDomain_Inbound
- PH_Rule_FortiSOAR_MalwareDomain_Outbound
- PH_Rule_FortiSOAR_MalwareIP_Inbound
- PH_Rule_FortiSOAR_MalwareIP_Outbound
- PH_Rule_FortiSOAR_MalwareURL_Outbound
- PH_Rule_Greensnow_MalwareIP_Inbound
- PH_Rule_Greensnow_MalwareIP_Outbound
- PH_Rule_IPSum_MalwareIP_Inbound
- PH_Rule_IPSum_MalwareIP_Outbound
- PH_Rule_MISP_MalwareDomain_Inbound
- PH_Rule_MISP_MalwareDomain_Outbound
- PH_Rule_MISP_MalwareIP_Inbound
- PH_Rule_MISP_MalwareIP_Outbound
- PH_Rule_MISP_MalwareURL_Outbound
- PH_Rule_Mandiant_MalwareDomain_Inbound
- PH_Rule_Mandiant_MalwareDomain_Outbound
- PH_Rule_Mandiant_MalwareIP_Inbound
- PH_Rule_Mandiant_MalwareIP_Outbound
- PH_Rule_Mandiant_MalwareURL_Outbound
- PH_Rule_OPENCTI_MalDomain_Inbound

- PH_Rule_OPENCTI_MalDomain_Outbound
- PH_Rule_OPENCTI_MalwareIP_Inbound
- PH_Rule_OPENCTI_MalwareIP_Outbound
- PH_Rule_OPENCTI_MalwareURL_Outbound
- PH_Rule_OpenPhish_MalwareURL_Outbound
- PH_Rule_Proofpoint_MalwareIP_Inbound
- PH_Rule_Proofpoint_MalwareIP_Outbound
- PH_Rule_Snort_MalwareIP_Inbound
- PH_Rule_Snort_MalwareIP_Outbound
- PH_Rule_ThreatFox_MalwareURL_Outbound
- PH_Rule_TweetFeed_MalwareDomain_Inbound
- PH_Rule_TweetFeed_MalwareDomain_Outbound
- PH_Rule_TweetFeed_MalwareURL_Outbound
- PH_Rule_Tweetfeed_MalwareIP_Inbound
- PH_Rule_Tweetfeed_MalwareIP_Outbound
- PH_SAAS_OP_COLLECTOR_DOWN
- PH_SAAS_OP_COLLECTOR_UP
- PH_SER_MON_SERVICE_DOWN
- PH_SHAREDSTORE_ACQUIRE_ERROR
- PH_SHAREDSTORE_WRITER_POS_UNEXPECTED_ALTERED
- PH_SHAREDSTORE_WRITE_ERROR
- PH_SSL_SHUTDOWN_ERROR
- PH_SYSTEM_DROP_UNKNOWN_ORG
- PH_SYSTEM_RAW_EVENT_SIZE
- PH_SYSTEM_STORAGE_LOW
- PH_SYS_ERROR_XML_SEND_ERROR
- PH_SYS_ERROR_XML_SENT
- PH_TASK_DATA_EMPTY
- PH_TASK_DATA_IS_WRONG
- PH_TASK_FAILED
- PH_TASK_NOT_CONTAIN_LIC
- PH_TASK_RUN_COMMAND_FAILED
- PH_TASK_SEND_FAILED
- PH_TASK_UNSUPPORT
- PH_THREAD_EXITING
- PH_THREAD_RECVD_EXIT
- PH_THREAD_STARTING
- PH_UNABLE_ACCESS_DIR
- PH_UNABLE_ALLOC_MEMORY
- PH_UNABLE_CREATE_DIR
- PH_UNABLE_CREATE_FILE
- PH_UNABLE_CREATE_TIMER
- PH_UNABLE_OPEN_DIR

- PH_UNABLE_OPEN_FILE
- PH_UNABLE_PARSE_XML
- PH_UNABLE_RENAME_FILE
- PH_UNRESOLVABLE_HOSTNAME
- PH_UNRESOLVABLE_IP
- PH_UTIL_BIZ_CHANGE_UPDATE_SPAWN_FAILURE
- PH_UTIL_BIZ_HTTP_REQUEST_FAILURE
- PH_UTIL_CMD_FAILURE
- PH_UTIL_CONFIG_IP_MISSING
- PH_UTIL_CONFIG_LOAD_FAILURE
- PH_UTIL_CONFIG_LOAD_FILE_ACCESS_FAILURE
- PH_UTIL_CONFIG_PARSE_FAILURE
- PH_UTIL_CONFIG_UNKNOWN_SERVER_TYPE
- PH_UTIL_CONNECTION_ERROR
- PH_UTIL_CSV_LINE_ILLEGAL
- PH_UTIL_CSV_READ_FAILURE
- PH_UTIL_CUSTOMER_COLLECTOR_MISSING
- PH_UTIL_CUSTOMER_COLLECTOR_PARSE_FAILURE
- PH_UTIL_CUSTOMER_DOMAIN_MISSING
- PH_UTIL_CUSTOMER_INFO_PARSE_FAILURE
- PH_UTIL_CUSTOMER_PARSE_FAILURE
- PH_UTIL_DASHBOARD_DUPLICATE_IP
- PH_UTIL_DASHBOARD_DUPLICATE_ITEM
- PH_UTIL_DASHBOARD_PARSE_FAILURE
- PH_UTIL_DEVICE_MAP_PROP_ERROR
- PH_UTIL_DEVICE_PROP_ERROR
- PH_UTIL_DEVICE_SIMPLE_PROP_PARSE_FAILURE
- PH_UTIL_DGA_FREQ_FILE_OPEN_FAILURE
- PH_UTIL_DGA_WHITELIST_FILE_OPEN_FAILURE
- PH_UTIL_DIR_CREATE_FAILURE
- PH_UTIL_DIR_CREATE_RETRIED
- PH_UTIL_DIR_OPEN_FAILURE
- PH_UTIL_DIR_PARENT_NOT_EXIST
- PH_UTIL_DIR_REMOVE_FAILURE
- PH_UTIL_DISK_USAGE_INFO_GET_FAILURE
- PH_UTIL_DISPATH_CMD_XML_ILLEGAL
- PH_UTIL_DISPATH_CMD_XML_PARSE_FAILURE
- PH_UTIL_EMAIL_SEND_FAILURE
- PH_UTIL_ETCD_COMPAGN_FAILED
- PH_UTIL_ETCD_GET_LEADER_FAILED
- PH_UTIL_ETCD_LEASE_FAILED
- PH_UTIL_ETCD_SET_FAILED
- PH_UTIL_EVENT_FILE_ERROR

- PH_UTIL_EVENT_GROUP_ERROR
- PH_UTIL_EVENT_STATUS_REPORTER_SPAWN_FAILURE
- PH_UTIL_EVENT_STATUS_UPLOAD_FAILURE
- PH_UTIL_EVENT_TYPE_ERROR
- PH_UTIL_FILE_NOT_EXIST
- PH_UTIL_FILE_OPEN_FAILURE
- PH_UTIL_FILE_READ_FAILURE
- PH_UTIL_FILE_SIZE_MISMATCH
- PH_UTIL_FILE_SIZE_TOO_SMALL
- PH_UTIL_FILE_STATFS_FAILURE
- PH_UTIL_FILE_STAT_FAILURE
- PH_UTIL_FILE_WRITE_FAILURE
- PH_UTIL_FORK_FAILURE
- PH_UTIL_GET_ADDR_FAILURE
- PH_UTIL_GET_ATTR_NAME_FAILED
- PH_UTIL_GET_JOB_STATUS_FAILURE
- PH_UTIL_HOSTNAME_GET_FAILURE
- PH_UTIL_INET_PTON_FAILURE
- PH_UTIL_INODE_INFO_GET_FAILURE
- PH_UTIL_INVALID_PARAM
- PH_UTIL_IOCTL_FAILURE
- PH_UTIL_IOCTL_SIOCGIFADDR_FAILURE
- PH_UTIL_IP_TYPE_INVALID
- PH_UTIL_IP_TYPE_MISMATCH
- PH_UTIL_JOB_STATUS_REPORTER_SPAWN_FAILURE
- PH_UTIL_JOB_STATUS_UPLOAD_FAILURE
- PH_UTIL_JSON_GET_NODE_FAILURE
- PH_UTIL_JSON_GET_TOTAL_COUNT_FAILURE
- PH_UTIL_JSON_OBJ_EMPTY
- PH_UTIL_JSON_PARSE_FAILURE
- PH_UTIL_KILLPG_FAILURE
- PH_UTIL_LOAD_EXT_FUNC_FILE_OPEN_FAILURE
- PH_UTIL_LOAD_EXT_FUNC_FORMAT_INVALID
- PH_UTIL_LOAD_EXT_FUNC_GET_NAME_FAILURE
- PH_UTIL_LOCAL_IP_MISSING
- PH_UTIL_LOOKUP_TABLES_DUPLICATE
- PH_UTIL_LOOKUP_TABLES_DUPLICATE_COLUMN
- PH_UTIL_LOOKUP_TABLES_DUPLICATE_KEY
- PH_UTIL_MAIL_CMD_RUN_FAILURE
- PH_UTIL_MAIL_SMTP_INIT_FAILURE
- PH_UTIL_MD5_ERROR
- PH_UTIL_MEM_ALLOC_FAILURE
- PH_UTIL_MKDTMP_FAILURE

- PH_UTIL_MKSTEMP_FAILURE
- PH_UTIL_MMAP_FAILURE
- PH_UTIL_MOVE_FILE_FAILURE
- PH_UTIL_NOTIFICATION_SENDER_SPAWN_FAILURE
- PH_UTIL_NOTIFICATION_SERVER_INIT_FAILURE
- PH_UTIL_NOTIFICATION_UPLOAD_FAILURE
- PH_UTIL_PCRE_COMPILE_FAILED
- PH_UTIL_PHOENIX_CONFIG_ITEM_MISSING
- PH_UTIL_PIPE_FAILURE
- PH_UTIL_PROP_DEF_SET_PARSE_FAILURE
- PH_UTIL_REDIS_CONNECTION_ERROR
- PH_UTIL_REGEX_PATTERN_EMPTY
- PH_UTIL_REGEX_PATTERN_TOO_LONG
- PH_UTIL_SEND_DATA_FAILED
- PH_UTIL_SEND_TO_UDP_PORT_FAILURE
- PH_UTIL_SETPGRP_FAILURE
- PH_UTIL_SET_JOB_STATUS_FAILURE
- PH_UTIL_SOCKET_FAILURE
- PH_UTIL_STR_TO_IP_FAILURE
- PH_UTIL_SVN_DIFF_FAILURE
- PH_UTIL_SYS_ERROR_REPORTER_INIT_FAILURE
- PH_UTIL_TIME_RANGE_INVALID
- PH_UTIL_TIME_STR_FORMAT_INVALID
- PH_UTIL_TLS_SERVER_RECV_FAILED
- PH_UTIL_UNKNOWN_PHOENIX_ERROR_NUMBER
- PH_UTIL_VALUE_GROUP_ERROR
- PH_UTIL_WAITPID_FAILURE
- PH_UTIL_WAITPID_LAST_TRY_FAILURE
- PH_UTIL_WINDOWS_BID_LOAD_FAILURE
- PH_UTIL_WRITE_BIN_FILE_OPEN_FAILURE
- PH_UTIL_WRITE_FILE_OPEN_FAILURE
- PH_UTIL_XML_HANDLING_ERROR
- PH_UTIL_ZIP_DECOMPRESS_FAILED
- PH_WORKER_DOWN
- PH_WORKER_PROVISION_FAILED
- PH_WORKER_UP
- PH_WS_COMM_ERROR

EventType: PH_BAD_ROUTE_OUTPUT

Description: FortiSIEM encountered bad route output

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_BASE_AGENT_JOB_NO_THREAD_NUM_ASSIGNED

Description: FortiSIEM module error - no thread count assigned

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_DUMP_STACK_TRACE_FAILURE

Description: FortiSIEM module error - stack trace failed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
filePath	File Path	string	

EventType: PH_BASE_PROC_GET_PID_FILE_FAILED

Description: FortiSIEM module error - failed to get process id

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_BASE_PROC_HANDLE_NOTIFICATION_ERROR

Description: FortiSIEM module error - notification error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_KILL_PROC_ERROR

Description: FortiSIEM module error - failed to kill process

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_BASE_PROC_NOTIFICATION_HANDLE_CONN_ERROR

Description: FortiSIEM module error - no notification connection

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_NO_CONN_TO_HEARTBEAT_SERVER

Description: FortiSIEM module error - no connection to heartbeat

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_RENAME_MINI_DUMP_FILE_FAILURE

Description: FortiSIEM module error - minidump error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_REST_CACHE_CHECKOUT_STATUS_WARNING

Description: FortiSIEM module error - REST cache access error

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event

EventType: PH_BASE_PROC_SEND_HEARTBEAT_FAILURE

Description: FortiSIEM module error - failed to send heartbeat

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
procName	Process Name	string	

EventType: PH_BASE_PROC_SEND_USER_DEFINED_SIG_FAILED

Description: FortiSIEM module error - user defined sig failed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_SET_PID_FILE_FAILED

Description: FortiSIEM module error - setpid failed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_BASE_PROC_STACK_TRACE

Description: FortiSIEM module stack trace

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_STACK_TRACK_TOO_LONG

Description: FortiSIEM module error - stack trace too large

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_SYS_INFO_CALC_CPU_ERROR

Description: FortiSIEM module error - failed to calculate CPU

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
procName	Process Name	string	

EventType: PH_BASE_PROC_SYS_PROC_INFO_GET_FAILURE

Description: FortiSIEM module error - failed to get proc info

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_SYS_PROC_INFO_INIT_ERROR

Description: FortiSIEM module error - proc info get error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_SYS_PROC_INFO_UNABLE_OPEN_PROC_PID_FILE

Description: FortiSIEM module error - unable to open proc pid file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_BASE_PROC_SYS_PROC_INFO_UNABLE_OPEN_PROC_STAT_FILE

Description: FortiSIEM module error - unable to open proc stat file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
procName	Process Name	string	

EventType: PH_BASE_PROC_THREAD_SPAWN_FAILED

Description: FortiSIEM module error - failed to spawn thread

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_THREAD_WRONG_PARAM

Description: FortiSIEM module error - wrong paremeters to thread span function

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_UPLOAD_FILE_FAILURE

Description: FortiSIEM module error - file upload failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_BASE_PROC_VALUE_GROUP_UPDATE_FAILURE

Description: FortiSIEM module error - value group update failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PRO_AQUIRE_SHARED_STORE_FAILED

Description: Unable to aquire shared store instance

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLIHOUSE_BUILD_QUERY_DIST_SQL_COMMAND_FAILURE

Description: Failed to build query dist sql command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLI_ERROR

Description: FortiSIEM CLI error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_CREATE_TEMP_FILE_FAILURE

Description: FortiSIEM temp file creation error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DISC_DATA_PROCESS_ERROR

Description: Discovery result process error

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DIVIDE_BY_ZERO

Description: Devide by zero

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_FAILED_TO_EXEC

Description: Failed to execute specified command

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_FILE_NOT_FOUND

Description: Can not find the specified file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GCS_BUCKET_ACCESS_FAILURE

Description: Failed to access GCS Bucket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GENERIC_CRITICAL

Description: PH system generic critical message

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_GENERIC_DEBUG

Description: PH system generic debug message

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_GENERIC_ERROR

Description: PH system generic error

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GENERIC_INFO

Description: PH system generic info

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_GENERIC_WARNING

Description: PH system generic warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GET_CURL_HANDLE_FAILED

Description: FortiSIEM HTTP Client failed to get handle

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GET_SUPER_LEADER_FAILURE

Description: Failed to get super leader IP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GRP_C_CERT_CREATE_SUCCESS

Description: Create gRPC certificate files

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_GRPC_CERT_ERROR

Description: 700-Grpc: Grpc cert error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_GRPC_CERT_LOADED_FAILED

Description: Failed to load certs file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_GRPC_CERT_UPDATE_FAILED

Description: Failed to update gRPC certificate file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_GRPC_CERT_UPDATE_SUCCESS

Description: Updated gRPC certificate file

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_GRPCTFORMAT_JSON_FAILED

Description: Failed to format Json response

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GRPCTINIT_SSL_CONTEXT

Description: Failed to initial ACE_SSL_Context

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_GRPCTTASK_DATA_EMPTY

Description: GRPC task is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_COMPRESS_FAILED

Description: FortiSIEM HTTP Client failed to compress payload

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_HTTP_CLIENT_CURL_ERROR

Description: FortiSIEM HTTP Client failed with curl error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event

EventType: PH_HTTP_CLIENT_GET_CACHE_FROM_MONITOR_FAILED

Description: FortiSIEM HTTP Client failed to get cache

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_HTTP_CLIENT_GET_DATA_FROM_CACHE_FAILED

Description: FortiSIEM HTTP Client failed to get data from cache

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_HTTP_CLIENT_GET_INIT_RESPONSE_FAILED

Description: FortiSIEM HTTP Client failed to get initialization response

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_HTTP_CLIENT_GET_INIT_RESPONSE_WARNING

Description: FortiSIEM HTTP Client encountered error getting initialization response

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_HTTP_CLIENT_GET_RESPONSE_WARNING

Description: FortiSIEM HTTP Client encountered error getting response

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event

EventType: PH_HTTP_CLIENT_HOST_IS_NULL

Description: FortiSIEM HTTP Client host is null error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_INIT_FAILURE

Description: FortiSIEM HTTP Client initialization failure

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_HTTP_CLIENT_INIT_WARNING

Description: FortiSIEM HTTP Client initialization warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_INVALID_FILE_SIZE

Description: FortiSIEM HTTP Client encountered invalid file size

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_MKSTEMP_FAILED

Description: FortiSIEM HTTP Client failed to mkstemp

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_HTTP_CLIENT_NO_FILE_PARAM

Description: FortiSIEM HTTP Client missing file paarameter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_PICK_SUPER_FAILED

Description: FortiSIEM HTTP Client failed to pick super

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_PREP_REQUEST_ERROR

Description: FortiSIEM HTTP Client Prep Request error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_HTTP_CLIENT_PUT_REDIRECT_FAILURE

Description: FortiSIEM HTTP Client PUT Redirect error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_HTTP_CLIENT_SETOPT_FAILED

Description: FortiSIEM HTTP Client setopt call failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_HTTP_CLIENT_SET_HOST_WARNING

Description: FortiSIEM HTTP Client set host call failed

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_UPLOAD_FILE_FAILED

Description: FortiSIEM HTTP Client file upload failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
infoURL	Informational URL	string	This field captures an URL if present in an event
httpStatusCode	HTTP Status	string	
errorNoInt	Error Number Int	int32	

EventType: PH_HTTP_CLIENT_WRITE_CACHE_NULL

Description: FortiSIEM HTTP Client cache write error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_INIT_FAILURE

Description: Http client initialization failure

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_RESPONSE_FAILURE

Description: HTTP response code failure

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_INCIDENT_ACTION_STATUS

Description: Record action result for incident notification

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
scriptOutput	Script Output	string	

EventType: PH_INVALID_IP_ADDR

Description: FortiSIEM backend module detected invalid IP address

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_INVALID_PARAM

Description: Invaoid Parameter

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
paraName	Param Name	string	

EventType: PH_INVALID_PARAM_CNT

Description: Invaoid number of parameter

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_INVALID_PARAM_VAL_EMPTY

Description: Invalid empty parameter value

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
paraName	Param Name	string	

EventType: PH_LOAD_CONFIG_CHANGE_FAILED

Description: FortiSIEM Rule/Report Master/Worker modules failed to load performance monitoring config change

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
item	Item	string	

EventType: PH_LOOKUP_TABLE_CANNOT_LOAD_DATA

Description: Failed to load data from Nodejs/Redis

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MODULE_ABORT

Description: Module exited abnormally

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
coreDumpFile	Coredump File Name	string	

EventType: PH_MODULE_ABORT_FOUND

Description: Module found aborted

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	
eventTime	Event Occur Time	Date	

EventType: PH_MODULE_ACCEPTED_CONN

Description: Module accepted connection

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_MODULE_ACE_ACCEPTOR_FAILED

Description: ACE failed to accept

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MODULE_ACE_HANDLE_EVENT_ERROR

Description: ACE failed to handle event

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MODULE_COMM_ERROR

Description: Module encountered inter-module communication error

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MODULE_COMM_HANDLER_REG

Description: Module registering notification handlers

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
notifId	Notification ID	uint32	
handlerName	Notification Handler Name	string	

EventType: PH_MODULE_COMM_PORTS_OPENED

Description: Module opened Notification Service ports

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event

EventType: PH_MODULE_DB_CONFIG_LOADED

Description: Module loaded database config successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_DIODE_CONFIG_ERROR

Description: Module failed to load diode collector config

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MODULE_EXCEPTION_NOT_CAUGHT

Description: Exception not caught

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MODULE_EXITING

Description: Module exiting

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_EXIT_OK

Description: Module exited gracefully

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_HEARTBEAT_INIT

Description: Module initializing heartbeat object

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_INITIALIZING

Description: Module initialization

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_INIT_COMPLETE

Description: Module successfully started

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_INIT_FAILURE

Description: Module initialization failure

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	

EventType: PH_MODULE_LOADED_NEW_CONFIG

Description: Module successfully loaded new config

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_LOAD_DIODE_CRED_ERROR

Description: Failed to load diode collector agent credential

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MODULE_LOCAL_CONFIG_LOADED

Description: Module loaded local config successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configName	Config Name	string	

EventType: PH_MODULE_LOCAL_CONFIG_SECTION_ERROR

Description: Module failed to load local config section

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configSectName	Config Section Name	string	

EventType: PH_MODULE_LOCAL_CONFIG_VALUE_ERROR

Description: Module failed to load local config value

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configName	Config Name	string	
configValue	Config Value	string	

EventType: PH_MODULE_LOG_LEVEL_CHANGE

Description: Module received log level change

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
oldLogLevel	Old Log Level	uint32	
newLogLevel	New Log Level	uint32	

EventType: PH_MODULE_RECVD_EXIT_EXT

Description: Module received external signal to exit

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_MODULE_RECVD_EXIT_MONITOR

Description: Module received exit request from Monitor

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_RECVD_NEW_CONFIG

Description: Module received config change notification

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_RECVD_START

Description: Module received start request

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_SETPIDFILE_ERR

Description: Module unable to set PID file

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_MODULE_UNABLE_INIT_SHARED_STORE

Description: Module unable to init shared store

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MODULE_UNABLE_OPEN_COMM_PORT

Description: Module unable to open inter-module comm port during initialization

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event

EventType: PH_NOTIFICATION_ACCEPT_FAILURE

Description: failed to accept connection

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NOTIFICATION_CALLBACK_ERROR

Description: FortiSIEM Notification module callback error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NOTIFICATION_CONN_FAILED

Description: FortiSIEM Notification module failed connection

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	
ipPort	IP Port	uint16	IP port number
module	Module Name	string	

EventType: PH_NOTIFICATION_INIT_FAILED

Description: FortiSIEM Notification module initialization failed

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_NOTIFICATION_NO_RESPONSE

Description: has no response on Notification

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NOTIFICATION_RETURN_FAILURE

Description: Notification returns failure

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NOTIFICATION_SEND_FAILURE

Description: FortiSIEM Notification module send failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NOTIFICATION_SEND_FILE_FAILURE

Description: FortiSIEM Notification module file send failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_OBJECT_NOT_FOUND

Description: Can not find specified object

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_PDF_BUILDER_ERROR

Description: PDF builder error

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_READER_BLOCK_WRITE

Description: Reader is blocking writer&Restart

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	

EventType: PH_Rule_AbuseCH_Botnetc2_MalwareIP_Inbound

Description: Permitted Traffic from AbuseCH Botnet C2 Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_AbuseCH_Botnetc2_MalwareIP_Outbound

Description: Traffic to AbuseCH Botnet C2 Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Blocklist_MalwareIP_Inbound

Description: Permitted Traffic from Blocklist DE Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Blocklist_MalwareIP_Outbound

Description: Traffic to Blocklist DE Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_C2_Tracker_MalwareIP_Inbound

Description: Permitted Traffic from C2 Tracker Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_C2_Tracker_MalwareIP_Outbound

Description: Traffic to C2 Tracker Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_CINSScore_MalwareIP_Inbound

Description: Permitted Traffic from CINS Score Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_CINSScore_MalwareIP_Outbound

Description: Traffic to CINS Score Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_CertPL_MalwareDomain_Inbound

Description: Permitted Traffic from CertPL Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_CertPL_MalwareDomain_Outbound

Description: Traffic to CertPL Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Cisco_Talos_MalwareIP_Inbound

Description: Permitted Traffic from Cisco Talos Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Cisco_Talos_MalwareIP_Outbound

Description: Traffic to Cisco Talos Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Cluster_DBLLeader_Changed

Description: FortiSIEM DB Leader Changed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_Rule_Cluster_REPL_Leader_Changed

Description: FortiSIEM Replication Leader Changed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_Rule_DigitalSide_MalwareDomain_Inbound

Description: Permitted Traffic from DigitalSide Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_DigitalSide_MalwareDomain_Outbound

Description: Traffic to DigitalSide Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_DigitalSide_MalwareIP_Inbound

Description: Permitted Traffic from DigitalSide Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_DigitalSide_MalwareIP_Outbound

Description: Traffic to DigitalSide Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_DigitalSide_MalwareURL_Outbound

Description: Traffic to DigitalSide Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FML_Antispam_Malicious_File

Description: FortiMail: Malicious Spam File Attachment Found

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FML_Antispam_Malicious_Url

Description: FortiMail: Antispam Malicious URL found

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FireHol_MalwareIP_Inbound

Description: Permitted Traffic from FireHol Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FireHol_MalwareIP_Outbound

Description: Traffic to FireHol Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiRecon_MalwareDomain_Inbound

Description: Permitted Traffic from FortiRecon Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiRecon_MalwareDomain_Outbound

Description: Traffic to FortiRecon Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiRecon_MalwareIP_Inbound

Description: Permitted Traffic from FortiRecon Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiRecon_MalwareIP_Outbound

Description: Traffic to FortiRecon Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiRecon_MalwareURL_Outbound

Description: Traffic to FortiRecon Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiSOAR_MalwareDomain_Inbound

Description: Permitted Traffic from FortiSOAR Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiSOAR_MalwareDomain_Outbound

Description: Traffic to FortiSOAR Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiSOAR_MalwareIP_Inbound

Description: Permitted Traffic from FortiSOAR Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiSOAR_MalwareIP_Outbound

Description: Traffic to FortiSOAR Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiSOAR_MalwareURL_Outbound

Description: Traffic to FortiSOAR Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Greensnow_MalwareIP_Inbound

Description: Permitted Traffic from Greensnow Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Greensnow_MalwareIP_Outbound

Description: Traffic to Greensnow Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_IPSum_MalwareIP_Inbound

Description: Permitted Traffic from IPSum Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_IPSum_MalwareIP_Outbound

Description: Traffic to IPSum Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_MISP_MalwareDomain_Inbound

Description: Permitted Traffic from MISP Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_MISP_MalwareDomain_Outbound

Description: Traffic to MISP Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_MISP_MalwareIP_Inbound

Description: Permitted Traffic from MISP Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_MISP_MalwareIP_Outbound

Description: Traffic to MISP Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_MISP_MalwareURL_Outbound

Description: Traffic to MISP Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Mandiant_MalwareDomain_Inbound

Description: Permitted Traffic from Mandiant Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Mandiant_MalwareDomain_Outbound

Description: Traffic to Mandiant Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Mandiant_MalwareIP_Inbound

Description: Permitted Traffic from Mandiant Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Mandiant_MalwareIP_Outbound

Description: Traffic to Mandiant Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Mandiant_MalwareURL_Outbound

Description: Traffic to Mandiant Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_OPENCTI_MalDomain_Inbound

Description: Permitted Traffic from OpenCTI Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_OPENCTI_MalDomain_Outbound

Description: Traffic to OpenCTI Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_OPENCTI_MalwareIP_Inbound

Description: Permitted Traffic from OpenCTI Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_OPENCTI_MalwareIP_Outbound

Description: Traffic to OpenCTI Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_OPENCTI_MalwareURL_Outbound

Description: Traffic to OpenCTI Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_OpenPhish_MalwareURL_Outbound

Description: Traffic to OpenPhish Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Proofpoint_MalwareIP_Inbound

Description: Permitted Traffic from Proofpoint Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Proofpoint_MalwareIP_Outbound

Description: Traffic to Proofpoint Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Snort_MalwareIP_Inbound

Description: Permitted Traffic from Snort Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Snort_MalwareIP_Outbound

Description: Traffic to Snort Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_ThreatFox_MalwareURL_Outbound

Description: Traffic to ThreatFox Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_TweetFeed_MalwareDomain_Inbound

Description: Permitted Traffic from TweetFeed Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_TweetFeed_MalwareDomain_Outbound

Description: Traffic to TweetFeed Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_TweetFeed_MalwareURL_Outbound

Description: Traffic to TweetFeed Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Tweetfeed_MalwareIP_Inbound

Description: Permitted Traffic from TweetFeed Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Tweetfeed_MalwareIP_Outbound

Description: Traffic to TweetFeed Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_SAAS_OP_COLLECTOR_DOWN

Description: Collector down

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SAAS_OP_COLLECTOR_UP

Description: Collector up

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SER_MON_SERVICE_DOWN

Description: PH process down

Severity: 8 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SHAREDSTORE_ACQUIRE_ERROR

Description: A module failed to acquire shared store. The module will abort

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_SHAREDSTORE_WRITER_POS_UNEXPECTED_ALTERED

Description: Shared store writer position altered unexpectedly

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_SHAREDSTORE_WRITE_ERROR

Description: Parser module encountered error while writing to shared store. Events will be lost

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_SSL_SHUTDOWN_ERROR

Description: PH system ssl shutdown error

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DROP_UNKNOWN_ORG

Description: Dropped events which belong to unknown organization

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_RAW_EVENT_SIZE

Description: Total event size in the last fifteen minutes

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phRecvTime	Event Receive Time	Date	This is the timestamp the collector records, when an event is ingested. This is converted and stored as epoch milliseconds. FortiSIEM uses this time in all its analytics. This time is obtained from NTP.
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_SYSTEM_STORAGE_LOW

Description: System data storage is low

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
diskName	Disk Name	string	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	

EventType: PH_SYS_ERROR_XML_SEND_ERROR

Description: Error in sending system error to app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYS_ERROR_XML_SENT

Description: System error sent to app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_TASK_DATA_EMPTY

Description: Task data is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_TASK_DATA_IS_WRONG

Description: Task data is wrong

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_TASK_FAILED

Description: Task Failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_TASK_NOT_CONTAIN_LIC

Description: Task data doesn't contain license data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_TASK_RUN_COMMAND_FAILED

Description: Failed to run command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_TASK_SEND_FAILED

Description: Failed to send task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
procName	Process Name	string	

EventType: PH_TASK_UNSupport

Description: Unsupport this task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_THREAD_EXITING

Description: Module exiting thread

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
threadName	Thread Name	string	

EventType: PH_THREAD_RECVD_EXIT

Description: Thread received exit request

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
threadName	Thread Name	string	

EventType: PH_THREAD_STARTING

Description: Module starting thread

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
threadName	Thread Name	string	

EventType: PH_UNABLE_ACCESS_DIR

Description: Unable to access archive directory

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_UNABLE_ALLOC_MEMORY

Description: Unable to allocate memory

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UNABLE_CREATE_DIR

Description: Unable to create dir

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_UNABLE_CREATE_FILE

Description: Unable to create file

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_UNABLE_CREATE_TIMER

Description: Unable to create timer

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UNABLE_OPEN_DIR

Description: Unable to open dir

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_UNABLE_OPEN_FILE

Description: Unable to open file

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_UNABLE_PARSE_XML

Description: Unable to parse xml

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_UNABLE_RENAME_FILE

Description: Unable to rename file

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_UNRESOLVABLE_HOSTNAME

Description: FortiSIEM module failed to resolve host name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_UNRESOLVABLE_IP

Description: FortiSIEM module failed to resolve ip to get host name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_UTIL_BIZ_CHANGE_UPDATE_SPAWN_FAILURE

Description: phMonitor encountered error in spawning thread

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_UTIL_BIZ_HTTP_REQUEST_FAILURE

Description: HTTP Request Error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_CMD_FAILURE

Description: FortiSIEM system command execution failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_CONFIG_IP_MISSING

Description: Found empty IP address

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_CONFIG_LOAD_FAILURE

Description: Failed to load configuration type from the app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
objType	Object Type	string	

EventType: PH_UTIL_CONFIG_LOAD_FILE_ACESS_FAILURE

Description: Failed to load configuration type from the app server - tmp file not accessible

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
objType	Object Type	string	

EventType: PH_UTIL_CONFIG_PARSE_FAILURE

Description: Failed to parse system/phoenixServer.xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_UTIL_CONFIG_UNKNOWN_SERVER_TYPE

Description: Found unknown server type in App server returned XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
objType	Object Type	string	

EventType: PH_UTIL_CONNECTION_ERROR

Description: Failed to initialize connection

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_UTIL_CSV_LINE_ILLEGAL

Description: Found illegal line in csv file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
lineContent	Line Content	string	

EventType: PH_UTIL_CSV_READ_FAILURE

Description: Failed to open CSV file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_CUSTOMER_COLLECTOR_MISSING

Description: Failed to parse collectors and no collector found

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_CUSTOMER_COLLECTOR_PARSE_FAILURE

Description: Failed to parsephCustomerDevice Collector info

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_CUSTOMER_DOMAIN_MISSING

Description: No domain item found in xml file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_CUSTOMER_INFO_PARSE_FAILURE

Description: Failed to parse value group xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_UTIL_CUSTOMER_PARSE_FAILURE

Description: Failed to parse phCustomerDevice Customer info in XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_DASHBOARD_DUPLICATE_IP

Description: Encountered duplicate ip in device info for same customer Id

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_UTIL_DASHBOARD_DUPLICATE_ITEM

Description: Encountered duplicate item id in device info for same custId

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
item	Item	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_UTIL_DASHBOARD_PARSE_FAILURE

Description: Failed to parse dashboard device info xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_UTIL_DEVICE_MAP_PROP_ERROR

Description: Encountered device map property error in XML

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_DEVICE_PROP_ERROR

Description: Encountered device property error in XML

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_DEVICE_SIMPLE_PROP_PARSE_FAILURE

Description: Failed to parse NULL element for property in XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propName	Property Name	string	

EventType: PH_UTIL_DGA_FREQ_FILE_OPEN_FAILURE

Description: Failed to open DGA freq file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_UTIL_DGA_WHITELIST_FILE_OPEN_FAILURE

Description: Failed to open DGA white list file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_UTIL_DIR_CREATE_FAILURE

Description: Failed to create directory after a few attempts

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_DIR_CREATE_RETRIED

Description: Retried to created dir

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_UTIL_DIR_OPEN_FAILURE

Description: Failed to open directory after a few attempts

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_DIR_PARENT_NOT_EXIST

Description: Failed to locate Parent directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_UTIL_DIR_REMOVE_FAILURE

Description: Failed to remove directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_DISK_USAGE_INFO_GET_FAILURE

Description: Unable to get disk usage information

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_UTIL_DISPATH_CMD_XML_ILLEGAL

Description: Encountered malformed XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_UTIL_DISPATH_CMD_XML_PARSE_FAILURE

Description: Encountered XML parsing failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_UTIL_EMAIL_SEND_FAILURE

Description: Failed to send email to server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_UTIL_ETCD_COMPAGN_FAILED

Description: etcd.compaighn has error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_ETCD_GET_LEADER_FAILED

Description: Failed to get super leader

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_ETCD_LEASE_FAILED

Description: etcd.leasekeepalive has error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_ETCD_SET_FAILED

Description: etcd.set has error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_EVENT_FILE_ERROR

Description: Encountered Event file error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_EVENT_GROUP_ERROR

Description: Encountered Event Group error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_EVENT_STATUS_REPORTER_SPAWN_FAILURE

Description: Failed to initialize external event status reporter thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_EVENT_STATUS_UPLOAD_FAILURE

Description: Failed to upload external event status xml after 3 retries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_EVENT_TYPE_ERROR

Description: Encountered Event type error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_FILE_NOT_EXIST

Description: File doesn't exist

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_UTIL_FILE_OPEN_FAILURE

Description: Failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_FILE_READ_FAILURE

Description: Error reading file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_FILE_SIZE_MISMATCH

Description: File size mismatch

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_FILE_SIZE_TOO_SMALL

Description: File size too small

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
fileSize64	File Size64 Bytes	uint64	

EventType: PH_UTIL_FILE_STATFS_FAILURE

Description: Failed to run statfs() command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_FILE_STAT_FAILURE**Description:** Failed to stat file**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_FILE_WRITE_FAILURE**Description:** Error writing file**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_FORK_FAILURE**Description:** System fork failed - likely system highly utilized**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_GET_ADDR_FAILURE

Description: Failed to run Getaddrinfo command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_UTIL_GET_ATTR_NAME_FAILED

Description: Failed to get attribute

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
details	Details	string	

EventType: PH_UTIL_GET_JOB_STATUS_FAILURE

Description: Failed to get job status to status file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
paraName	Param Name	string	

EventType: PH_UTIL_HOSTNAME_GET_FAILURE**Description:** Failed to look up Host name**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_INET_PTON_FAILURE**Description:** Failed to run inet_ntop command**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_INODE_INFO_GET_FAILURE**Description:** Unable to get inode information**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	

EventType: PH_UTIL_INVALID_PARAM**Description:** Invalide parameter**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
details	Details	string	

EventType: PH_UTIL_IOCTL_FAILURE**Description:** Failed to run ioctl commands**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_IOCTL_SIOCGIFADDR_FAILURE**Description:** Failed to run ioctl SIOCGIFADDR command**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_IP_TYPE_MISMATCH

Description: Mismatch IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_JOB_STATUS_REPORTER_SPAWN_FAILURE

Description: Failed to initialize job status reporter thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_JOB_STATUS_UPLOAD_FAILURE

Description: Failed to upload job status xml after 3 retries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_JSON_GET_NODE_FAILURE

Description: Failed to get JSON node value from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
jsonBody	JSON Body	string	

EventType: PH_UTIL_JSON_GET_TOTAL_COUNT_FAILURE**Description:** Failed to fetch total_count**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_JSON_OBJ_EMPTY**Description:** JSON object empty**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**EventType: PH_UTIL_JSON_PARSE_FAILURE****Description:** Failed to parse JSON**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
jsonBody	JSON Body	string	

EventType: PH_UTIL_KILLPG_FAILURE

Description: Failed to send SIGKILL to child process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_LOAD_EXT_FUNC_FILE_OPEN_FAILURE

Description: Dynamic loaded function load failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_LOAD_EXT_FUNC_FORMAT_INVALID

Description: Dynamic loaded function name should be fileName.functionName format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propValue	Property Value	string	

EventType: PH_UTIL_LOAD_EXT_FUNC_GET_NAME_FAILUE

Description: Dynamic loaded function in file failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_LOCAL_IP_MISSING

Description: Failed to get ip address of this machine

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_LOOKUP_TABLES_DUPLICATE

Description: Duplicate lookup table found

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbTable	Database Table	string	

EventType: PH_UTIL_LOOKUP_TABLES_DUPLICATE_COLUMN

Description: Duplicate lookup table column found

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbTable	Database Table	string	
dbColumn	Database Column	string	

EventType: PH_UTIL_LOOKUP_TABLES_DUPLICATE_KEY

Description: Duplicate lookup table key found

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbTable	Database Table	string	
dbId	DB ID	uint32	

EventType: PH_UTIL_MAIL_CMD_RUN_FAILURE

Description: Failed to send email to server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_UTIL_MAIL_SMTP_INIT_FAILURE

Description: Fail to initialize SMTP server problem

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_MD5_ERROR

Description: Failed to calculate MD5

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_MEM_ALLOC_FAILURE

Description: Could not allocate memory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileSize64	File Size64 Bytes	uint64	

EventType: PH_UTIL_MKDTEMP_FAILURE

Description: Failed to create directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
filePath	File Path	string	

EventType: PH_UTIL_MKSTEMP_FAILURE

Description: Failed to create temporary filename

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
filePath	File Path	string	

EventType: PH_UTIL_MMAP_FAILURE

Description: Failed to mmap file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
fileSize64	File Size64 Bytes	uint64	
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_MOVE_FILE_FAILURE

Description: Failed to rename file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_NOTIFICATION_SENDER_SPAWN_FAILURE

Description: Failed to initialize notification sender thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_NOTIFICATION_SERVER_INIT_FAILURE

Description: Failed to initialize notification reporter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_NOTIFICATION_UPLOAD_FAILURE

Description: Failed to Send Notification

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

EventType: PH_UTIL_PCRE_COMPILE_FAILED

Description: pcre_compile regex error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_PHOENIX_CONFIG_ITEM_MISSING

Description: Could not find specific item in phoenix_config.txt

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propName	Property Name	string	

EventType: PH_UTIL_PIPE_FAILURE

Description: The command pipe() returned error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_PROP_DEF_SET_PARSE_FAILURE

Description: Failed to parse propertyDefs xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_UTIL_REDIS_CONNECTION_ERROR

Description: redis connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_REGEX_PATTERN_EMPTY

Description: Regex Pattern is NULL

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_REGEX_PATTERN_TOO_LONG

Description: Regex Pattern too long

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msgLen	Message Length	uint64	

EventType: PH_UTIL_SEND_DATA_FAILED

Description: Failed to sent data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_UTIL_SEND_TO_UDP_PORT_FAILURE

Description: Failed to send message to udp port

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_UTIL_SETPGRP_FAILURE

Description: Failed to run system comand setpgrp()

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_SET_JOB_STATUS_FAILURE

Description: Failed to set job status to status file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
paraName	Param Name	string	

EventType: PH_UTIL_SOCKET_FAILURE

Description: Failed to run system command socket()

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_STR_TO_IP_FAILURE

Description: Failed to run system call inet_pton

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propValue	Property Value	string	

EventType: PH_UTIL_SVN_DIFF_FAILURE

Description: Failed to execute system command svn diff

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_SYS_ERROR_REPORTER_INIT_FAILURE

Description: Failed to initialize system error reporter thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_TIME_RANGE_INVALID

Description: Found Invalid time range

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propValue	Property Value	string	

EventType: PH_UTIL_TIME_STR_FORMAT_INVALID

Description: Found incorrect time string parameters

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
paraName	Param Name	string	

EventType: PH_UTIL_TLS_SERVER_RECV_FAILED

Description: Tls server failed to receive data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_UNKNOWN_PHOENIX_ERROR_NUMBER

Description: Found incorrect PH error number

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_UTIL_VALUE_GROUP_ERROR

Description: Encountered Value group error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_WAITPID_FAILURE

Description: Failed to run system command waitpid on child process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_WAITPID_LAST_TRY_FAILUE

Description: Failed to run system command waitpid on child process after several tries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_WINDOWS_BID_LOAD_FAILURE

Description: Failed to load Windows Built In SID file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_UTIL_WRITE_BIN_FILE_OPEN_FAILURE

Description: Failed to open binary file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_UTIL_WRITE_FILE_OPEN_FAILURE

Description: Failed to open file for write

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_XML_HANDLING_ERROR

Description: Found Invalid xml from App Server

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_ZIP_DECOMPRESS_FAILED

Description: Failed to decompress zip string

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_WORKER_DOWN

Description: Worker down

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_WORKER_PROVISION_FAILED

Description: Phoenix worker provision failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_WORKER_UP

Description: Worker up

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_WS_COMM_ERROR

Description: Web service communication error

Severity: 6 (Medium)

Event Category: 3 (System Logs)

All Logs Page 1

Every FortiSIEM internally generated event log regardless of category

- JDBC_PULL_UNSUPP_DEV
- JMX_JDBC_PULL_STAT
- MSSQL_JDBC_PULL_STAT
- MYSQL_JDBC_PULL_STAT
- ORADB_JDBC_PULL_STAT
- PH_AGENTMGR_ACI_ATTR_NOT_FOUND
- PH_AGENTMGR_ACI_CURL_HANDLE_GET_FAILED
- PH_AGENTMGR_ACI_FILE_WRITE_ERROR
- PH_AGENTMGR_ACI_JSON_PARSE_FAILED
- PH_AGENTMGR_ACI_SERVER_EMPTY
- PH_AGENTMGR_ACI_TOKEN_GET_FAILED
- PH_AGENTMGR_ALERTLOGIC_CURL_HANDLE_GET_FAILED
- PH_AGENTMGR_ALERTLOGIC_FILE_LOAD_ERROR
- PH_AGENTMGR_ALERTLOGIC_FILE_READ_ERROR
- PH_AGENTMGR_ALERTLOGIC_FILE_WRITE_ERROR
- PH_AGENTMGR_ALERTLOGIC_INVALID_DATA
- PH_AGENTMGR_ALERTLOGIC_INVALID_PATH
- PH_AGENTMGR_ALERTLOGIC_QUERY_INTERVAL_TOO_LONG
- PH_AGENTMGR_ALERTLOGIC_SERVER_EMPTY
- PH_AGENTMGR_AMPCLOUD_CURL_CONNECT_FAILED
- PH_AGENTMGR_AMPCLOUD_CURL_HANDLE_GET_FAILED
- PH_AGENTMGR_AMPCLOUD_FILE_LOAD_ERROR
- PH_AGENTMGR_AMPCLOUD_FILE_READ_ERROR
- PH_AGENTMGR_AMPCLOUD_INVALID_DATA
- PH_AGENTMGR_AMPCLOUD_JSON_PARSE_FAILED
- PH_AGENTMGR_AMPCLOUD_NO_DEFINE_SEVERITY
- PH_AGENTMGR_AMPCLOUD_SERVER_EMPTY
- PH_AGENTMGR_API_PERMISSION_MISSING
- PH_AGENTMGR_AWSCLOUDWATCH_GETLOGS
- PH_AGENTMGR_AWSFLOWLOG_EVENT_PULL_FAILED
- PH_AGENTMGR_AWSFLOWLOG_FILE_WRITE_ERROR
- PH_AGENTMGR_AWSFLOWLOG_LOG_FORMAT_WRONG
- PH_AGENTMGR_AWSKINESIS_CONSUMER_START_FAILED
- PH_AGENTMGR_AWS_CACHE_FILE_ERROR
- PH_AGENTMGR_AWS_DELETE_OJECTKEY_FAILED
- PH_AGENTMGR_AWS_DOWNLOAD_OJECT_FAILED
- PH_AGENTMGR_AWS_EVT_DOWNLOAD_FAILED

- PH_AGENTMGR_AWS_EVT_SEND_FAILED
- PH_AGENTMGR_AWS_GET_OJECTKEY_FAILED
- PH_AGENTMGR_AWS_GZ_FILE_OPEN_ERROR
- PH_AGENTMGR_AWS_JSON_PARSE_FAILED
- PH_AGENTMGR_AWS_SQSURL_FORMAT_ERROR
- PH_AGENTMGR_BOX_API_CALL_FAILED
- PH_AGENTMGR_BOX_ATTR_NOT_FOUND
- PH_AGENTMGR_BOX_EVENT_PULL_FAILED
- PH_AGENTMGR_BOX_FILE_ID_EMPTY
- PH_AGENTMGR_BOX_FILE_LIMIT_EXCEED
- PH_AGENTMGR_BOX_FILE_NOT_MONITORED_ERROR
- PH_AGENTMGR_BOX_FILE_PATH_PARSE_FAILED
- PH_AGENTMGR_BOX_FILE_TYPE_WRONG
- PH_AGENTMGR_BOX_FOLDER_TYPE_WRONG
- PH_AGENTMGR_BOX_HTTP_NO_RESPONSE
- PH_AGENTMGR_BOX_JSON_PARSE_FAILED
- PH_AGENTMGR_BOX_RESPONSE_NO_SPECIAL_ATTRIBUTE
- PH_AGENTMGR_BOX_TIME_CONVERT_FAILED
- PH_AGENTMGR_BOX_XML_PARSE_FAILED
- PH_AGENTMGR_CISCOAMP_CONSUMER_START_FAILED
- PH_AGENTMGR_CLOUDPASSAGE_API_CALL_FAILED
- PH_AGENTMGR_CLOUDPASSAGE_FILE_WRITE_ERROR
- PH_AGENTMGR_CLOUDPASSAGE_GET_EVENT_FAILED
- PH_AGENTMGR_CLOUDPASSAGE_JSON_EMPTY
- PH_AGENTMGR_CLOUDPASSAGE_JSON_PARSE_FAILED
- PH_AGENTMGR_CLOUDPASSAGE_TOKEN_EMPTY
- PH_AGENTMGR_CLOUDTRAIL_FILE_READ_FAILED
- PH_AGENTMGR_CONFIG_ERROR
- PH_AGENTMGR_CONFIG_VERSION_SEND_FAILED
- PH_AGENTMGR_CONFIG_WARNING
- PH_AGENTMGR_CREDENTIAL_GET_FAILED
- PH_AGENTMGR_CROWDSTRIKE_GET_DATAFEED_URL_FAILED
- PH_AGENTMGR_CUST_RESULT_UPLOAD_FAILED
- PH_AGENTMGR_DIR_CREATE_FAILED
- PH_AGENTMGR_EVENT_PULL_FAILED
- PH_AGENTMGR_FALCONDATAREP_SCRIPT_FAILED
- PH_AGENTMGR_FILE_PARSE_ERROR
- PH_AGENTMGR_FILE_WRITE_ERROR
- PH_AGENTMGR_FIREAMP_CERT_DOWNLOAD_FAILED
- PH_AGENTMGR_FIREAMP_DATA_FORMAT_SET_FAILED
- PH_AGENTMGR_FIREAMP_EVENT_PULL_FAILED
- PH_AGENTMGR_FIREAMP_EVT_TYPE_LOAD_FAILED
- PH_AGENTMGR_FIREAMP_FILE_LOAD_ERROR

- PH_AGENTMGR_FIREAMP_FILE_OPEN_ERROR
- PH_AGENTMGR_FIREAMP_INVALID_DATA
- PH_AGENTMGR_FIREAMP_NEW_AGENT_FAILED
- PH_AGENTMGR_FIREAMP_NO_ATTR
- PH_AGENTMGR_FIREAMP_NO_PROTOCOL
- PH_AGENTMGR_FORTICASB_GET_SERVICE_ALERT_ERROR
- PH_AGENTMGR_FORTICASB_GET_SERVICE_ERROR
- PH_AGENTMGR_FORTINDR_GET_API_CALL_FAILED
- PH_AGENTMGR_FORTINDR_GET_API_CALL_NEXT_PAGE
- PH_AGENTMGR_FORTINDR_GET_API_CALL_NO_RESULTS
- PH_AGENTMGR_FORTINDR_GET_API_CALL_RESULTS
- PH_AGENTMGR_FORTINDR_GET_BUCKET_KEY
- PH_AGENTMGR_FORTINDR_GET_BUCKET_OBJ
- PH_AGENTMGR_GET_SCAN_RESULTS_FAILED
- PH_AGENTMGR_GITHUB_API_CALL_FAILED
- PH_AGENTMGR_GITHUB_CREDENTIAL_GET_FAILED
- PH_AGENTMGR_GITHUB_EVENT_PULL_FAILED
- PH_AGENTMGR_GITHUB_FILE_OPEN_ERROR
- PH_AGENTMGR_GITHUB_JSON_PARSE_FAILED
- PH_AGENTMGR_GITHUB_TIME_CONVERT_FAILED
- PH_AGENTMGR_GIT_CLONE_REPO_FAILED
- PH_AGENTMGR_GIT_HANDLE_ERR_FILE_FAILED
- PH_AGENTMGR_GIT_PULL_EVT_FAILED
- PH_AGENTMGR_GIT_SAVE_COMMITID_FAILED
- PH_AGENTMGR_GZ_FILE_OPEN_ERROR
- PH_AGENTMGR_INIT_AGENT
- PH_AGENTMGR_INIT_CACHE_FILE_FAILED
- PH_AGENTMGR_INIT_NO_CRED
- PH_AGENTMGR_INVALID_MGR
- PH_AGENTMGR_IPS_AUTH_FAILED
- PH_AGENTMGR_IPS_EVENT_PULL_FAILED
- PH_AGENTMGR_IPS_FILE_OPEN_ERROR
- PH_AGENTMGR_IPS_OBTAIN_SUBSCRIPTION_FAILED
- PH_AGENTMGR_IPS_SET_SSL_FAILED
- PH_AGENTMGR_JAVA_AGENT_PIPE_WRITE_FAILED
- PH_AGENTMGR_JAVA_AGENT_START_FAILED
- PH_AGENTMGR_JAVA_AGENT_TYPE_UNKNOWN
- PH_AGENTMGR_JAVA_AGENT_USER_MISSING
- PH_AGENTMGR_JAVA_AGENT_ZOMBIE
- PH_AGENTMGR_JAVA_CMD_SEND_FAILED
- PH_AGENTMGR_JAVA_FORK_FAILED
- PH_AGENTMGR_JAVA_INCOMPLETE_DEV_INFO
- PH_AGENTMGR_JAVA_NO_DEV_TYPE_FOR_JDBC

- PH_AGENTMGR_JAVA_NO_STATUS_FILE
- PH_AGENTMGR_JAVA_PIPE_FAILED
- PH_AGENTMGR_JAVA_PROCESS_STATE_GET_FAILED
- PH_AGENTMGR_JAVA_SIGKILL_SEND_FAILED
- PH_AGENTMGR_JAVA_UNSUPPORT_DEV_TYPE_FOR_JDBC
- PH_AGENTMGR_JAVA_USER_PWD_GET_FAILED
- PH_AGENTMGR_JSON_PARSE_FAILED
- PH_AGENTMGR_KAFKA_CONSUME_LOG_FAILED
- PH_AGENTMGR_KAFKA_CREATE_CONSUMER
- PH_AGENTMGR_KAFKA_CREATE_CONSUMER_FAILED
- PH_AGENTMGR_KAFKA_CREATE_PRODUCER_FAILED
- PH_AGENTMGR_KAFKA_CREATE_TOPIC_FAILED
- PH_AGENTMGR_KAFKA_ERROR
- PH_AGENTMGR_KAFKA_METADATA_FAILED
- PH_AGENTMGR_KAFKA_PRODUCER_ERROR
- PH_AGENTMGR_KAFKA_PULL_JOB_FAILED
- PH_AGENTMGR_KAFKA_REBALANCE
- PH_AGENTMGR_KAFKA_RELEASE_CONSUMER
- PH_AGENTMGR_KAFKA_START_FAILED
- PH_AGENTMGR_KAFKA_SUBSCRIBE_FAILED
- PH_AGENTMGR_KAFKA_UPDATE_CONFIG_FAILED
- PH_AGENTMGR_KAFKA_UPDATE_ERROR
- PH_AGENTMGR_KILL_PROCESS
- PH_AGENTMGR_MSAZURE_CONFIG_ARM_FAILED
- PH_AGENTMGR_MSAZURE_DOWNLOAD_FAILED
- PH_AGENTMGR_MSAZURE_JSON_EMPTY
- PH_AGENTMGR_MSAZURE_JSON_FILE_NAME_EMPTY
- PH_AGENTMGR_MSAZURE_JSON_FILE_PARSE_FAILED
- PH_AGENTMGR_MSAZURE_JSON_PARSE_FAILED
- PH_AGENTMGR_MSAZURE_LOGIN_FAILED
- PH_AGENTMGR_MSG_QUEUE_ACCESS_FAILED
- PH_AGENTMGR_MSG_RECV_FAILED
- PH_AGENTMGR_OCI_SET_INSTANCE_NAME_FAILED
- PH_AGENTMGR_OFFICE365_API_CALL_FAILED
- PH_AGENTMGR_OFFICE365_EVENT_PULL_FAILED
- PH_AGENTMGR_OFFICE365_FILE_WRITE_ERROR
- PH_AGENTMGR_OFFICE365_GET_SUBSCRIBE_FAILED
- PH_AGENTMGR_OFFICE365_JSON_PARSE_FAILED
- PH_AGENTMGR_OFFICE365_START_SUBSCRIBE_FAILED
- PH_AGENTMGR_OFFICE365_SUBSCRIBE_EMPTY
- PH_AGENTMGR_OFFICE365_SUBSCRIBE_FAILED
- PH_AGENTMGR_OFFICE365_TOKEN_EMPTY
- PH_AGENTMGR_OKTA_EVT_DOWNLOAD_FAILED

- PH_AGENTMGR_OKTA_FILE_WRONG
- PH_AGENTMGR_OKTA_NO_USER_INFO
- PH_AGENTMGR_OKTA_RESULT_UPLOAD_FAILED
- PH_AGENTMGR_OKTA_RESULT_UPLOAD_WARNING
- PH_AGENTMGR_PARSER_UNABLE_CONNECT
- PH_AGENTMGR_PERF_OBJ_PARSE_FAILURE
- PH_AGENTMGR_PROCESS_INIT_FAILED
- PH_AGENTMGR_PULLING_JOB_OUTDATE
- PH_AGENTMGR_REMOVE_FILE_FAILED
- PH_AGENTMGR_REST_API_CALL_FAILED
- PH_AGENTMGR_RSAS_XML_PARSE_FAILED
- PH_AGENTMGR_RUN_CMD_FAILED
- PH_AGENTMGR_RUN_SCRIPT_FAILED
- PH_AGENTMGR_RUN_SCRIPT_WITHOUT_TASK_ID
- PH_AGENTMGR_SALESFORCE_ATTR_NOT_FOUND
- PH_AGENTMGR_SALESFORCE_COLUMN_NOT_FOUND
- PH_AGENTMGR_SALESFORCE_CURL_EXECUTE_FAILED
- PH_AGENTMGR_SALESFORCE_CURL_HANDLE_GET_FAILED
- PH_AGENTMGR_SALESFORCE_FILE_LOAD_ERROR
- PH_AGENTMGR_SALESFORCE_FILE_WRITE_ERROR
- PH_AGENTMGR_SALESFORCE_INVALID_DATA
- PH_AGENTMGR_SALESFORCE_INVALID_LOG_FILE
- PH_AGENTMGR_SALESFORCE_JSON_PARSE_FAILED
- PH_AGENTMGR_SALESFORCE_LOGIN_FAILED
- PH_AGENTMGR_SALESFORCE_SERVER_EMPTY
- PH_AGENTMGR_SALESFORCE_TOKEN_GET_FAILED
- PH_AGENTMGR_SALESFORCE_TOKEN_REGET_FAILED
- PH_AGENTMGR_SALESFORCE_VERSION_PATH_EMPTY
- PH_AGENTMGR_SALESFORCE_XML_PARSE_FAILED
- PH_AGENTMGR_SCRIPT_NOTIFICATION_SPAWN_FAILED
- PH_AGENTMGR_SERVER_HOST_NAME_RESOLVE_FAILED
- PH_AGENTMGR_SERVER_HOST_NAME_RESOLVE_WARNING
- PH_AGENTMGR_SERVER_IP_RESOLVE_FAILED
- PH_AGENTMGR_SERVER_IP_RESOLVE_WARNING
- PH_AGENTMGR_SETUP_STREAM_FAILED
- PH_AGENTMGR_START_THREAD_FAILED
- PH_AGENTMGR_STATUS_REPORT_FAILED
- PH_AGENTMGR_STATUS_REPORT_INIT_FAILED
- PH_AGENTMGR_STOP_STREAM_FAILED
- PH_AGENTMGR_TENABLE_EXPORT_SCAN_FAILED
- PH_AGENTMGR_TENABLE_GET_DOWNLOAD_FAILED
- PH_AGENTMGR_TENABLE_GET_SCANS_FAILED
- PH_AGENTMGR_TENABLE_GET_STATUS_FAILED

- PH_AGENTMGR_TENABLE_PULL_FAILED
- PH_AGENTMGR_TIME_CONVERSION_FAILED
- PH_AGENTMGR_TIME_STR_FORMAT_INVALID
- PH_AGENTMGR_TOKEN_GET_FAILED
- PH_AGENTMGR_UNPACK_FILE_FAILED
- PH_AGENTMGR_UPDATE_AGENT
- PH_AGENTMGR_UPDATE_BOOKMARK_FAILED
- PH_AGENTMGR_UPDATE_WEBHOOK_CRED_FAILED
- PH_AGENTMGR_UPDATE_WEBHOOK_CRED_SUCCESS
- PH_AGENTMGR_WINDEFATP_API_CALL_FAILED
- PH_AGENTMGR_WINDEFATP_FILE_WRITE_ERROR
- PH_AGENTMGR_WINDEFATP_GET_ALERT_FAILED
- PH_AGENTMGR_WINDEFATP_JSON_EMPTY
- PH_AGENTMGR_WINDEFATP_JSON_PARSE_FAILED
- PH_AGENTMGR_WINDEFATP_TOKEN_EMPTY
- PH_AGENTMGR_WMI_EVENT_PULL_ERROR
- PH_AGENTMGR_WMI_EVENT_PULL_WARNING
- PH_AGENTMGR_WMI_FILE_OPEN_ERROR
- PH_AGENTMGR_WMI_LOG_PULL_ERROR
- PH_AGENTMGR_WMI_MISSING_LOG
- PH_AGENTMGR_WMI_STATUS_REPORT_FAILED
- PH_AGENTMGR_WMI_USER_PWD_GET_FAILED
- PH_AGENTMGR_WVSS_XML_PARSE_FAILED
- PH_AGENTMGR_XML_PARSE_FAILED
- PH_ANOMALY_CONFIG
- PH_ANOMALY_LATERAL_MOVEMENT_ANALYZE
- PH_ANOMALY_LATERAL_MOVEMENT_DETECT
- PH_ANOMALY_LATERAL_MOVEMENT_TRAIN
- PH_ANOMALY_SYSTEM
- PH_ANOMALY_TIMER
- PH_APPSERVER_ADMIN_AGENT_GET_UPDATE_FAILED_ERROR
- PH_APPSERVER_ADMIN_AGENT_UNKOWN_TASK_ID_ERROR
- PH_APPSERVER_ADMIN_CUST_GENERATE_KEY_ERROR
- PH_APPSERVER_ADMIN_GET_RESOURCE_FAILED
- PH_APPSERVER_ADMIN_LOCATE_KEY_FAILED
- PH_APPSERVER_ADMIN_RESET_FIELD_FAILED_ERROR
- PH_APPSERVER_AUDIT_REPORT_EXPORT_ERROR
- PH_APPSERVER_BEACON_LIB_ERROR
- PH_APPSERVER_BEACON_REGISTER_ERROR
- PH_APPSERVER_BEACON_SERVER_ERROR
- PH_APPSERVER_BEACON_WEB_SERVER_ERROR
- PH_APPSERVER_BEAN_REF_CHECK_WARN
- PH_APPSERVER_BEAN_SYNC_PROPERTIES_ERROR

- PH_APPSERVER_BEAN_TO_VALUE_ERROR
- PH_APPSERVER_BEAN_TO_XML_ERROR
- PH_APPSERVER_BEAN_VALUE_TO_BEAN_ERROR
- PH_APPSERVER_CMDB_REPORT_DATA_ERROR
- PH_APPSERVER_CMDB_REPORT_EXPORT_ERROR
- PH_APPSERVER_CMDB_REPORT_IMPORT_ERROR
- PH_APPSERVER_CMDB_REPORT_QUERY_ERROR
- PH_APPSERVER_CMDB_REPORT_TYPE_ERROR
- PH_APPSERVER_COLLECTOR_INFO_ERROR
- PH_APPSERVER_COLLECTOR_LICENSE_ERROR
- PH_APPSERVER_COLLECTOR_STATUS_ERROR
- PH_APPSERVER_COMMONPWD_EXPORT_ERROR
- PH_APPSERVER_DASHBOARD_DATA_ERROR
- PH_APPSERVER_DASHBOARD_HTML_BUILD_XML_ERROR
- PH_APPSERVER_DASHBOARD_WIDGET_ERROR
- PH_APPSERVER_DATA_IMPORT_ERROR
- PH_APPSERVER_DATA_ROBUST_INFO_ERROR
- PH_APPSERVER_DB_CONNECTION_CLOSE_ERROR
- PH_APPSERVER_DB_DATA_ERROR
- PH_APPSERVER_DB_DELETE_ERROR
- PH_APPSERVER_DB_QUERY_ERROR
- PH_APPSERVER_DB_UPDATE_ERROR
- PH_APPSERVER_DISCOVERY_CREDENTIAL_DECRYPT_PASSWORD_WARN
- PH_APPSERVER_DISCOVERY_RESULT_ENCRYPT_XML_ELEMENT_ERROR
- PH_APPSERVER_DISCOVERY_RESULT_ERROR
- PH_APPSERVER_DISCOVERY_RESULT_UNKOWN_TASK_ID_ERROR
- PH_APPSERVER_EAMIL_GENERATE_EVENT_ERROR
- PH_APPSERVER_ELASTIC_UPDATE_ERROR
- PH_APPSERVER_EMAIL_PREPARE_DATA_ERROR
- PH_APPSERVER_EVENTDB_EXPORT_ERROR
- PH_APPSERVER_EVENT_ATTRIBUTE_BUILD_XML_ERROR
- PH_APPSERVER_EXPORT_ERROR
- PH_APPSERVER_EXT_THREAT_INTEL_DOWNLOAD_ERROR
- PH_APPSERVER_EXT_THREAT_INTEL_PARSE_ERROR
- PH_APPSERVER_EXT_THREAT_INTEL_UPDATE_ERROR
- PH_APPSERVER_FILE_NOT_FOUND
- PH_APPSERVER_FILE_READ_ERROR
- PH_APPSERVER_FILE_SYSTEM_ERROR
- PH_APPSERVER_FILE_WRITE_ERROR
- PH_APPSERVER_FLEX_INTERCEPTOR_NO_LOGIN_EXCEPTION_ERROR
- PH_APPSERVER_FORTIGUARD_IOC_INTEGRATION_ERROR
- PH_APPSERVER_FRAMEWORK_REGISTER_ERROR
- PH_APPSERVER_FRAMEWORK_RUN_THREAD_ERROR

- PH_APPSERVER_FRAMEWORK_SECURITY_CHECK_LICENSE_WARN
- PH_APPSERVER_FRAMEWORK_SECURITY_GET_ENTITY_MANAGER_ERROR
- PH_APPSERVER_FRAMEWORK_SECURITY_GET_RS_EXPIRATION_ERROR
- PH_APPSERVER_FRAMEWORK_SECURITY_INIT_SYSTEM_ERROR
- PH_APPSERVER_FRAMEWORK_SERVICE_MISSED_WARN
- PH_APPSERVER_FRAMEWORK_SHUTDOWN_SERVICE_STARTER_WARN
- PH_APPSERVER_GENERIC_ERROR
- PH_APPSERVER_GENERIC_INFO
- PH_APPSERVER_GENERIC_WARN
- PH_APPSERVER_GET_MAX_CONFIG_ITEM_COUNT_ERROR
- PH_APPSERVER_GROUP_DATA_ERROR
- PH_APPSERVER_IDENTITYLOCATION_EXPORT_ERROR
- PH_APPSERVER_INCIDENT_NOTIFY_ERROR
- PH_APPSERVER_INCIDENT_UPDATE_ERROR
- PH_APPSERVER_INTEGRATION_ERROR
- PH_APPSERVER_INTEGRATION_UPDATE_POLICY_ERROR
- PH_APPSERVER_INTEGRATION_UPDATE_POLICY_WARN
- PH_APPSERVER_INTEGRATION_WARN
- PH_APPSERVER_IN_INTEGRATION_ERROR
- PH_APPSERVER_IOC_LICENSE_CHECK_FAILED_WARN
- PH_APPSERVER_IOC_TASK_CREATE_FAILED_ERROR
- PH_APPSERVER_JOB_DISTRIBUTE_ERROR
- PH_APPSERVER_LICENSE_EXPIRY_ERROR
- PH_APPSERVER_LICENSE_VALIDATION_ERROR
- PH_APPSERVER_LOGIN_ERROR
- PH_APPSERVER_LOG_INTEGRITY_ERROR
- PH_APPSERVER_MONITOR_AUDIT_PERF_ERROR
- PH_APPSERVER_MONITOR_HEALTH_CONFIG_SET_ERROR
- PH_APPSERVER_NETSEGMENT_EXPORT_ERROR
- PH_APPSERVER_NOTIFICATION_EMAIL_GET_RESOURCE_FAILED
- PH_APPSERVER_NOTIFICATION_ERROR
- PH_APPSERVER_NOTIFICATION_JMS_CONNECTION_ERROR
- PH_APPSERVER_NOTIFICATION_UPDATE_ERROR
- PH_APPSERVER_NOTIFIER_ERROR
- PH_APPSERVER_NO_WATCHLIST_SELECTED_WARN
- PH_APPSERVER_OPENPROXY_EXPORT_ERROR
- PH_APPSERVER_OUT_INTEGRATION_ERROR
- PH_APPSERVER_PARSER_IMPORT_ERROR
- PH_APPSERVER_PARSER_UPDATE_ERROR
- PH_APPSERVER_PARSING_CONSTRAINT_ERROR
- PH_APPSERVER_PDF_BUILDER_ERROR
- PH_APPSERVER_PERFMON_TASK_ERROR
- PH_APPSERVER_QUERY_CHECK_POLICY_ACTION_WARN

- PH_APPSERVER_QUERY_EXPORT_ERROR
- PH_APPSERVER_QUERY_RESULT_PARSER_ERROR
- PH_APPSERVER_QUERY_RESULT_RETRIEVE_ERROR
- PH_APPSERVER_QUERY_RUN_ERROR
- PH_APPSERVER_QUERY_STOP_ERROR
- PH_APPSERVER_QUERY_STRING_ESCAPE_ERROR
- PH_APPSERVER_RBAC_ERROR
- PH_APPSERVER_RBAC_NO_PERMISSION_WARN
- PH_APPSERVER_REALTIME_QUERY_ERROR
- PH_APPSERVER_REMEDY_ERROR
- PH_APPSERVER_REPORT_BUNDLE_PRINT_ERROR
- PH_APPSERVER_REPORT_COMPILE_ERROR
- PH_APPSERVER_REPORT_DEVICE_COMPONENT_SN_ERROR
- PH_APPSERVER_REPORT_DEVICE_DETAIL_ERROR
- PH_APPSERVER_REPORT_DEVICE_SN_ERROR
- PH_APPSERVER_REPORT_DEVICE_SUMMARY_ERROR
- PH_APPSERVER_REPORT_EXPORT_ERROR
- PH_APPSERVER_REPORT_FAILED_BLOCK_SUMMARY_ERROR
- PH_APPSERVER_REPORT_FIRE_TRIGGER_EVENT_ERROR
- PH_APPSERVER_REPORT_GET_PH_CONFIG_ERROR
- PH_APPSERVER_REPORT_IDENTITY_AND_LOCATION_ERROR
- PH_APPSERVER_REPORT_LOG_FILE_SUMMARY_ERROR
- PH_APPSERVER_REPORT_TEMPLATE_GENERATE_PDF_ERROR
- PH_APPSERVER_REPORT_TEMPLATE_INIT_IMAGE_ERROR
- PH_APPSERVER_REPORT_TEMPLATE_INIT_PARM_ERROR
- PH_APPSERVER_REPORT_TEMPLATE_PDF_SUMMARY_ERROR
- PH_APPSERVER_REPORT_TICKET_SUMMARY_ERROR
- PH_APPSERVER_REPORT_UPDATE_ERROR
- PH_APPSERVER_REPORT_USER_SUMMARY_ERROR
- PH_APPSERVER_REST_ERROR
- PH_APPSERVER_REST_H5_ERROR
- PH_APPSERVER_RISKSCORE_CALCULATE_ERROR
- PH_APPSERVER_RULE_ACTIVE_ERROR
- PH_APPSERVER_RULE_CLONE_ERROR
- PH_APPSERVER_RULE_DEBUG_INVALID_EVENT_DB_ID_ERROR
- PH_APPSERVER_RULE_DEBUG_WORKERS_SETTING_ERROR
- PH_APPSERVER_RULE_TEST_ERROR
- PH_APPSERVER_RULE_UPDATE_ERROR
- PH_APPSERVER_SCHEDULE_ERROR
- PH_APPSERVER_SCHEDULE_UPDATE_ERROR
- PH_APPSERVER_SECURITY_ERROR
- PH_APPSERVER_SERVLET_ERROR
- PH_APPSERVER_SERVLET_NO_ACCESS_TO_URI_WARN

- PH_APPSERVER_SOCKET_COMM_ERROR
- PH_APPSERVER_SVN_ERROR
- PH_APPSERVER_SYNC_UPDATE_CONFIG_ERROR
- PH_APPSERVER_SYSCONFIG_GET_ERROR
- PH_APPSERVER_SYSTEM_WINAGENT_REGISTER_WARN
- PH_APPSERVER_SYS_APPLICATION_ERROR
- PH_APPSERVER_SYS_DATA_UPDATE_ERROR
- PH_APPSERVER_TASK_CREATE_ERROR
- PH_APPSERVER_TASK_FLEX_RESULT_BUILD_XML_ERROR
- PH_APPSERVER_TASK_GET_ERROR
- PH_APPSERVER_TASK_UPDATE_ERROR
- PH_APPSERVER_TICKET_EXPORT_ERROR
- PH_APPSERVER_UPDATER_FIND_EXIST_USER_BY_NOHING_ERROR
- PH_APPSERVER_USERAGENT_EXPORT_ERROR
- PH_APPSERVER_VULNERABILITY_IGNORE_WARN
- PH_APPSERVER_WATCHLIST_ADD_TO_DISTIRBUTED_QUEUE
- PH_APPSERVER_WATCHLIST_EXPORT_ERROR
- PH_APPSERVER_WATCHLIST_IMPORT_ERROR
- PH_APPSERVER_WATCHLIST_IMPORT_WARN
- PH_APPSERVER_WATCHLIST_UPDATE_ERROR
- PH_APPSERVER_WEBSERVICE_UPDATE_TASK_ERROR
- PH_APPSERVER_WORKER_PROVISION_FAILED
- PH_APPSERVER_WS_COMM_ERROR
- PH_APPSERVER_XML_PARSE_ERROR
- PH_AUDIT_ACCOUNT_LOCKED
- PH_AUDIT_AGENT_DISABLED
- PH_AUDIT_AGENT_INSTALLED
- PH_AUDIT_AGENT_NOTRESPONDING
- PH_AUDIT_AGENT_RUNNING
- PH_AUDIT_AGENT_STARTED
- PH_AUDIT_AGENT_STOPPED
- PH_AUDIT_AGENT_UNINSTALLED
- PH_AUDIT_CASE_ASSIGNED
- PH_AUDIT_CASE_CLOSED
- PH_AUDIT_CASE_CREATED
- PH_AUDIT_CASE_EVIDENCE_ADDED
- PH_AUDIT_CASE_EVIDENCE_DELETED
- PH_AUDIT_CASE_INCIDENT_ADDED
- PH_AUDIT_CASE_MERGED
- PH_AUDIT_CASE_NOTE_ADDED
- PH_AUDIT_CASE_NOTE_DELETED
- PH_AUDIT_CASE_NOTE_MODIFIED
- PH_AUDIT_CASE_PRIORITY_CHANGED

- PH_AUDIT_CASE_REASSIGNED
- PH_AUDIT_CASE_STAGE_CHANGED
- PH_AUDIT_CASE_STAT
- PH_AUDIT_CASE_STATUS_CHANGED
- PH_AUDIT_CASE_SUMMARY_CHANGED
- PH_AUDIT_CASE_UPDATED
- PH_AUDIT_CI_QUOTE_EXCEEDED
- PH_AUDIT_CMDB_DISK_PRUNE_FAILED
- PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS
- PH_AUDIT_DASHBOARD_SHARED
- PH_AUDIT_DATA_PURGE
- PH_AUDIT_DB_LEADER_CHANGE
- PH_AUDIT_DEFAULT_PWD_MATCH
- PH_AUDIT_DEVICE_ADDED
- PH_AUDIT_DEVICE_DELETED
- PH_AUDIT_DEVICE_DISCOVERY_ITEM_CHANGED
- PH_AUDIT_DEVICE_MAINTENANCE_ENDED
- PH_AUDIT_DEVICE_MAINTENANCE_STARTED
- PH_AUDIT_DEVICE_MERGED_BY_IP_WITH_DIFF_NAME
- PH_AUDIT_DEVICE_STATUS_CHANGED
- PH_AUDIT_DEVICE_UNMANAGED
- PH_AUDIT_DEV_MON_JOB_NOT_STARTED
- PH_AUDIT_DEV_MON_JOB_STATUS_CHANGE
- PH_AUDIT_DISCOVERY
- PH_AUDIT_EXPORT_REPORT_END
- PH_AUDIT_GENAI_USER_QUERY
- PH_AUDIT_GENERIC
- PH_AUDIT_GROUP_CREATED
- PH_AUDIT_GROUP_DELETED
- PH_AUDIT_INACTIVE_USER_LOGIN
- PH_AUDIT_INCIDENT_SYS_CLEAR
- PH_AUDIT_INCIDENT_USER_CLEAR
- PH_AUDIT_INTEGRATION_POLICY_EXECUTED
- PH_AUDIT_MALWARE_DATA_DELETED
- PH_AUDIT_MALWARE_DATA_UPDATED
- PH_AUDIT_ML_GENERIC_ERROR
- PH_AUDIT_ML_GENERIC_INFO
- PH_AUDIT_ML_INFERENCE_COMPLETED
- PH_AUDIT_ML_INFERENCE_RESULT
- PH_AUDIT_ML_INFERENCE_STARTED
- PH_AUDIT_ML_TRAINING_COMPLETED
- PH_AUDIT_ML_TRAINING_STARTED
- PH_AUDIT_NOTIF_POLICY_EXECUTED

- PH_AUDIT_OBJECT_CREATED
- PH_AUDIT_OBJECT_DELETED
- PH_AUDIT_OBJECT_UPDATED
- PH_AUDIT_ONDEMAND_REMEDIATION_EXECUTED
- PH_AUDIT_PASSWORD_CHANGED
- PH_AUDIT_QUERY_COMPLETED
- PH_AUDIT_QUERY_SCHEDULED
- PH_AUDIT_QUERY_START
- PH_AUDIT_QUERY_STOP
- PH_AUDIT_REPL_LEADER_CHANGE
- PH_AUDIT_REPORT_SCHEDULED
- PH_AUDIT_REPORT_SCHEDULE_APPROVE
- PH_AUDIT_REPORT_SCHEDULE_REQUEST
- PH_AUDIT_REPORT_SERVER_LICENSE_EXPIRED
- PH_AUDIT_REPORT_SERVER_LICENSE_REMOVED
- PH_AUDIT_REPORT_SERVER_LICENSE_TO_EXPIRE
- PH_AUDIT_RISK_DECREASE_LOW
- PH_AUDIT_RISK_DECREASE_MED
- PH_AUDIT_RISK_INCREASE_HIGH
- PH_AUDIT_RISK_INCREASE_MED
- PH_AUDIT_RULE_ACTIVATED
- PH_AUDIT_RULE_ACTIVATION_APPROVE
- PH_AUDIT_RULE_ACTIVATION_REQUEST
- PH_AUDIT_RULE_DEACTIVATED
- PH_AUDIT_RULE_DEACTIVATION_APPROVE
- PH_AUDIT_RULE_DEACTIVATION_REQUEST
- PH_AUDIT_SVC_LOGIN_FAILURE
- PH_AUDIT_SVC_LOGIN_SUCCESS
- PH_AUDIT_SVC_LOGOFF
- PH_AUDIT_SVC_SESSION_TIMEOUT
- PH_AUDIT_TUNNEL_CLOSE
- PH_AUDIT_TUNNEL_OPEN
- PH_AUDIT_USER_ADDED
- PH_AUDIT_USER_CHANGE_ORG_SCOPE
- PH_AUDIT_USER_DEFAULT_ROLE_CHANGED
- PH_AUDIT_USER_DELETED
- PH_AUDIT_USER_LOGIN_FAILURE
- PH_AUDIT_USER_LOGIN_SUCCESS
- PH_AUDIT_USER_LOGOFF
- PH_AUDIT_USER_ORGANIZATION_ROLE_CHANGED
- PH_AUDIT_USER_ORGANIZATION_ROLE_ENABLED
- PH_AUDIT_USER_ORGANIZATION_ROLE_REMOVED
- PH_AUDIT_USER_SESSION_TIMEOUT

- PH_AUDIT_WS_COMM
- PH_BAD_NETFLOW_PACKET
- PH_BAD_NETFLOW_VER
- PH_BAD_ROUTE_OUTPUT
- PH_BASE_PROC_BASE_AGENT_JOB_NO_THREAD_NUM_ASSIGNED
- PH_BASE_PROC_DUMP_STACK_TRACE_FAILURE
- PH_BASE_PROC_GET_PID_FILE_FAILED
- PH_BASE_PROC_HANDLE_NOTIFICATION_ERROR
- PH_BASE_PROC_KILL_PROC_ERROR
- PH_BASE_PROC_NOTIFICATION_HANDLE_CONN_ERROR
- PH_BASE_PROC_NO_CONN_TO_HEARTBEAT_SERVER
- PH_BASE_PROC_RENAME_MINI_DUMP_FILE_FAILURE
- PH_BASE_PROC_REST_CACHE_CHECKOUT_STATUS_WARNING
- PH_BASE_PROC_SEND_HEARTBEAT_FAILURE
- PH_BASE_PROC_SEND_USER_DEFINED_SIG_FAILED
- PH_BASE_PROC_SET_PID_FILE_FAILED
- PH_BASE_PROC_STACK_TRACE
- PH_BASE_PROC_STACK_TRACK_TOO_LONG
- PH_BASE_PROC_SYS_INFO_CALC_CPU_ERROR
- PH_BASE_PROC_SYS_PROC_INFO_GET_FAILURE
- PH_BASE_PROC_SYS_PROC_INFO_INIT_ERROR
- PH_BASE_PROC_SYS_PROC_INFO_UNABLE_OPEN_PROC_PID_FILE
- PH_BASE_PROC_SYS_PROC_INFO_UNABLE_OPEN_PROC_STAT_FILE
- PH_BASE_PROC_THREAD_SPAWN_FAILED
- PH_BASE_PROC_THREAD_WRONG_PARAM
- PH_BASE_PROC_UPLOAD_FILE_FAILURE
- PH_BASE_PROC_VALUE_GROUP_UPDATE_FAILURE
- PH_BASE_PRO_AQUIRE_SHARED_STORE_FAILED
- PH_CHECKPOINT_CERTHANDLER_ERROR
- PH_CHECKPOINT_CERTPULL_ERROR
- PH_CHECKPOINT_CMD_USAGE_ERROR
- PH_CHECKPOINT_CPMI_FETCH_ERROR
- PH_CHECKPOINT_DEV_INIT_ERROR
- PH_CHECKPOINT_FILE_RENAME_FAILURE
- PH_CHECKPOINT_FWLOGHANDLER_ERROR
- PH_CHECKPOINT_FWLOGHANDLER_INIT_ERROR
- PH_CHECKPOINT_HTTP_ERROR
- PH_CHECKPOINT_LOGHANDLER_ERROR
- PH_CHECKPOINT_PROCESS_GET_FAILED
- PH_CHECKPOINT_TESTCONN_ERROR
- PH_CHECKPOINT_UNABLE_PARSE_XML
- PH_CLICKHOUSE_CHECKIN_QUERY_THREADS_FAILED
- PH_CLICKHOUSE_CHECKOUT_QUERY_THREADS_FAILED

- [PH_CLICKHOUSE_DISK_UTILS_PER_STORAGE_TIER](#)
- [PH_CLICKHOUSE_DROP_PARTITION_FAILED](#)
- [PH_CLICKHOUSE_DROP_PARTITION_STARTED](#)
- [PH_CLICKHOUSE_DROP_PARTITION_SUCCEEDED](#)

EventType: JDBC_PULL_UNSUPP_DEV

Description: Unsupported device type for JDBC Pull

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: JMX_JDBC_PULL_STAT

Description: JDBC Event pull statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: MSSQL_JDBC_PULL_STAT

Description: JDBC Event pull statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: MYSQL_JDBC_PULL_STAT

Description: JDBC Event pull statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: ORADB_JDBC_PULL_STAT

Description: JDBC Event pull statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ACI_ATTR_NOT_FOUND

Description: Agent Manager Cisco ACI monitoring module cannot find specific attribute

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ACI_CURL_HANDLE_GET_FAILED

Description: Agent Manager Cisco ACI monitoring module unable to get curl handle

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ACI_FILE_WRITE_ERROR

Description: Agent Manager Cisco ACI monitoring module unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_ACI_JSON_PARSE_FAILED

Description: Agent Manager Cisco ACI monitoring module failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ACI_SERVER_EMPTY

Description: Agent Manager Cisco ACI monitoring module found server is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ACI_TOKEN_GET_FAILED

Description: Agent Manager Cisco ACI monitoring module cannot get login token

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ALERTLOGIC_CURL_HANDLE_GET_FAILED

Description: Agent Manager Alert Logic log parsing module unable to get curl handle

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ALERTLOGIC_FILE_LOAD_ERROR

Description: Agent Manager Alert Logic log parsing module failed to load file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_ALERTLOGIC_FILE_READ_ERROR

Description: Agent Manager Alert Logic log parsing module found wrong format in file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_ALERTLOGIC_FILE_WRITE_ERROR

Description: Agent Manager Alert Logic log parsing module unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_ALERTLOGIC_INVALID_DATA

Description: Agent Manager Alert Logic log parsing module found invalid data format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ALERTLOGIC_INVALID_PATH

Description: Agent Manager Alert Logic log parsing module found invalid incident path

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_ALERTLOGIC_QUERY_INTERVAL_TOO_LONG

Description: Agent Manager Alert Logic log parsing module found query interval is larger, it will be narrowed in one week

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_ALERTLOGIC_SERVER_EMPTY

Description: Agent Manager Alert Logic log parsing module found server is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AMPCLOUD_CURL_CONNECT_FAILED

Description: Agent Manager AMP Cloud log parsing module unable to connect server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
httpStatusCode	HTTP Status	string	

EventType: PH_AGENTMGR_AMPCLOUD_CURL_HANDLE_GET_FAILED

Description: Agent Manager AMP Cloud log parsing module unable to get curl handle

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AMPCLOUD_FILE_LOAD_ERROR

Description: Agent Manager AMP Cloud log parsing module failed to load file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_AMPCLOUD_FILE_READ_ERROR

Description: Agent Manager AMP Cloud log parsing module found wrong format in file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_AMPCLOUD_INVALID_DATA

Description: Agent Manager AMP Cloud log parsing module found Invalid data format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AMPCLOUD_JSON_PARSE_FAILED

Description: Agent Manager AMP Cloud log parsing module failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AGENTMGR_AMPCLOUD_NO_DEFINE_SEVERITY

Description: Agent Manager AMP Cloud log parsing module found event severity is not defined

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AMPCLOUD_SERVER_EMPTY

Description: Agent Manager AMP Cloud log parsing module found server is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_API_PERMISSION_MISSING

Description: There is no permission

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_AWSCLOUDWATCH_GETLOGS

Description: Attempting to get cloudwatch logs from log group and stream

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
groupName	Group Name	string	
streamName	AWS Stream Name	string	

Id	Display name	Type	Description
startTime	Start Time	Date	This is the start time of a given item or task, and is stored in epoch milliseconds
endTime	End Time	Date	This is the end time of a given item or task, stored in epoch milliseconds.

EventType: PH_AGENTMGR_AWSFLOWLOG_EVENT_PULL_FAILED

Description: Agent Manager AWS module failed to get AWS Flow log after 5 tries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_AWSFLOWLOG_FILE_WRITE_ERROR

Description: Agent Manager AWS Flow log handling module unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_AWSFLOWLOG_LOG_FORMAT_WRONG

Description: Agent Manager AWS Flow log handling module encountered wrong log format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AWSKINESIS_CONSUMER_START_FAILED

Description: Failed to start Kinesis consumer process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_AWS_CACHE_FILE_ERROR

Description: Agent Manager AWS Cache file is not available

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AWS_DELETE_OJECTKEY_FAILED

Description: Failed to delete object key from SQS

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_AWS_DOWNLOAD_OJECT_FAILED

Description: Failed to download object from bucket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_AWS_EVT_DOWNLOAD_FAILED

Description: Agent Manager AWS module failed to download event by do_system failed

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_AGENTMGR_AWS_EVT_SEND_FAILED

Description: Agent Manager AWS module failed to send cloudtrail event to phParser after 5 tries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AWS_GET_OJBJECTKEY_FAILED

Description: Agent Manager AWS agent failed to get object key from SQS

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_AWS_GZ_FILE_OPEN_ERROR

Description: Agent Manager AWS module gailed to open gz file, or not enough memory to open it

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_AWS_JSON_PARSE_FAILED

Description: Agent Manager AWS module failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_AWS_SQSURL_FORMAT_ERROR

Description: Agent Manager AWS Sqs Url format is wrong

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_API_CALL_FAILED

Description: Agent Manager BOX module failed to call BOX API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_ATTR_NOT_FOUND

Description: Agent Manager BOX module cannot find attribute

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_EVENT_PULL_FAILED

Description: Agent Manager BOX module failed to pull BOX log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
accountName	Account Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_BOX_FILE_ID_EMPTY

Description: Agent Manager BOX module found empty file ID

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_FILE_LIMIT_EXCEED

Description: Agent Manager BOX module found that the number of monitoring file exceeded limit

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_FILE_NOT_MONITORED_ERROR

Description: Agent Manager BOX module found that the file is not monitored before

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_BOX_FILE_PATH_PARSE_FAILED

Description: Agent Manager BOX module could not parse file path

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_BOX_FILE_TYPE_WRONG

Description: Agent Manager BOX module found wrong file type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileType	File Type	string	

EventType: PH_AGENTMGR_BOX_FOLDER_TYPE_WRONG

Description: Agent Manager BOX module found wrong folder type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_HTTP_NO_RESPONSE

Description: Agent Manager BOX module did not find response from App Server Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_AGENTMGR_BOX_JSON_PARSE_FAILED

Description: Agent Manager BOX module failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_RESPONSE_NO_SPECIAL_ATTRIBUTE

Description: Agent Manager BOX module response doesn't have special node

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_BOX_TIME_CONVERT_FAILED

Description: Agent Manager BOX module could not convert time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_BOX_XML_PARSE_FAILED

Description: Agent Manager BOX module failed to parse XML from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_CISCOAMP_CONSUMER_START_FAILED

Description: Failed to start Cisco AMP consumer process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_CLOUDPASSAGE_API_CALL_FAILED

Description: CloudPassage Halo REST API call api failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_CLOUDPASSAGE_FILE_WRITE_ERROR

Description: Unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_CLOUDPASSAGE_GET_EVENT_FAILED

Description: Failed to get event from CloudPassage API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_CLOUDPASSAGE_JSON_EMPTY

Description: JSON is empty

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_CLOUDPASSAGE_JSON_PARSE_FAILED

Description: Failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_CLOUDPASSAGE_TOKEN_EMPTY

Description: Token is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_CLOUDTRAIL_FILE_READ_FAILED

Description: Agent Manager AWS CloudTrail module encountered error while reading Cloudtrail queue cache file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_CONFIG_ERROR

Description: Agent Manager own configuration error

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_CONFIG_VERSION_SEND_FAILED

Description: Agent Manager failed to send config version to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_AGENTMGR_CONFIG_WARNING

Description: FortiSIEM Agent Manager configuration warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AGENTMGR_CREDENTIAL_GET_FAILED

Description: Agent Manager failed to get credentials

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobName	Job Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_CROWDSTRIKE_GET_DATAFEED_URL_FAILED

Description: Failed to get crowdstrike datafeed url

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_CUST_RESULT_UPLOAD_FAILED

Description: Agent Manager failed to upload test custom performance monitor result xml to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_DIR_CREATE_FAILED

Description: Could not create dir

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_AGENTMGR_EVENT_PULL_FAILED

Description: Agent Manager Rapid7 InsightVM pulling engine failed to pull log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
accountName	Account Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_FALCONDATAREP_SCRIPT_FAILED

Description: Failed to run Falcon Data Replicator script

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_FILE_PARSE_ERROR

Description: Agent Manager/module failed to parse file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_FILE_WRITE_ERROR

Description: Agent Manager Rapid7 InsightVM pulling engine failed to write file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_FIREAMP_CERT_DOWNLOAD_FAILED

Description: Agent Manager/FireAMP Module cannot download certificate file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_FIREAMP_DATA_FORMAT_SET_FAILED

Description: Agent Manager/FireAMP Module encountered missing event mapping configuration

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_FIREAMP_EVENT_PULL_FAILED

Description: Agent Manager/FireAMP Module failed to pull log from server!

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_FIREAMP_EVT_TYPE_LOAD_FAILED

Description: Agent Manager/FireAMP Module encountered empty event mapping configuration

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_FIREAMP_FILE_LOAD_ERROR

Description: Agent Manager/FireAMP Module failed to load file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_FIREAMP_FILE_OPEN_ERROR

Description: Agent Manager/FireAMP Module failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_FIREAMP_INVALID_DATA

Description: Agent Manager/FireAMP Module found invalid response data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_FIREAMP_NEW_AGENT_FAILED

Description: Agent Manager/FireAMP Module - new agent failed

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_FIREAMP_NO_ATTR

Description: No configuration event attribute

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_FIREAMP_NO_PROTOCOL

Description: Can't find protocol number from IANA table

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_FORTICASB_GET_SERVICE_ALERT_ERROR

Description: Failed to get services alerts

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serviceName	Service Name	string	

EventType: PH_AGENTMGR_FORTICASB_GET_SERVICE_ERROR

Description: Failed to get services

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
unitId	Unit Id	string	

EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_FAILED

Description: FortiNDR cloud integration failed to call API URI

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_NEXT_PAGE

Description: FortiNDR paginated api call being made

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_NO_RESULTS

Description: API call to FortiNDR api returned no results, this is normal if no results in defined time interval

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

EventType: PH_AGENTMGR_FORTINDR_GET_API_CALL_RESULTS

Description: FortiNDR cloud integration called API URI successfully

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

EventType: PH_AGENTMGR_FORTINDR_GET_BUCKET_KEY

Description: FortiNDR integration is processing an s3 bucket key

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
bucketName	Bucket Name	string	
userKey	User Key	string	
categoryType	Category Type	string	

EventType: PH_AGENTMGR_FORTINDR_GET_BUCKET_OBJ

Description: FortiNDR integration is downloading an object from s3 bucket

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
bucketName	Bucket Name	string	
userKey	User Key	string	
categoryType	Category Type	string	

EventType: PH_AGENTMGR_GET_SCAN_RESULTS_FAILED

Description: Failed to get the scan result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_GITHUB_API_CALL_FAILED

Description: Agent Manager/GitHub module failed to call Github API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_GITHUB_CREDENTIAL_GET_FAILED

Description: Agent Manager/GitHub module failed to get credential from App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_AGENTMGR_GITHUB_EVENT_PULL_FAILED

Description: Agent Manager/GitHub module failed to pull log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
accountName	Account Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_GITHUB_FILE_OPEN_ERROR

Description: Agent Manager/GitHub module failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_GITHUB_JSON_PARSE_FAILED

Description: Agent Manager/GitHub module failed to parse JSON response from GitHub server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_GITHUB_TIME_CONVERT_FAILED

Description: Agent Manager/GitHub module failed to convert time in JSON response from GitHub server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_GIT_CLONE_REPO_FAILED

Description: Failed to git clone by do_system

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_AGENTMGR_GIT_HANDLE_ERR_FILE_FAILED

Description: Failed to handle error file

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_GIT_PULL_EVT_FAILED

Description: Failed to get git log by do_system

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_AGENTMGR_GIT_SAVE_COMMITID_FAILED

Description: Failed to save CommitId of repository

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_GZ_FILE_OPEN_ERROR

Description: Failed to open gz file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_INIT_AGENT

Description: Initialize agent

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_INIT_CACHE_FILE_FAILED

Description: FortiSIEM Agent Manager failed to initialize cache

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobName	Job Name	string	

EventType: PH_AGENTMGR_INIT_NO_CRED

Description: Agent Manager/Cisco IPS log pulling module failed to initialize due to missing credentials

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobName	Job Name	string	

EventType: PH_AGENTMGR_INVALID_MGR

Description: Invalid Agent Manager

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_IPS_AUTH_FAILED

Description: Agent Manager/Cisco IPS log pulling module found wrong user name, password for logging to IPS appliance

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_IPS_EVENT_PULL_FAILED

Description: Agent Manager/Cisco IPS log pulling module failed to pull Cisco IPS log from server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_AGENTMGR_IPS_FILE_OPEN_ERROR

Description: Agent Manager/Cisco IPS log pulling module failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_IPS_OBTAIN_SUBSCRIPTION_FAILED

Description: Agent Manager/Cisco IPS log pulling module failed to obtain subscription id

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_IPS_SET_SSL_FAILED

Description: SSL setting doesn't work

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_JAVA_AGENT_PIPE_WRITE_FAILED

Description: Failed to write to java agent pipe

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_JAVA_AGENT_START_FAILED

Description: Agent Manager failed to start Java agent, will retry

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_JAVA_AGENT_TYPE_UNKNOWN

Description: Agent Manager encountered unknown java agent job type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_JAVA_AGENT_USER_MISSING

Description: FortiSIEM Agent Manager found user name missing in java Agent configuration

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_AGENTMGR_JAVA_AGENT_ZOMBIE

Description: Agent Manager found Java Agent is in zombie state

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_JAVA_CMD_SEND_FAILED

Description: Agent Manager failed to send commands to java agent, need to be killed

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_JAVA_FORK_FAILED

Description: Agent Manager failed to fork Java Agent

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_JAVA_INCOMPLETE_DEV_INFO

Description: Agent Manager found incomplete device info for Java Agent

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_JAVA_NO_DEV_TYPE_FOR_JDBC

Description: Agent Manager encountered missing device type for Java Agent JDBC monitoring

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_AGENTMGR_JAVA_NO_STATUS_FILE

Description: Agent Manager missing status file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_JAVA_PIPE_FAILED

Description: Agent Manager failed to Pipe command for Java Agent

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_JAVA_PROCESS_STATE_GET_FAILED

Description: Agent Manager failed to get Java Agent process state

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_JAVA_SIGKILL_SEND_FAILED

Description: Agent Manager failed to send SIGKILL to java agent

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_JAVA_UNSupport_DEV_Type_FOR_JDBC

Description: Agent Manager encountered unsupported device type for Java Agent JDBC monitoring

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_AGENTMGR_JAVA_USER_PWD_GET_FAILED

Description: Agent Manager failed to get user name and password

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_JSON_PARSE_FAILED

Description: Agent Manager Rapid7 InsightVM monitoring module failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_KAFKA_CONSUME_LOG_FAILED

Description: Agent Manager / Kafka Consumer failed to pull log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_CREATE_CONSUMER

Description: phKafkaConsumer creates a consumer handle successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
groupName	Group Name	string	
user	User	string	
topicName	Topic Name	string	Kafka Topic Name

EventType: PH_AGENTMGR_KAFKA_CREATE_CONSUMER_FAILED

Description: Agent Manager / Kafka Consumer failed to create consumer

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_CREATE_PRODUCER_FAILED

Description: Agent Manager / Kafka Consumer failed to create producer

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_CREATE_TOPIC_FAILED

Description: Agent Manager / Kafka Consumer failed to create topic

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
topicName	Topic Name	string	Kafka Topic Name
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_ERROR

Description: Agent Manager / Kafka Consumer encountered occur

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_AGENTMGR_KAFKA_METADATA_FAILED

Description: Agent Manager / Kafka Consumer failed to get metadata

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_PRODUCER_ERROR

Description: Event Forwarder failed to write events into Kafka

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_AGENTMGR_KAFKA_PULL_JOB_FAILED

Description: Agent Manager / Kafka Consumer failed to Consume log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_KAFKA_REBALANCE

Description: Kafka rebalanceCb

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_KAFKA_RELEASE_CONSUMER

Description: phKafkaConsumer releases a consumer handle

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
groupName	Group Name	string	
user	User	string	
topicName	Topic Name	string	Kafka Topic Name

EventType: PH_AGENTMGR_KAFKA_START_FAILED

Description: Agent Manager / Kafka Consumer failed to start

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_SUBSCRIBE_FAILED

Description: Agent Manager / Kafka Consumer failed to subscribe topic

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
topicName	Topic Name	string	Kafka Topic Name
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_UPDATE_CONFIG_FAILED

Description: Agent Manager / Kafka Consumer failed to update attribute in config

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KAFKA_UPDATE_ERROR

Description: Agent Manager / Kafka Consumer failed to update failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_KILL_PROCESS

Description: Try to kill process

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_MSAZURE_CONFIG_ARM_FAILED

Description: Agent Manager / MS Azure config mode arm failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_MSAZURE_DOWNLOAD_FAILED

Description: Agent Manager / MS Azure failed to download Azure audit log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_MSAZURE_JSON_EMPTY

Description: Agent Manager / MS Azure found empty returned JSON from Azure

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_MSAZURE_JSON_FILE_NAME_EMPTY

Description: Agent Manager / MS Azure JSON file name is empty from Azure

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_MSAZURE_JSON_FILE_PARSE_FAILED

Description: Agent Manager / MS Azure found malformed JSON file from Azure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_MSAZURE_JSON_PARSE_FAILED

Description: Agent Manager / MS Azure found malformed JSON from Azure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_MSAZURE_LOGIN_FAILED

Description: Agent Manager / MS Azure failed to login to Azure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_MSG_QUEUE_ACCESS_FAILED

Description: Agent Manager failed to access message queue

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_MSG_RECV_FAILED

Description: Agent Manager failed to receive msg

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_OCI_SET_INSTANCE_NAME_FAILED

Description: Failed to set Oracle OCI Instance Name to hostname of this node, leaving as instance1

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_OFFICE365_API_CALL_FAILED

Description: Agent Manager / Office365 log pulling engine failed to call api

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_OFFICE365_EVENT_PULL_FAILED

Description: Agent Manager / Office365 log pulling engine failed to pull log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
accountName	Account Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_OFFICE365_FILE_WRITE_ERROR

Description: Agent Manager / Office365 log pulling engine unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_OFFICE365_GET_SUBSCRIBE_FAILED

Description: FortiSIEM Agent Manager failed to get Office365 subscription

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_OFFICE365_JSON_PARSE_FAILED

Description: Agent Manager / Office365 log pulling engine failed to parse Office365 JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_OFFICE365_START_SUBSCRIBE_FAILED

Description: FortiSIEM Agent Manager failed to start Office365 subscription

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_OFFICE365_SUBSCRIBE_EMPTY

Description: FortiSIEM Agent Manager found Office365 subscription to be empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_OFFICE365_SUBSCRIBE_FAILED

Description: Agent Manager / Office365 log pulling engine failed to get subscription list

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_OFFICE365_TOKEN_EMPTY

Description: Agent Manager / Office365 log pulling engine found empty Token

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_OKTA_EVT_DOWNLOAD_FAILED

Description: Agent Manager / OKTA failed to download events

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_OKTA_FILE_WRONG

Description: Agent Manager / OKTA encountered wrong Okta user list file. Please download again

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_OKTA_NO_USER_INFO

Description: Agent Manager / OKTA user list file doesn't contain any user info

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_OKTA_RESULT_UPLOAD_FAILED

Description: Agent Manager / OKTA failed to upload discovery result to App server

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_OKTA_RESULT_UPLOAD_WARNING

Description: FortiSIEM Agent Manager failed to upload OKTA User list to App Server

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_PARSER_UNABLE_CONNECT

Description: Agent Manager unable to connect to parser host

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
ipPort	IP Port	uint16	IP port number

EventType: PH_AGENTMGR_PERF_OBJ_PARSE_FAILURE

Description: Agent Manager did not find any performance objects to monitor

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_PROCESS_INIT_FAILED

Description: Agent Manager failed to initialize

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_PULLING_JOB_OUTDATE

Description: FortiSIEM Agent Manager job pull error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobName	Job Name	string	
serverIpAddr	Server IP	IP	

EventType: PH_AGENTMGR_REMOVE_FILE_FAILED

Description: Failed to remove file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_AGENTMGR_REST_API_CALL_FAILED

Description: Agent fails to call rest API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
infoURL	Informational URL	string	This field captures an URL if present in an event
httpStatusCode	HTTP Status	string	

EventType: PH_AGENTMGR_RSAS_XML_PARSE_FAILED

Description: AgentManager failed to parse XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_RUN_CMD_FAILED

Description: do_system failed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_RUN_SCRIPT_FAILED

Description: AgentManager failed to run script

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_RUN_SCRIPT_WITHOUT_TASK_ID

Description: AgentManager found missing task id in run script notification

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_ATTR_NOT_FOUND

Description: Agent Manager / Salesforce log pulling engine cannot find attribute

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_COLUMN_NOT_FOUND

Description: Agent Manager / Salesforce log pulling engine can not find a specific column in Salesforce Event Log File

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_CURL_EXECUTE_FAILED

Description: Agent Manager / Salesforce log pulling engine failed to execute curl to get Salesforce log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_AGENTMGR_SALESFORCE_CURL_HANDLE_GET_FAILED

Description: Agent Manager / Salesforce log pulling engine unable to get curl handle

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_FILE_LOAD_ERROR

Description: Agent Manager / Salesforce log pulling engine failed to load file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_SALESFORCE_FILE_WRITE_ERROR

Description: Agent Manager / Salesforce log pulling engine unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_SALESFORCE_INVALID_DATA

Description: Agent Manager / Salesforce log pulling engine received invalid response from Salesforce

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_INVALID_LOG_FILE

Description: Agent Manager / Salesforce log pulling engine received invalid Salesforce Event Log File csv

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_JSON_PARSE_FAILED

Description: Agent Manager / Salesforce log pulling engine received failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_LOGIN_FAILED

Description: Agent Manager / Salesforce log pulling engine failed to login to Salesforce

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
infoURL	Informational URL	string	This field captures an URL if present in an event

EventType: PH_AGENTMGR_SALESFORCE_SERVER_EMPTY

Description: Agent Manager / Salesforce log pulling engine found Server is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_TOKEN_GET_FAILED

Description: Agent Manager / Salesforce log pulling engine can't get login token

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_TOKEN_REGET_FAILED

Description: Agent Manager / Salesforce log pulling engine login session is expired and failed to re-get token

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_VERSION_PATH_EMPTY

Description: Agent Manager / Salesforce log pulling engine found empty version path

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SALESFORCE_XML_PARSE_FAILED

Description: Agent Manager / Salesforce log pulling engine failed to parse XML from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SCRIPT_NOTIFICATION_SPAWN_FAILED

Description: Agent Manager encountered error in spawning run script notification thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SERVER_HOST_NAME_RESOLVE_FAILED

Description: Agent Manager could not resolve server host name

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SERVER_HOST_NAME_RESOLVE_WARNING

Description: FortiSIEM Agent Manager failed to resolve Host Name to IP

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	
jobName	Job Name	string	

EventType: PH_AGENTMGR_SERVER_IP_RESOLVE_FAILED

Description: Agent Manager could not resolve server IP

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_SERVER_IP_RESOLVE_WARNING

Description: FortiSIEM Agent Manager failed to resolve IP to Host Name

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
jobName	Job Name	string	

EventType: PH_AGENTMGR_SETUP_STREAM_FAILED

Description: Failed to setup stream connection

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_START_THREAD_FAILED

Description: Failed to start thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_STATUS_REPORT_FAILED

Description: Agent Manager failed to report task status to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_STATUS_REPORT_INIT_FAILED

Description: Agent Manager failed to initialize job status reporter

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_STOP_STREAM_FAILED

Description: Failed to stop stream connection

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_TENABLE_EXPORT_SCAN_FAILED

Description: Exported scan failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_TENABLE_GET_DOWNLOAD_FAILED

Description: Download exported scan failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_TENABLE_GET_SCANS_FAILED

Description: Get the scan list failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_TENABLE_GET_STATUS_FAILED

Description: Check the file status of exported scan failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_TENABLE_PULL_FAILED

Description: Failed to pull Tenable.io data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_TIME_CONVERSION_FAILED

Description: Agent Manager/module failed to convert time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_TIME_STR_FORMAT_INVALID

Description: The format of time string is wrong

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
paraName	Param Name	string	

EventType: PH_AGENTMGR_TOKEN_GET_FAILED

Description: Agent Manager monitoring module cannot get login token

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_UNPACK_FILE_FAILED

Description: Agent Manager unpack file failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_AGENTMGR_UPDATE_AGENT

Description: Update agent

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_UPDATE_BOOKMARK_FAILED

Description: Failed to update bookmark

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_UPDATE_WEBHOOK_CRED_FAILED

Description: Failed to update Webhook credential

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_UPDATE_WEBHOOK_CRED_SUCCESS

Description: Update Webhook credential successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_WINDEFATP_API_CALL_FAILED

Description: Windows Defender ATP REST API call api failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_WINDEFATP_FILE_WRITE_ERROR

Description: Unable to write timestamp file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_AGENTMGR_WINDEFATP_GET_ALERT_FAILED

Description: Failed to get alert from Windows Defender ATP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_WINDEFATP_JSON_EMPTY

Description: JSON is empty

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_WINDEFATP_JSON_PARSE_FAILED

Description: Failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_WINDEFATP_TOKEN_EMPTY

Description: Token is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_WMI_EVENT_PULL_ERROR

Description: Agent Manager / Windows WMI event log pulling engine encountered error

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_WMI_EVENT_PULL_WARNING

Description: FortiSIEM Agent Manager WMI event pull warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_WMI_FILE_OPEN_ERROR

Description: Agent Manager / Windows WMI event log pulling engine failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_AGENTMGR_WMI_LOG_PULL_ERROR

Description: Failed to pull logs by WMI

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
errorString	Error String	string	This is the error message, synonymous to attribute errReason
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AGENTMGR_WMI_MISSING_LOG

Description: Some logs are missing

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AGENTMGR_WMI_STATUS_REPORT_FAILED

Description: Agent Manager / Windows WMI event log pulling engine failed to report task status to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_WMI_USER_PWD_GET_FAILED

Description: Agent Manager / Windows WMI event log pulling engine failed to get WMI user name and password

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_AGENTMGR_WVSS_XML_PARSE_FAILED

Description: Agent Manager / Windows WMI event log pulling engine failed to parse XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AGENTMGR_XML_PARSE_FAILED

Description: Agent Manager / Windows WMI event log pulling engine failed to parse XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_ANOMALY_CONFIG

Description: Anomaly Detection System Config Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_ANOMALY_LATERAL_MOVEMENT_ANALYZE

Description: FSM Anomaly engine: Lateral Movement Module in analyze mode

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

Id	Display name	Type	Description
startTime	Start Time	Date	This is the start time of a given item or task, and is stored in epoch milliseconds
endTime	End Time	Date	This is the end time of a given item or task, stored in epoch milliseconds.

EventType: PH_ANOMALY_LATERAL_MOVEMENT_DETECT

Description: FSM Anomaly engine detected Lateral Movement

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcIpAddrList	Source IP List	string	Comma separated list of source IP addresses as identified in a log message
destIpAddrList	Destination IP List	string	Comma separated list of destination IP addresses as identified in a log message
endTime	End Time	Date	This is the end time of a given item or task, stored in epoch milliseconds.

EventType: PH_ANOMALY_LATERAL_MOVEMENT_TRAIN

Description: FSM Anomaly engine: Lateral Movement Module in training mode

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
startTime	Start Time	Date	This is the start time of a given item or task, and is stored in epoch milliseconds
endTime	End Time	Date	This is the end time of a given item or task, stored in epoch milliseconds.

EventType: PH_ANOMALY_SYSTEM

Description: Anomaly Detection System Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_ANOMALY_TIMER

Description: Anomaly Detection System Timer Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_APPSERVER_ADMIN_AGENT_GET_UPDATE_FAILED_ERROR

Description: App Server failed to get update

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_ADMIN_AGENT_UNKOWN_TASK_ID_ERROR

Description: App Server detects unkown Admin Agent task ID

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_ADMIN_CUST_GENERATE_KEY_ERROR

Description: App Server failed to generate organization key

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_ADMIN_GET_RESOURCE_FAILED

Description: App Server failed to get resource for admin tab

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_ADMIN_LOCATE_KEY_FAILED

Description: App Server failed to locate resource for admin tab

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_ADMIN_RESET_FIELD_FAILED_ERROR

Description: App Server failed to reset resource for admin tab

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_AUDIT_REPORT_EXPORT_ERROR

Description: Audit Data Export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEACON_LIB_ERROR

Description: App Server Beaconsing library error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEACON_REGISTER_ERROR

Description: App Server Beaconsing Register error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEACON_SERVER_ERROR

Description: App Server Beaconsing Server error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEACON_WEB_SERVER_ERROR

Description: App Server Beaconsing Web Server error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEAN_REF_CHECK_WARN

Description: App Server check entity bean reference warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEAN_SYNC_PROPERTIES_ERROR

Description: App Server entity bean sync properties error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEAN_TO_VALUE_ERROR

Description: App Server entity bean to property value map error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEAN_TO_XML_ERROR

Description: App Server entity to XML generation error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_BEAN_VALUE_TO_BEAN_ERROR

Description: App Server set value for Entity bean error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_CMDB_REPORT_DATA_ERROR

Description: CMDB Report Data error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_CMDB_REPORT_EXPORT_ERROR

Description: CMDB Report export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_CMDB_REPORT_IMPORT_ERROR

Description: CMDB Report import error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_CMDB_REPORT_QUERY_ERROR

Description: CMDB Report query error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_CMDB_REPORT_TYPE_ERROR

Description: CMDB Report Type error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_COLLECTOR_INFO_ERROR

Description: Collector information error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_COLLECTOR_LICENSE_ERROR

Description: Collector license error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_COLLECTOR_STATUS_ERROR

Description: Collector status error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_COMMONPWD_EXPORT_ERROR

Description: Common password data export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DASHBOARD_DATA_ERROR

Description: Dashbaord Data error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DASHBOARD_HTML_BUILD_XML_ERROR

Description: App Server failed to build dashboard XML content

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DASHBOARD_WIDGET_ERROR

Description: Dashbaord Widget error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DATA_IMPORT_ERROR

Description: App Server failed to import data during initialization

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DATA_ROBUST_INFO_ERROR

Description: Data Robust Info error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DB_CONNECTION_CLOSE_ERROR

Description: PostgreSQL database connection close error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DB_DATA_ERROR

Description: PostgreSQL database data error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DB_DELETE_ERROR

Description: PostgreSQL database data delete error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DB_QUERY_ERROR

Description: PostGreSQL database query error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DB_UPDATE_ERROR

Description: PostGreSQL database data update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DISCOVERY_CREDENTIAL_DECRYPT_PASSWORD_WARN

Description: App Server discovery result credential decrypt error

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DISCOVERY_RESULT_ENCRYPT_XML_ELEMENT_ERROR

Description: App Server discovery result credential encrypt error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DISCOVERY_RESULT_ERROR

Description: App Server failed to process discovery result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_DISCOVERY_RESULT_UNKOWN_TASK_ID_ERROR

Description: App Server detects unknown Discovery Result task ID

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EAMIL_GENERATE_EVENT_ERROR

Description: App Server failed to generate raw event for email notification

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_ELASTIC_UPDATE_ERROR

Description: App Server failed to update Elasticsearch configuration

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EMAIL_PREPARE_DATA_ERROR

Description: App Server failed to prepare email body for email notification

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EVENTDB_EXPORT_ERROR

Description: Event DB data export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EVENT_ATTRIBUTE_BUILD_XML_ERROR

Description: App Server failed to build Event Attribute XML content

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EXPORT_ERROR

Description: App Server Generic Export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EXT_THREAT_INTEL_DOWNLOAD_ERROR

Description: External Threat Intelligence download error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EXT_THREAT_INTEL_PARSE_ERROR

Description: External Threat Intelligence parse error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_EXT_THREAT_INTEL_UPDATE_ERROR

Description: External Threat Intelligence update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FILE_NOT_FOUND

Description: App Server cannot find specified file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FILE_READ_ERROR

Description: App Server cannot read from specified file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FILE_SYSTEM_ERROR

Description: App Server encountered file system error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FILE_WRITE_ERROR

Description: App Server cannot write to specified file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FLEX_INTERCEPTOR_NO_LOGIN_EXCEPTION_ERROR

Description: App Server encountered Flex API exception

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FORTIGUARD_IOC_INTEGRATION_ERROR

Description: FortiGuard IOC data download/parse error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_REGISTER_ERROR

Description: App Server Registration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_RUN_THREAD_ERROR

Description: App Server run thread error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_SECURITY_CHECK_LICENSE_WARN

Description: App Server Check license warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_SECURITY_GET_ENTITY_MANAGER_ERROR

Description: App Server cannot get EntityManager

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_SECURITY_GET_RS_EXPIRATION_ERROR

Description: App Server Get Report Server expiration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_SECURITY_INIT_SYSTEM_ERROR

Description: App Server Phoenix Caching system initialization failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_SERVICE_MISSED_WARN

Description: App Server can not find service

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_FRAMEWORK_SHUTDOWN_SERVICE_STARTER_WARN

Description: App Server cannot shutdown service starter

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_GENERIC_ERROR

Description: Unknown Application Server error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_GENERIC_INFO

Description: Generic Application Server Informational log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_GENERIC_WARN

Description: Generic Application Server Warn

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_GET_MAX_CONFIG_ITEM_COUNT_ERROR

Description: App Server encountered error while getting max system configuration item count

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_GROUP_DATA_ERROR

Description: Group Data error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_IDENTITYLOCATION_EXPORT_ERROR

Description: Identity location export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_INCIDENT_NOTIFY_ERROR

Description: App Server failed to notify Incident via email or other methods

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_INCIDENT_UPDATE_ERROR

Description: App Server failed to update Incident in PostgreSQL database

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_INTEGRATION_ERROR

Description: External ticketing system integration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_INTEGRATION_UPDATE_POLICY_ERROR

Description: App Server encountered error while updating Ticketing system integration policy

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_INTEGRATION_UPDATE_POLICY_WARN

Description: App Server encountered warning while updating Ticketing system integration policy

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_INTEGRATION_WARN

Description: External ticketing system integration warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_IN_INTEGRATION_ERROR

Description: Inbound external ticketing system integration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_IOC_LICENSE_CHECK_FAILED_WARN

Description: App Server failed to check External Threat Intelligence License

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_IOC_TASK_CREATE_FAILED_ERROR

Description: App Server failed to create External Threat Intelligence Update task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_JOB_DISTRIBUTE_ERROR

Description: Application Server monitoring job distribution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_LICENSE_EXPIRY_ERROR

Description: License Expiration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_LICENSE_VALIDATION_ERROR

Description: License Validation error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_LOGIN_ERROR

Description: App Server Login exception

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_LOG_INTEGRITY_ERROR

Description: App Server failed to update log integrity hashes

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_MONITOR_AUDIT_PERF_ERROR

Description: App Server encountered exception while updating performance monitor job status

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_MONITOR_HEALTH_CONFIG_SET_ERROR

Description: App Server failed to update CMDB Device Monitor Health

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NETSEGMENT_EXPORT_ERROR

Description: Network Segment Export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NOTIFICATION_EMAIL_GET_RESOURCE_FAILED

Description: App Server failed to get resource for email notification

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NOTIFICATION_ERROR

Description: App Server notification error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NOTIFICATION_JMS_CONNECTION_ERROR

Description: App Server create JMS connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NOTIFICATION_UPDATE_ERROR

Description: App Server notification Update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NOTIFIER_ERROR

Description: App Server Notifier error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_NO_WATCHLIST_SELECTED_WARN

Description: No watch list selected for entry warn

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_OPENPROXY_EXPORT_ERROR

Description: Open proxy data export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_OUT_INTEGRATION_ERROR

Description: Outbound external ticketing system integration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_PARSER_IMPORT_ERROR

Description: Custom parser import error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_PARSER_UPDATE_ERROR

Description: Custom parser update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_PARSING_CONSTRAINT_ERROR

Description: Rule/Report constraint parsing error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_PDF_BUILDER_ERROR

Description: App Server failed to build PDF during report export

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_PERFMON_TASK_ERROR

Description: App Server failed to create Performance Monitoring Task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_CHECK_POLICY_ACTION_WARN

Description: App Server failed to validate Incident notification policy action

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_EXPORT_ERROR

Description: App Server failed to export historical query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_RESULT_PARSER_ERROR

Description: App Server failed to parse historical query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_RESULT_RETRIEVE_ERROR

Description: App Server failed to retrieve historical query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_RUN_ERROR

Description: App Server failed to run historical query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_STOP_ERROR

Description: App Server failed to stop historical query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_QUERY_STRING_ESCAPE_ERROR

Description: App Server can't find close escape string

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RBAC_ERROR

Description: App Server encountered error while setting RBAC policies

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RBAC_NO_PERMISSION_WARN

Description: App Server enforced user RBAC

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REALTIME_QUERY_ERROR

Description: App Server failed to start real time query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REMEDY_ERROR

Description: App Server failed to create tickets in Remedy

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_BUNDLE_PRINT_ERROR

Description: Print report bundle error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_COMPILE_ERROR

Description: Compile report to file error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_DEVICE_COMPONENT_SN_ERROR

Description: CMDB device serial number report error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_DEVICE_DETAIL_ERROR

Description: CMDB detail report error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_DEVICE_SN_ERROR

Description: CMDB server serial number report error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_DEVICE_SUMMARY_ERROR

Description: CMDB summary report error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_EXPORT_ERROR

Description: Report Export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_FAILED_BLOCK_SUMMARY_ERROR

Description: Get failed blocks error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_FIRE_TRIGGER_EVENT_ERROR

Description: App Server incident trigger events report error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_GET_PH_CONFIG_ERROR

Description: App Server get phoenix configuration error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_IDENTITY_AND_LOCATION_ERROR

Description: Identity and location report error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_LOG_FILE_SUMMARY_ERROR

Description: App Server get log files error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_TEMPLATE_GENERATE_PDF_ERROR

Description: App Server Report template generate PDF error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_TEMPLATE_INIT_IMAGE_ERROR

Description: App Server Report template init image error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_TEMPLATE_INIT_PARM_ERROR

Description: App Server Report template init parameter error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_TEMPLATE_PDF_SUMMARY_ERROR

Description: App Server Report template create PDF summary error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_TICKET_SUMMARY_ERROR

Description: App Server get tickets error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_UPDATE_ERROR

Description: User defined report update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REPORT_USER_SUMMARY_ERROR

Description: App Server get users error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REST_ERROR

Description: App Server REST error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_REST_H5_ERROR

Description: App Server HTML5 REST error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RISKSCORE_CALCULATE_ERROR

Description: Risk score calculation error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RULE_ACTIVE_ERROR

Description: App Server failed to activate rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RULE_CLONE_ERROR

Description: App Server failed to clone rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RULE_DEBUG_INVALID_EVENT_DB_ID_ERROR

Description: App Server found invalid event id during rule testing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RULE_DEBUG_WORKERS_SETTING_ERROR

Description: App Server detected Worker Settings error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RULE_TEST_ERROR

Description: App Server encountered error while testing rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_RULE_UPDATE_ERROR

Description: App Server failed to update rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SCHEDULE_ERROR

Description: App Server job schedule error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SCHEDULE_UPDATE_ERROR

Description: App Server job schedule Update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SECURITY_ERROR

Description: Application Server System Security Data error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SERVLET_ERROR

Description: App Server Servlet error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SERVLET_NO_ACCESS_TO_URI_WARN

Description: App Server Servlet has no access to URI

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SOCKET_COMM_ERROR

Description: App Server Socket communication error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SVN_ERROR

Description: App Server SVN Repository error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SYNC_UPDATE_CONFIG_ERROR

Description: App Server encountered error on syncing update config for performance monitoring jobs

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SYSCONFIG_GET_ERROR

Description: App Server failed to get system configuration from PostGreSQL database

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SYSTEM_WINAGENT_REGISTER_WARN

Description: Windows Agent Manager not found or not registered

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SYS_APPLICATION_ERROR

Description: Application Server System error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_SYS_DATA_UPDATE_ERROR

Description: Application Server Data Update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_TASK_CREATE_ERROR

Description: App Server create task error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_TASK_FLEX_RESULT_BUILD_XML_ERROR

Description: App Server failed to build Flex XML content

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_TASK_GET_ERROR

Description: App Server get task error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_TASK_UPDATE_ERROR

Description: App Server update task error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_TICKET_EXPORT_ERROR

Description: Incident ticket export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_UPDATER_FIND_EXIST_USER_BY_NOTHING_ERROR

Description: App Server failed to locate existing user in CMDB

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_USERAGENT_EXPORT_ERROR

Description: User agent export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_VULNERABILITY_IGNORE_WARN

Description: App Server ignored host Vulnerability result

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WATCHLIST_ADD_TO_DISTIRBUTED_QUEUE

Description: App Server failed to add incident attribute to watch list

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WATCHLIST_EXPORT_ERROR

Description: Watch List export error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WATCHLIST_IMPORT_ERROR

Description: Watch List import error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WATCHLIST_IMPORT_WARN

Description: Watch List import warnings

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WATCHLIST_UPDATE_ERROR

Description: Watch List update error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WEBSERVICE_UPDATE_TASK_ERROR

Description: App Server encountered error while updating task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WORKER_PROVISION_FAILED

Description: App Server failed to provision Worker

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_WS_COMM_ERROR

Description: App Server Web service communication error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_APPSERVER_XML_PARSE_ERROR

Description: App Server failed to parse XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ACCOUNT_LOCKED

Description: System user account locked due to excessive login failures

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
reason	Reason	string	
targetUser	Target User	string	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.

EventType: PH_AUDIT_AGENT_DISABLED

Description: FortiSIEM Windows/Linux Agent disabled

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	

Id	Display name	Type	Description
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_INSTALLED

Description: FortiSIEM Windows/Linux Agent installed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_NOTRESPONDING

Description: FortiSIEM Windows/Linux Agent not responding

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	

Id	Display name	Type	Description
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_RUNNING

Description: FortiSIEM Windows/Linux Agent is running and sending events

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_STARTED

Description: FortiSIEM Windows/Linux Agent started

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	

Id	Display name	Type	Description
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_STOPPED

Description: FortiSIEM Windows/Linux Agent stopped

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_AGENT_UNINSTALLED

Description: FortiSIEM Windows/Linux Agent uninstalled

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
monitorState	Monitor State	string	

Id	Display name	Type	Description
type	Type	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_AUDIT_CASE_ASSIGNED

Description: FortiSIEM Case Assigned to a User

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
targetUser	Target User	string	

EventType: PH_AUDIT_CASE_CLOSED

Description: FortiSIEM Case Closed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	

Id	Display name	Type	Description
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
comment	Comment	string	

EventType: PH_AUDIT_CASE_CREATED

Description: FortiSIEM Case Created

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

EventType: PH_AUDIT_CASE_EVIDENCE_ADDED

Description: FortiSIEM Case Evidence Added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
type	Type	string	
fileName	File Name	string	

EventType: PH_AUDIT_CASE_EVIDENCE_DELETED

Description: FortiSIEM Case Evidence Deleted

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
type	Type	string	
fileName	File Name	string	

EventType: PH_AUDIT_CASE_INCIDENT_ADDED

Description: FortiSIEM Incident added to a Case

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

EventType: PH_AUDIT_CASE_MERGED

Description: FortiSIEM Case Merged

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case

EventType: PH_AUDIT_CASE_NOTE_ADDED

Description: FortiSIEM Case Note Added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
comment	Comment	string	

EventType: PH_AUDIT_CASE_NOTE_DELETED

Description: FortiSIEM Case Note Deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

Id	Display name	Type	Description
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

EventType: PH_AUDIT_CASE_NOTE_MODIFIED

Description: FortiSIEM Case Note Modified

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
comment	Comment	string	

EventType: PH_AUDIT_CASE_PRIORITY_CHANGED

Description: FortiSIEM Case Priority Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

Id	Display name	Type	Description
oldSeverity	Old Severity	string	
newSeverity	New Severity	string	

EventType: PH_AUDIT_CASE_REASSIGNED

Description: FortiSIEM Case Reassigned

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
targetUser	Target User	string	

EventType: PH_AUDIT_CASE_STAGE_CHANGED

Description: FortiSIEM Case Stage Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

EventType: PH_AUDIT_CASE_STAT

Description: FortiSIEM Case Closed Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
user	User	string	
newDuration	New Duration	uint64	Duration of a case in the new status
assignedDuration	Assigned Duration	uint64	Duration of a case in the assigned status
inProgressDuration	In-Progress Duration	uint64	Duration of a case in the in-progress status
pendCustFeedbackDuration	Pending Customer Feedback Duration	uint64	Duration of a case in the pending feedback status
recvCustFeedbackDuration	Received Customer Feedback Duration	uint64	Duration of a case in the received feedback status
timeToClose	Time to Close	uint64	Total duration that a case was open

EventType: PH_AUDIT_CASE_STATUS_CHANGED

Description: FortiSIEM Case Status Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	

EventType: PH_AUDIT_CASE_SUMMARY_CHANGED

Description: FortiSIEM Case Summary Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
caseId	Case ID	uint64	Unique ID of a FortiSIEM Case
title	Title	string	
oldTitle	Old Title	string	

EventType: PH_AUDIT_CASE_UPDATED

Description: FortiSIEM Case Updated

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_CI_QUOTE_EXCEEDED

Description: System CI Quote Exceeded

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_CMDB_DISK_PRUNE_FAILED

Description: CMDB Disk Prune Failed

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
freeDiskMB	Free Disk MB	uint32	

EventType: PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS

Description: CMDB Disk Prune Success

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
freeDiskMB	Free Disk MB	uint32	

EventType: PH_AUDIT_DASHBOARD_SHARED

Description: FortiSIEM dashboard folder shared

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	
targetUserGrp	Target User Group	string	

EventType: PH_AUDIT_DATA_PURGE

Description: System data has been purged

Severity: 1 (Low)**Event Category:** 3 (System Logs)

EventType: PH_AUDIT_DB_LEADER_CHANGE

Description: DB Leader Changed**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phEventCategory	System Event Category	uint16	This is the category of log event. (Values: 0 - External, 1 - Incidents, 2 - Audit, 3 - System, 4 - Traffic Flow, 5- Health, 6 - Performance). When you query events in FortiSIEM, only Category 0 events show up in search results by default. To include other events, you need to explicitly include Categories in the Search condition; for example to search for Incidents, use System Event Category = 1.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_AUDIT_DEFAULT_PWD_MATCH

Description: Default password match**Severity:** 7 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
reptVendor	Reporting Vendor	string	This field captures the vendor of the reported event
reptModel	Reporting Model	string	This field captures the model of the reported event

Id	Display name	Type	Description
appTransportProto	Application Protocol	string	
user	User	string	

EventType: PH_AUDIT_DEVICE_ADDED

Description: System CMDB device added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_AUDIT_DEVICE_DELETED

Description: System CMDB device deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_AUDIT_DEVICE_DISCOVERY_ITEM_CHANGED

Description: System CMDB device changed by discovery

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
objType	Object Type	string	
addedItem	Added Item	string	

EventType: PH_AUDIT_DEVICE_MAINTENANCE_ENDED

Description: System device maintenance ended

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
maintScheduleName	Maintenance Schedule Name	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
endTime	End Time	Date	This is the end time of a given item or task, stored in epoch milliseconds.

EventType: PH_AUDIT_DEVICE_MAINTENANCE_STARTED

Description: System device maintenance started

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
maintScheduleName	Maintenance Schedule Name	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
startTime	Start Time	Date	This is the start time of a given item or task, and is stored in epoch milliseconds

EventType: PH_AUDIT_DEVICE_MERGED_BY_IP_WITH_DIFF_NAME

Description: Two devices with different hostname merged because of overlapping IP addresses

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
targetHostName	Target Host Name	string	
overlapIp	Overlapping IP	string	This field represents the list of IP addresses of a just discovered device that overlaps with an existing device in CMDB.

EventType: PH_AUDIT_DEVICE_STATUS_CHANGED

Description: CMDB Device audit status changed

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
origStatus	Original Status	string	
newStatus	New Status	string	
eventSource	Event Source	string	

EventType: PH_AUDIT_DEVICE_UNMANAGED

Description: license exceeded - newly discovered device set to Unmanaged

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
status	Status	string	

Id	Display name	Type	Description
eventSource	Event Source	string	
details	Details	string	

EventType: PH_AUDIT_DEV_MON_JOB_NOT_STARTED

Description: Performance monitoring Job is not picked up for execution for a long time

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_DEV_MON_JOB_STATUS_CHANGE

Description: Performance monitoring job status changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_DISCOVERY

Description: Audit discovery

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
startTime	Start Time	Date	This is the start time of a given item or task, and is stored in epoch milliseconds
type	Type	string	
task	Task	string	
osObjName	Object Name	string	

EventType: PH_AUDIT_EXPORT_REPORT_END

Description: User exported FortiSIEM Report result via GUI or Scheduled Report

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_GENAI_USER_QUERY

Description: FortiSIEM sent Generative AI Query to ChatGPT

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_GENERIC

Description: System generic audit message

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_GROUP_CREATED

Description: FortiSIEM GUI Group Created

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
osObjName	Object Name	string	
osObjType	OS Object Type	string	

EventType: PH_AUDIT_GROUP_DELETED

Description: FortiSIEM GUI Group Deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
osObjName	Object Name	string	
osObjType	OS Object Type	string	

EventType: PH_AUDIT_INACTIVE_USER_LOGIN

Description: A system inactive user tried to login

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_INCIDENT_SYS_CLEAR

Description: FortiSIEM Incident System Auto-Cleared

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	
osObjHandleID	Object Handle	string	

EventType: PH_AUDIT_INCIDENT_USER_CLEAR

Description: FortiSIEM Incident User Cleared

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	
osObjHandleID	Object Handle	string	

EventType: PH_AUDIT_INTEGRATION_POLICY_EXECUTED

Description: FortiSIEM Integration Policy Executed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	

EventType: PH_AUDIT_MALWARE_DATA_DELETED

Description: Malware data deleted by scheduled update

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
updateTime	Update Time	Date	

Id	Display name	Type	Description
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.
folder	Folder	string	

EventType: PH_AUDIT_MALWARE_DATA_UPDATED

Description: Malware data updated by scheduled update

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
updateTime	Update Time	Date	
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.
folder	Folder	string	

EventType: PH_AUDIT_ML_GENERIC_ERROR

Description: Machine Learning generic error log

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ML_GENERIC_INFO

Description: Machine Learning generic info log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ML_INFERENCE_COMPLETED

Description: Machine Learning audit inference completed log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ML_INFERENCE_RESULT

Description: Machine Learning audit inference result log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ML_INFERENCE_STARTED

Description: Machine Learning audit inference started log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ML_TRAINING_COMPLETED

Description: Machine Learning audit training completed log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_ML_TRAINING_STARTED

Description: Machine Learning audit training started log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_NOTIF_POLICY_EXECUTED

Description: FortiSIEM Incident Notification Policy Executed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
osObjHandleID	Object Handle	string	

EventType: PH_AUDIT_OBJECT_CREATED

Description: System data object created

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjType	OS Object Type	string	
osObjName	Object Name	string	

EventType: PH_AUDIT_OBJECT_DELETED

Description: System data object deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	

EventType: PH_AUDIT_OBJECT_UPDATED

Description: System data object updated

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjType	OS Object Type	string	
objType	Object Type	string	
osObjName	Object Name	string	
osObjAction	Object Action	string	
targetCustomer	Target Organization Name	string	
oldSettingsValue	Old Settings Value	string	
newSettingsValue	New Settings Value	string	

EventType: PH_AUDIT_ONDEMAND_REMEDIATION_EXECUTED

Description: FortiSIEM Ondemand Remediation Executed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	

EventType: PH_AUDIT_PASSWORD_CHANGED

Description: System user password changed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
user	User	string	
domain	Domain	string	

EventType: PH_AUDIT_QUERY_COMPLETED

Description: Audit query completed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
osObjName	Object Name	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
durationMSec	Duration	uint32	Duration of a connection (in msec)
queryFilter	Query Filter	string	
queryDisplay	Query Display	string	
queryId	Query Id	string	
usageType	Usage Type	string	

EventType: PH_AUDIT_QUERY_SCHEDULED

Description: System scheduled a query

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.

EventType: PH_AUDIT_QUERY_START

Description: System started a query

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
osObjName	Object Name	string	

EventType: PH_AUDIT_QUERY_STOP

Description: System stopped a query

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
osObjName	Object Name	string	
durationMSec	Duration	uint32	Duration of a connection (in msec)

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_AUDIT_REPL_LEADER_CHANGE

Description: Replication Leader Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
phEventCategory	System Event Category	uint16	This is the category of log event. (Values: 0 - External, 1 - Incidents, 2 - Audit, 3 - System, 4 - Traffic Flow, 5- Health, 6 - Performance). When you query events in FortiSIEM, only Category 0 events show up in search results by default. To include other events, you need to explicitly include Categories in the Search condition; for example to search for Incidents, use System Event Category = 1.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_AUDIT_REPORT_SCHEDULED

Description: FortiSIEM Report Scheduled

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_REPORT_SCHEDULE_APPROVE

Description: FortiSIEM Report schedule approval

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
objId	DB Object Id	string	
status	Status	string	
targetUser	Target User	string	
reportId	Report ID	uint32	
reportName	Report Name	string	FortiSIEM report name.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AUDIT_REPORT_SCHEDULE_REQUEST**Description:** FortiSIEM Report schedule request**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
user	User	string	
objId	DB Object Id	string	
status	Status	string	
targetUser	Target User	string	
reportId	Report ID	uint32	
reportName	Report Name	string	FortiSIEM report name.

EventType: PH_AUDIT_REPORT_SERVER_LICENSE_EXPIRED**Description:** FortiSIEM Report Server license expired**Severity:** 10 (High)**Event Category:** 3 (System Logs)

EventType: PH_AUDIT_REPORT_SERVER_LICENSE_REMOVED

Description: FortiSIEM Report Server Removed After License Expiry

Severity: 8 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_REPORT_SERVER_LICENSE_TO_EXPIRE

Description: FortiSIEM Report Server license about to expire

Severity: 8 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_RISK_DECREASE_LOW

Description: Device Risk Score decreased to LOW level

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_RISK_DECREASE_MED

Description: Device Risk Score decreased to MEDIUM level

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_RISK_INCREASE_HIGH

Description: Device Risk Score increased to HIGH level

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_RISK_INCREASE_MED

Description: Device Risk Score increased to MEDIUM level

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_RULE_ACTIVATED

Description: FortiSIEM Rule activated

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	

EventType: PH_AUDIT_RULE_ACTIVATION_APPROVE

Description: FortiSIEM Rule activation approval

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
objId	DB Object Id	string	
status	Status	string	
targetUser	Target User	string	
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AUDIT_RULE_ACTIVATION_REQUEST

Description: FortiSIEM Rule activation request

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
objId	DB Object Id	string	
status	Status	string	
targetUser	Target User	string	
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_AUDIT_RULE_DEACTIVATED**Description:** FortiSIEM Rule de-activated**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
osObjName	Object Name	string	

EventType: PH_AUDIT_RULE_DEACTIVATION_APPROVE**Description:** FortiSIEM Rule de-activation approval**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
user	User	string	
objId	DB Object Id	string	
status	Status	string	
targetUser	Target User	string	
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

Id	Display name	Type	Description
ruleName	Rule Name	string	FortiSIEM rule name.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_AUDIT_RULE_DEACTIVATION_REQUEST

Description: FortiSIEM Rule de-activation request

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
objId	DB Object Id	string	
status	Status	string	
targetUser	Target User	string	
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_AUDIT_SVC_LOGIN_FAILURE

Description: System service user failed to login

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_SVC_LOGIN_SUCCESS

Description: System service user login success

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_SVC_LOGOFF

Description: System Service user logoff

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_SVC_SESSION_TIMEOUT

Description: System service user session timeout

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_TUNNEL_CLOSE

Description: Collector to Super Reverse SSH Tunnel closed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
appTransportProto	Application Protocol	string	
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
collectorIp	Collector IP	IP	This field captures the IP address of a FortiSIEM Collector
tunnelUpTime	Tunnel Uptime	uint64	
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.

EventType: PH_AUDIT_TUNNEL_OPEN

Description: Collector to Super Reverse SSH Tunnel opened

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
appTransportProto	Application Protocol	string	
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
collectorIp	Collector IP	IP	This field captures the IP address of a FortiSIEM Collector
tunnelUpTime	Tunnel Uptime	uint64	
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.

EventType: PH_AUDIT_USER_ADDED

Description: System user added

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
user	User	string	
domain	Domain	string	

EventType: PH_AUDIT_USER_CHANGE_ORG_SCOPE

Description: FortiSIEM user changed organization scope

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
userFullName	User Full Name	string	
targetCustomer	Target Organization Name	string	

EventType: PH_AUDIT_USER_DEFAULT_ROLE_CHANGED

Description: FortiSIEM Admin User Default Role Changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
targetCustomer	Target Organization Name	string	
role	Role	string	

EventType: PH_AUDIT_USER_DELETED

Description: System user deleted

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
user	User	string	
targetUser	Target User	string	
details	Details	string	

EventType: PH_AUDIT_USER_LOGIN_FAILURE

Description: System user failed to login

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
domain	Domain	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_AUDIT_USER_LOGIN_SUCCESS

Description: System user login success

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
userFullName	User Full Name	string	

EventType: PH_AUDIT_USER_LOGOFF

Description: System user logoff

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
userFullName	User Full Name	string	

EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_CHANGED

Description: FortiSIEM Admin User Organization Role changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
targetCustomer	Target Organization Name	string	
role	Role	string	

EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_ENABLED

Description: FortiSIEM Admin User Organization Role enabled

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_AUDIT_USER_ORGANIZATION_ROLE_REMOVED

Description: FortiSIEM Admin User Organization Role disabled

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
targetUser	Target User	string	
targetCustomer	Target Organization Name	string	
role	Role	string	

EventType: PH_AUDIT_USER_SESSION_TIMEOUT

Description: System user session timeout

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
userFullName	User Full Name	string	

EventType: PH_AUDIT_WS_COMM

Description: System web service communication

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_BAD_NETFLOW_PACKET

Description: Bad netflow packet

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BAD_NETFLOW_VER

Description: Unsupported netflow version

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BAD_ROUTE_OUTPUT

Description: FortiSIEM encountered bad route output

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_BASE_AGENT_JOB_NO_THREAD_NUM_ASSIGNED

Description: FortiSIEM module error - no thread count assigned

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_DUMP_STACK_TRACE_FAILURE

Description: FortiSIEM module error - stack trace failed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
filePath	File Path	string	

EventType: PH_BASE_PROC_GET_PID_FILE_FAILED

Description: FortiSIEM module error - failed to get process id

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_BASE_PROC_HANDLE_NOTIFICATION_ERROR

Description: FortiSIEM module error - notification error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_KILL_PROC_ERROR

Description: FortiSIEM module error - failed to kill process

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_BASE_PROC_NOTIFICATION_HANDLE_CONN_ERROR

Description: FortiSIEM module error - no notification connection

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_NO_CONN_TO_HEARTBEAT_SERVER

Description: FortiSIEM module error - no connection to heartbeat

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_RENAME_MINI_DUMP_FILE_FAILURE

Description: FortiSIEM module error - minidump error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_REST_CACHE_CHECKOUT_STATUS_WARNING

Description: FortiSIEM module error - REST cache access error

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event

EventType: PH_BASE_PROC_SEND_HEARTBEAT_FAILURE

Description: FortiSIEM module error - failed to send heartbeat

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
procName	Process Name	string	

EventType: PH_BASE_PROC_SEND_USER_DEFINED_SIG_FAILED

Description: FortiSIEM module error - user defined sig failed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_SET_PID_FILE_FAILED

Description: FortiSIEM module error - setpid failed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_BASE_PROC_STACK_TRACE

Description: FortiSIEM module stack trace

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_STACK_TRACK_TOO_LONG

Description: FortiSIEM module erro - stack trace too large

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_SYS_INFO_CALC_CPU_ERROR

Description: FortiSIEM module error - failed to calculate CPU

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
procName	Process Name	string	

EventType: PH_BASE_PROC_SYS_PROC_INFO_GET_FAILURE

Description: FortiSIEM module error - failed to get proc info

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_SYS_PROC_INFO_INIT_ERROR

Description: FortiSIEM module error - proc info get error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_SYS_PROC_INFO_UNABLE_OPEN_PROC_PID_FILE

Description: FortiSIEM module error - unable to open proc pid file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_BASE_PROC_SYS_PROC_INFO_UNABLE_OPEN_PROC_STAT_FILE

Description: FortiSIEM module error - unable to open proc stat file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
procName	Process Name	string	

EventType: PH_BASE_PROC_THREAD_SPAWN_FAILED

Description: FortiSIEM module error - failed to spawn thread

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_THREAD_WRONG_PARAM

Description: FortiSIEM module error - wrong paremeters to thread span function

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PROC_UPLOAD_FILE_FAILURE

Description: FortiSIEM module error - file upload failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_BASE_PROC_VALUE_GROUP_UPDATE_FAILURE

Description: FortiSIEM module error - value group update failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_BASE_PRO_AQUIRE_SHARED_STORE_FAILED

Description: Unable to acquire shared store instance

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CHECKPOINT_CERTHANDLER_ERROR

Description: Checkpoint failed to parse device certificate received from App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_CERTPULL_ERROR

Description: Checkpoint failed to obtain certificate from App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_CMD_USAGE_ERROR

Description: Checkpoint command usage error

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_CPMI_FETCH_ERROR

Description: Checkpoint CPMI fetch error. Events may miss some metadata

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
errReason	Reason for Error	string	This is the reason for an error if given.
errorString	Error String	string	This is the error message, synonymous to attribute errReason
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_CHECKPOINT_DEV_INIT_ERROR

Description: Checkpoint device initialization error. Checkpoint device can not be monitored

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_FILE_RENAME_FAILURE

Description: FortiSIEM Checkpoint module failed to rename file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_CHECKPOINT_FWLOGHANDLER_ERROR

Description: Checkpoint LEA handler protocol error. Checkpoint device can not be monitored

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_FWLOGHANDLER_INIT_ERROR

Description: Checkpoint OPSEC log handler initialization error. Checkpoint device can not be monitored

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_HTTP_ERROR

Description: Checkpoint module failed to connect to App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_CHECKPOINT_LOGHANDLER_ERROR

Description: Checkpoint OPSEC log handler internal error

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CHECKPOINT_PROCESS_GET_FAILED

Description: Checkpoint module failed to get its parent process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CHECKPOINT_TESTCONN_ERROR

Description: Checkpoint test connectivity error. Checkpoint device can not be discovered

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_CHECKPOINT_UNABLE_PARSE_XML

Description: Checkpoint module unable to parse device credential XML received from App Server

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_CHECKIN_QUERY_THREADS_FAILED

Description: Failed to checkin query threads

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_CHECKOUT_QUERY_THREADS_FAILED

Description: Failed to checkout query threads

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_DISK_UTILS_PER_STORAGE_TIER

Description: ClickHouse disk utils per storage tier

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
diskType	Disk Type	string	
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_CLICKHOUSE_DROP_PARTITION_FAILED

Description: Failed to drop ClickHouse partitions

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
dbPartition	DB Partition	string	
errReason	Reason for Error	string	This is the reason for an error if given.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_DROP_PARTITION_STARTED

Description: Drop ClickHouse partition started

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
dbPartition	DB Partition	string	
command	Command	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_DROP_PARTITION_SUCCEEDED

Description: Drop ClickHouse partition successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
dbPartition	DB Partition	string	
command	Command	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

All Logs Page 2

Every FortiSIEM internally generated event log regardless of category

- PH_CLICKHOUSE_GET_ONLINE_NODE_FAILED
- PH_CLICKHOUSE_GET_PARTITIONS_FAILED
- PH_CLICKHOUSE_GET_SHARDS_FAILED
- PH_CLICKHOUSE_GET_STORAGE_STATS_FAILED
- PH_CLICKHOUSE_GET_STORAGE_TIER_FAILED
- PH_CLICKHOUSE_INSERTION_DROP_EVENTS
- PH_CLICKHOUSE_INSERTION_EPS
- PH_CLICKHOUSE_JSON_ENCODER_EPS
- PH_CLICKHOUSE_JSON_ENCODER_EPS_PER_THREAD
- PH_CLICKHOUSE_LOG_INTEGRITY_ACTIVE_CONSOLIDATION
- PH_CLICKHOUSE_LOG_INTEGRITY_CALCULATE_REQUEST_PARSE_FAILED
- PH_CLICKHOUSE_LOG_INTEGRITY_CALCULATE_REQUEST_STARTED
- PH_CLICKHOUSE_LOG_INTEGRITY_CANDIDATE_PARTITIONS
- PH_CLICKHOUSE_LOG_INTEGRITY_CONSOLIDATION_DATE
- PH_CLICKHOUSE_LOG_INTEGRITY_CONSOLIDATION_STATUS_CHANGE
- PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_DONE
- PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_STARTED
- PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_STOPPED
- PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_TIMER
- PH_CLICKHOUSE_LOG_INTEGRITY_DB_QUERY_FAILED
- PH_CLICKHOUSE_LOG_INTEGRITY_EMPTY_PARTITION_CHECKSUM
- PH_CLICKHOUSE_LOG_INTEGRITY_EXEC_FAILED
- PH_CLICKHOUSE_LOG_INTEGRITY_MIN_MAX_QUERY_FAILED
- PH_CLICKHOUSE_LOG_INTEGRITY_OPTIMIZE_COMMAND_FAILED
- PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_CONSOLIDATION_DONE
- PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_CONSOLIDATION_STARTED
- PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_UPDATED_AFTER_CHECKSUM
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_MISMATCH
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_MISMATCH_REPLICAS
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_PARTITION_INFO_EMPTY
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_REQUEST_PARSE_FAILED
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_EMPTY
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_ERROR
- PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_PARSE_FAILED
- PH_CLICKHOUSE_MOVE_PARTITION_FAILED
- PH_CLICKHOUSE_MOVE_PARTITION_STARTED
- PH_CLICKHOUSE_MOVE_PARTITION_SUCCEEDED

- PH_CLICKHOUSE_NOT_REACHABLE
- PH_CLICKHOUSE_QUERY_REDIS_CONN_FAILURE
- PH_CLICKHOUSE_QUERY_REDIS_GET_FAILURE
- PH_CLICKHOUSE_QUERY_UNCOMPRESS_FAILURE
- PH_CLICKHOUSE_QUERY_ZLIB_INIT_FAILURE
- PH_CLICKHOUSE_RESOURCE_TRACKER_QUERY_CHECKIN
- PH_CLICKHOUSE_RESOURCE_TRACKER_QUERY_CHECKOUT
- PH_CLICKHOUSE_RESOURCE_TRACKER_THREADS_CHECKIN
- PH_CLICKHOUSE_RESOURCE_TRACKER_THREADS_CHECKOUT
- PH_CLICKHOUSE_ROUND_ROBIN_INSERTION
- PH_CLICKHOUSE_ROUND_ROBIN_QUERY
- PH_CLICKHOUSE_STORAGE_FREE_SPACE_CRITICAL
- PH_CLICKHOUSE_STORAGE_FREE_SPACE_LOW
- PH_CLICKHOUSE_STORAGE_UTILS_PER_ORG_PER_DAY
- PH_CLICKHOUSE_WRITE_FAILED
- PH_CLICKHOUSE_BUILD_QUERY_DIST_SQL_COMMAND_FAILURE
- PH_CLI_ERROR
- PH_CLUSTER_COLLECT_ALL_IP_FAILED
- PH_CLUSTER_COLLECT_CONFIG_DATA_FAILED
- PH_CLUSTER_CONFIG_SSH_KEY_FAILED
- PH_CLUSTER_GET_FW_IP_FAILED
- PH_CLUSTER_GET_TASK_FAILED
- PH_CLUSTER_NOT_SUPPORT_TASK
- PH_CLUSTER_NOT_VALID_FELLOWER
- PH_CLUSTER_NO_LICENSE
- PH_CLUSTER_RELOAD_CONFIG_FAILED
- PH_CLUSTER_RM_DB_FAILED
- PH_CLUSTER_RUN_COMMAND_FAILED
- PH_CLUSTER_SCRIPT_FAILED
- PH_CLUSTER_SEND_TASK_FAILED
- PH_CLUSTER_SSH_KEY_IS_WRONG
- PH_CLUSTER_TASK_DATA_EMPTY
- PH_CLUSTER_TASK_INFO_IS_WRONG
- PH_CLUSTER_TASK_NOT_CONTAIN_LIC
- PH_CLUSTER_UPDATE_CONFIG_ERROR
- PH_COLLECTOR_CLOCK_SKEW
- PH_COLLECTOR_DOWN
- PH_COLLECTOR_EVENT_ARRIVAL_DELAYED
- PH_COLLECTOR_EVENT_ARRIVAL_OK
- PH_COLLECTOR_EVENT_STORE_DELAYED
- PH_COLLECTOR_EVENT_STORE_OK
- PH_COLLECTOR_LICENSE_UPDATE
- PH_COLLECTOR_UP

- PH_CREATE_TEMP_FILE_FAILURE
- PH_CYBERARK_INIT_ERROR
- PH_DATAINTEGRITY_PASSPHRASE_LOAD_ERROR
- PH_DATAINTEGRITY_SIGNER_ERROR
- PH_DATAINTEGRITY_UTILS_ERROR
- PH_DATAINTEGRITY_VERIFIER_ERROR
- PH_DATAMANAGER_CLICKHOUSE_HTTP_UPLOAD_ERROR
- PH_DATAMANAGER_CLUSTER_ENCODE_ERROR
- PH_DATAMANAGER_CLUSTER_INIT_ERROR
- PH_DATAMANAGER_CLUSTER_WAIT_ERROR
- PH_DATAMANAGER_CLUSTER_WRITER_ERROR
- PH_DATAMANAGER_DASHBOARD_RESPONSE_ERROR
- PH_DATAMANAGER_ELASTICWRITER_ERROR
- PH_DATAMANAGER_EVTATTR_ERROR
- PH_DATAMANAGER_EVTCACHE_DUPLICATE_ERROR
- PH_DATAMANAGER_EVTCACHE_GET_ERROR
- PH_DATAMANAGER_EVTCACHE_PARSE_ERROR
- PH_DATAMANAGER_EVTDBNOTIFIER_ERROR
- PH_DATAMANAGER_EVTIDX_CORRUPT_ERROR
- PH_DATAMANAGER_EVTIDX_MERGE_ERROR
- PH_DATAMANAGER_EVTIDX_QUERY_ERROR
- PH_DATAMANAGER_EVTIDX_READ_BLOCK_ERROR
- PH_DATAMANAGER_EVTIDX_READ_KEY_ERROR
- PH_DATAMANAGER_EVTIDX_READ_POST_ERROR
- PH_DATAMANAGER_EVTIDX_WRITE_ERROR
- PH_DATAMANAGER_EVTIDX_WRITE_KEY_ERROR
- PH_DATAMANAGER_EVTIDX_WRITE_POST_ERROR
- PH_DATAMANAGER_EVTLOADER_ERROR
- PH_DATAMANAGER_EVTWRITER_ERROR
- PH_DATAMANAGER_EXPORT_ERROR
- PH_DATAMANAGER_FILE_READ_FAILURE
- PH_DATAMANAGER_FILE_RENAME_FAILURE
- PH_DATAMANAGER_FILE_SIGN_ERROR
- PH_DATAMANAGER_FILE_WRITE_FAILURE
- PH_DATAMANAGER_GET_SIGN_ERROR
- PH_DATAMANAGER_GLOBAL_CACHE_MISSING
- PH_DATAMANAGER_HDFSWRITER_ERROR
- PH_DATAMANAGER_HTTP_UPLOAD_ERROR
- PH_DATAMANAGER_INIT_ERROR
- PH_DATAMANAGER_INTEGRITY_CHECK_ERROR
- PH_DATAMANAGER_INTEGRITY_RESPONSE_ERROR
- PH_DATAMANAGER_INVALID_LOG_FILE
- PH_DATAMANAGER_IP_TYPE_INVALID

- PH_DATAMANAGER_KAFKAWRITER_CONFIG_ERROR
- PH_DATAMANAGER_KAFKAWRITER_ERROR
- PH_DATAMANAGER_LOG_BUFFER_PAUSED_LOW_SPACE
- PH_DATAMANAGER_LOG_BUFFER_PAUSED_STATFS_FAILURE
- PH_DATAMANAGER_LOG_BUFFER_RESUMED
- PH_DATAMANAGER_PUT_SIGN_ERROR
- PH_DATAMANAGER_QUERY_EXPR_ERROR
- PH_DATAMANAGER_QUERY_RESPONSE_ERROR
- PH_DATAMANAGER_REDIS_KEY_NOT_EXIST
- PH_DATAMANAGER_SUMMARYWRITER_ERROR
- PH_DATAMGR_BAD_EVTBLKIDX_FILE
- PH_DATAMGR_BAD_SEGMENT
- PH_DATAMGR_INDEX_MERGE_FAILED
- PH_DATAMGR_INDEX_MERGE_FAILED_INDEX
- PH_DATAMGR_INDEX_MERGE_FAILED_INDEX_GROUP
- PH_DATAMGR_SEGMENT_MERGE_ERROR
- PH_DATAMGR_SEGMENT_MERGE_FAILED
- PH_DATAMGR_UNABLE_FLUSH_INDEX
- PH_DATAMGR_UNABLE_OPEN_EVTBLK_FILE
- PH_DATAPURGER_ARCHIVE_TASK_ERROR
- PH_DATAPURGER_CMD_FAILURE
- PH_DATAPURGER_DR_ES_RESTORE_FAILED
- PH_DATAPURGER_DR_ES_ROLE_UNKNOWN
- PH_DATAPURGER_DR_ES_SNAPSHOTS_GET_FAILED
- PH_DATAPURGER_DR_ES_SNAPSHOT_DELETION_FAILED
- PH_DATAPURGER_DR_ES_SNAPSHOT_FAILED
- PH_DATAPURGER_DUCHECKER_ERROR
- PH_DATAPURGER_ENFORCE_ERROR
- PH_DATAPURGER_EVAL_ERROR
- PH_DATAPURGER_HTTP_UPLOAD_ERROR
- PH_DATAPURGER_INIT_ERROR
- PH_DATAPURGER_OPEN_FILE_ERROR
- PH_DATAPURGER_PARSE_XML_ERROR
- PH_DATAPURGER_POLICY_ERROR
- PH_DATAPURGER_RESPONSE_ERROR
- PH_DATAPURGER_STORAGE_POLICY_CLICKHOUSE_NODES_EMPTY
- PH_DATA_CLUSTER_ALL_COORDINATOR_DOWN
- PH_DATA_CLUSTER_BUSY
- PH_DATA_CLUSTER_CLICKHOUSE_CONFIG_NO_PORT
- PH_DATA_CLUSTER_COORDINATOR_DOWN
- PH_DATA_CLUSTER_COORDINATOR_UP
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_HTTPPORT
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_IP

- PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_JAVAPORT
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NAME
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NUMREPLICAS
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NUMSHARD
- PH_DATA_CLUSTER_ELASTIC_CONFIG_NULL
- PH_DATA_CLUSTER_ELASTIC_CONFIG_WRONG_FORMAT
- PH_DATA_CLUSTER_ELASTIC_EVENTID_NOT_FOUND
- PH_DATA_CLUSTER_ELASTIC_HTTP_CLIENT_FAIL
- PH_DATA_CLUSTER_ELASTIC_HTTP_CMD_FAIL
- PH_DATA_CLUSTER_ELASTIC_INDEX_FAIL
- PH_DATA_CLUSTER_ELASTIC_INDEX_RESEND_FAIL
- PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FAIL
- PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FIRST_FAIL
- PH_DATA_CLUSTER_ELASTIC_INDEX_UPLOAD_FAIL
- PH_DATA_CLUSTER_ELASTIC_WRONG_JSON_FORMAT
- PH_DATA_CLUSTER_GET_HOSTNAME_FAIL
- PH_DATA_CLUSTER_HDFS_CONFIG_NO_PORT
- PH_DATA_CLUSTER_HDFS_CONFIG_NO_SERVER
- PH_DATA_CLUSTER_HDFS_CONFIG_NO_YARN_PORT
- PH_DATA_CLUSTER_HDFS_CONFIG_NO_YARN_SERVER
- PH_DATA_CLUSTER_HDFS_CONFIG_NULL
- PH_DATA_CLUSTER_HDFS_HTTP_CMD_FAIL
- PH_DATA_CLUSTER_HDFS_LISTSTATUS_FAIL
- PH_DATA_CLUSTER_HDFS_SEND_FAIL
- PH_DATA_CLUSTER_HDFS_UPLOAD_FAIL
- PH_DATA_CLUSTER_JSON_GET_ATTRIBUTE_NAME_FAIL
- PH_DEVICE_NOT_ADDED
- PH_DEV_FAIL_TO_PULL_EVENTS
- PH_DEV_MON_ACME_PACKET_SESSION_AGENT_STATUS
- PH_DEV_MON_ACME_PACKET_SYS_STATUS
- PH_DEV_MON_APP_APACHE_MET
- PH_DEV_MON_APP_ASPNET_MET
- PH_DEV_MON_APP_DHCP_MET
- PH_DEV_MON_APP_DNS_MET
- PH_DEV_MON_APP_ICA_SESS_MET
- PH_DEV_MON_APP_IIS_MET
- PH_DEV_MON_APP_MSEXCH_ERR_MET
- PH_DEV_MON_APP_MSEXCH_ISDB_INST_MET
- PH_DEV_MON_APP_MSEXCH_ISDB_MET
- PH_DEV_MON_APP_MSEXCH_MBOX_MET
- PH_DEV_MON_APP_MSEXCH_MET
- PH_DEV_MON_APP_MSEXCH_REPL_MET
- PH_DEV_MON_APP_MSEXCH_SMTP_MET

- PH_DEV_MON_APP_MSEXCH_STORE_INTF_MET
- PH_DEV_MON_APP_MSEXCH_SUBMIT_MET
- PH_DEV_MON_APP_MSEXCH_TRANS_MET
- PH_DEV_MON_APP_MSEXCH_WS_MET
- PH_DEV_MON_APP_NTDS_MET
- PH_DEV_MON_ARUBA_WLAN_RADIO_METRIC
- PH_DEV_MON_AUTH_STATS
- PH_DEV_MON_AUTO_SVC_START_TO_STOP
- PH_DEV_MON_AUTO_SVC_STOP
- PH_DEV_MON_AUTO_SVC_STOP_TO_START
- PH_DEV_MON_BC_PROXY_METRIC
- PH_DEV_MON_BGP_NBR_STATUS
- PH_DEV_MON_BOX_FILE_CREATE
- PH_DEV_MON_BOX_FILE_DELETE
- PH_DEV_MON_BOX_FILE_MODIFY
- PH_DEV_MON_BOX_FILE_SHARE
- PH_DEV_MON_CBQOS_CMSTAT
- PH_DEV_MON_CBQOS_POLICESTAT
- PH_DEV_MON_CBQOS_QUEUESTAT
- PH_DEV_MON_CCM_CTI_STAT
- PH_DEV_MON_CCM_CTI_STAT_CHANGE
- PH_DEV_MON_CCM_DEL_CTI
- PH_DEV_MON_CCM_DEL_GW
- PH_DEV_MON_CCM_DEL_H323
- PH_DEV_MON_CCM_DEL_MEDIA
- PH_DEV_MON_CCM_DEL_SIP_TRUNK
- PH_DEV_MON_CCM_DEL_VM
- PH_DEV_MON_CCM_GLOBAL_INFO
- PH_DEV_MON_CCM_GW_STAT
- PH_DEV_MON_CCM_GW_STAT_CHANGE
- PH_DEV_MON_CCM_H323_STAT
- PH_DEV_MON_CCM_H323_STAT_CHANGE
- PH_DEV_MON_CCM_MEDIA_STAT
- PH_DEV_MON_CCM_MEDIA_STAT_CHANGE
- PH_DEV_MON_CCM_NEW_CTI
- PH_DEV_MON_CCM_NEW_GW
- PH_DEV_MON_CCM_NEW_H323
- PH_DEV_MON_CCM_NEW_MEDIA
- PH_DEV_MON_CCM_NEW_SIP_TRUNK
- PH_DEV_MON_CCM_NEW_VM
- PH_DEV_MON_CCM_SIP_TRUNK_STAT
- PH_DEV_MON_CCM_VM_STAT
- PH_DEV_MON_CCM_VM_STAT_CHANGE

- PH_DEV_MON_CHANGE_CUST_CONFIG
- PH_DEV_MON_CHANGE_INST_SW
- PH_DEV_MON_CHANGE_RUN_CONFIG
- PH_DEV_MON_CHANGE_RUN_SW
- PH_DEV_MON_CHANGE_STARTUP_CONFIG
- PH_DEV_MON_CISCO_NBAR_STAT
- PH_DEV_MON_CISCO_RAS_VPN_MET
- PH_DEV_MON_CISCO_VPN_P1_TUNNEL_MET
- PH_DEV_MON_CISCO_VPN_P2_TUNNEL_MET
- PH_DEV_MON_CISCO_WLAN_RADIO_METRIC
- PH_DEV_MON_CITRIX_SDWAN_INTF
- PH_DEV_MON_CITRIX_SDWAN_LINK
- PH_DEV_MON_CLARION_ARRAY_UTIL
- PH_DEV_MON_CLARION_DISK_HEALTH
- PH_DEV_MON_CLARION_HOST_CONN
- PH_DEV_MON_CLARION_LUN_UTIL
- PH_DEV_MON_CLARION_PER_HOST_LUN_UTIL
- PH_DEV_MON_CLARION_PORT_UTIL
- PH_DEV_MON_CLARION_RG_UTIL
- PH_DEV_MON_CLARION_SP_UTIL
- PH_DEV_MON_CLARION_STORAGE_USAGE
- PH_DEV_MON_CLARION_STORE_POOL_UTIL
- PH_DEV_MON_CLARION_UNREG_HOST
- PH_DEV_MON_CLOUD_SERVICE_HEARTBEAT
- PH_DEV_MON_CMDB_DISK_PRUNE_FAILED
- PH_DEV_MON_CMDB_DISK_PRUNE_SUCCESS
- PH_DEV_MON_CUST_FILE_CHANGE_ATTRIB
- PH_DEV_MON_CUST_FILE_CHANGE_CONTENT
- PH_DEV_MON_CUST_FILE_CREATE
- PH_DEV_MON_CUST_FILE_DELETE
- PH_DEV_MON_CUST_FILE_SCAN
- PH_DEV_MON_CUST_TARGET_FILE_CHANGE
- PH_DEV_MON_DATASTORE_UTIL
- PH_DEV_MON_DCDIAG
- PH_DEV_MON_DDNS_UPDATE_STAT
- PH_DEV_MON_DELLFORCE10_EXT_INTF_UTIL
- PH_DEV_MON_DELL_BLADE_POWER_STATUS
- PH_DEV_MON_DELL_BLADE_PSU_STATUS
- PH_DEV_MON_DELTA_CONFIG
- PH_DEV_MON_DGA_DETECTED
- PH_DEV_MON_DHCP_SUBNET_USAGE
- PH_DEV_MON_DISK_IO_UTIL
- PH_DEV_MON_DISK_MON_SKIP

- PH_DEV_MON_DNS_CLUST_REPL_STAT
- PH_DEV_MON_DNS_PERF_STAT
- PH_DEV_MON_DNS_ZONETX_MET
- PH_DEV_MON_DST_AD_REPL_STAT
- PH_DEV_MON_EBS_METRIC
- PH_DEV_MON_EC2_INSTANCE_DOWN
- PH_DEV_MON_EC2_INSTANCE_UP
- PH_DEV_MON_EC2_METRIC
- PH_DEV_MON EMC_DATADOMAIN_DISK_PERF
- PH_DEV_MON EMC_DATADOMAIN_OVERALL_PERF
- PH_DEV_MON_EQL_CONN_MET
- PH_DEV_MON_EQL_DISK_HEALTH
- PH_DEV_MON_EQL_DISK_MET
- PH_DEV_MON_EQL_GROUP_MET
- PH_DEV_MON_ESX_DATASTORE_IO
- PH_DEV_MON_ESX_DISK_IO
- PH_DEV_MON_ESX_DISK_UTIL
- PH_DEV_MON_ESX_STATE
- PH_DEV_MON_ESX_UPTIME
- PH_DEV_MON_EUM_FAIL
- PH_DEV_MON_EUM_INTERNAL_ERR
- PH_DEV_MON_EUM_STATUS
- PH_DEV_MON_EUM_SUCCESS
- PH_DEV_MON_F5_ACTIVE_CONN
- PH_DEV_MON_F5_LTM_NODE_STAT
- PH_DEV_MON_F5_LTM_POOL_MEMBER_STAT
- PH_DEV_MON_F5_LTM_POOL_STAT
- PH_DEV_MON_F5_LTM_VIRT_ADDR_STAT
- PH_DEV_MON_F5_LTM_VIRT_SERVER_STAT
- PH_DEV_MON_F5_NEW_CONN
- PH_DEV_MON_F5_RAM_CACHE
- PH_DEV_MON_F5_THROUGHPUT
- PH_DEV_MON_F5_TMM_MEM_UTIL
- PH_DEV_MON_FGT_SEC_POSTURE_DETAILS
- PH_DEV_MON_FGT_SEC_POSTURE_DETECTED_ENDPOINTS
- PH_DEV_MON_FGT_SEC_POSTURE_FABRIC_GRADE
- PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_GRADE
- PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_STATS
- PH_DEV_MON_FGT_SEC_POSTURE_PER_DEVICE_STATS
- PH_DEV_MON_FGT_USER_INFO
- PH_DEV_MON_FILE_CONTENT_CHANGE
- PH_DEV_MON_FIREAMP_DISCOVERY_CLIENT_APP
- PH_DEV_MON_FIREAMP_DISCOVERY_NETWORK_PROTOCOL

- PH_DEV_MON_FIREAMP_DISCOVERY_OS_FINGERPRINT
- PH_DEV_MON_FIREAMP_DISCOVERY_SERVER
- PH_DEV_MON_FIREAMP_FILE
- PH_DEV_MON_FIREAMP_IMPACT_FLAG
- PH_DEV_MON_FIREAMP_INTRUSION
- PH_DEV_MON_FIREAMP_MALWARE
- PH_DEV_MON_FIREAMP_USER_LOGIN
- PH_DEV_MON_FORTIAP_INTF_UTIL
- PH_DEV_MON_FORTIAP_PERF
- PH_DEV_MON_FORTIAP_STAT
- PH_DEV_MON_FORTIGATE_INTF_UTIL
- PH_DEV_MON_FORTIGATE_PERF
- PH_DEV_MON_FORTIMAIL_SESSION_COUNT
- PH_DEV_MON_FORTIMAIL_SYS_LOAD
- PH_DEV_MON_FORTINET_PROCESSOR_USAGE
- PH_DEV_MON_FORTINET_QOS
- PH_DEV_MON_FORTISWITCH_PERF
- PH_DEV_MON_FORTIWLC_QOS_STAT
- PH_DEV_MON_FORTIWLC_STATIONS
- PH_DEV_MON_FORTIWLC_SYS_THRUPUT
- PH_DEV_MON_FPC_LIEBERT_METRIC
- PH_DEV_MON_FW_CONN_UTIL
- PH_DEV_MON_GITHUB_BRANCH_EVENT
- PH_DEV_MON_GITHUB_COMMIT
- PH_DEV_MON_GITHUB_EVENT
- PH_DEV_MON_GITHUB_FORK_REPOSITORY_EVENT
- PH_DEV_MON_GITHUB_ISSUE_EVENT
- PH_DEV_MON_GITHUB_MEMBER_EVENT
- PH_DEV_MON_GITHUB_ORG_EVENT
- PH_DEV_MON_GITHUB_PROJECT_EVENT
- PH_DEV_MON_GITHUB_PULL_REQUEST_EVENT
- PH_DEV_MON_GITHUB_PULL_REQUEST_REVIEW_EVENT
- PH_DEV_MON_GITHUB_REPOSITORY_EVENT
- PH_DEV_MON_GITHUB_TAG_EVENT
- PH_DEV_MON_GLASSFISH_APP
- PH_DEV_MON_GLASSFISH_CONN_STAT
- PH_DEV_MON_GLASSFISH_CPU
- PH_DEV_MON_GLASSFISH_DB_POOL
- PH_DEV_MON_GLASSFISH_EJB
- PH_DEV_MON_GLASSFISH_JMS
- PH_DEV_MON_GLASSFISH_MEMORY
- PH_DEV_MON_GLASSFISH_REQUEST_PROCESSOR
- PH_DEV_MON_GLASSFISH_SERVLET

- PH_DEV_MON_GLASSFISH_SESSION
- PH_DEV_MON_GLASSFISH_THREAD_POOL
- PH_DEV_MON_HARDWARE_STATUS
- PH_DEV_MON_HOST_PERF_STATE
- PH_DEV_MON_HVAC_LIEBERT_METRIC
- PH_DEV_MON_HW_AIRFLOW
- PH_DEV_MON_HW_AMP
- PH_DEV_MON_HW_AUDIO
- PH_DEV_MON_HW_CAMERA_MOTION
- PH_DEV_MON_HW_CHASSIS_COMP_STAT
- PH_DEV_MON_HW_CURRENT
- PH_DEV_MON_HW_DEWPT
- PH_DEV_MON_HW_DOOR_SWITCH
- PH_DEV_MON_HW_DRY_CONTACT
- PH_DEV_MON_HW_FAN_SPEED
- PH_DEV_MON_HW_HUMIDITY
- PH_DEV_MON_HW_POWER
- PH_DEV_MON_HW_PS_STAT
- PH_DEV_MON_HW_STACK_UNIT
- PH_DEV_MON_HW_STATUS
- PH_DEV_MON_HW_STATUS_AIRFLOW_CRIT
- PH_DEV_MON_HW_STATUS_AIRFLOW_WARN
- PH_DEV_MON_HW_STATUS_ALARMDEVICE_CRIT
- PH_DEV_MON_HW_STATUS_ALARMDEVICE_WARN
- PH_DEV_MON_HW_STATUS_AMP_CRIT
- PH_DEV_MON_HW_STATUS_AMP_WARN
- PH_DEV_MON_HW_STATUS_AUDIO_CRIT
- PH_DEV_MON_HW_STATUS_AUDIO_WARN
- PH_DEV_MON_HW_STATUS_BATTERY_CRIT
- PH_DEV_MON_HW_STATUS_BATTERY_WARN
- PH_DEV_MON_HW_STATUS_CAMERA_MOTION_CRIT
- PH_DEV_MON_HW_STATUS_CAMERA_MOTION_WARN
- PH_DEV_MON_HW_STATUS_DEWPT_CRIT
- PH_DEV_MON_HW_STATUS_DEWPT_WARN
- PH_DEV_MON_HW_STATUS_DISK_CRIT
- PH_DEV_MON_HW_STATUS_DISK_WARN
- PH_DEV_MON_HW_STATUS_DOOR_SWITCH_CRIT
- PH_DEV_MON_HW_STATUS_DOOR_SWITCH_WARN
- PH_DEV_MON_HW_STATUS_DRY_CONTACT_CRIT
- PH_DEV_MON_HW_STATUS_DRY_CONTACT_WARN
- PH_DEV_MON_HW_STATUS_FAN_CRIT
- PH_DEV_MON_HW_STATUS_FAN_WARN
- PH_DEV_MON_HW_STATUS_FILESYSTEM_CRIT

- PH_DEV_MON_HW_STATUS_FILESYSTEM_WARN
- PH_DEV_MON_HW_STATUS_GEN_NUMERIC_SENSOR_CRIT
- PH_DEV_MON_HW_STATUS_GEN_NUMERIC_SENSOR_WARN
- PH_DEV_MON_HW_STATUS_GEN_STATE_SENSOR_CRIT
- PH_DEV_MON_HW_STATUS_GEN_STATE_SENSOR_WARN
- PH_DEV_MON_HW_STATUS_HUMIDITY_CRIT
- PH_DEV_MON_HW_STATUS_HUMIDITY_WARN
- PH_DEV_MON_HW_STATUS_INPUTCONTACT_CRIT
- PH_DEV_MON_HW_STATUS_INPUTCONTACT_WARN
- PH_DEV_MON_HW_STATUS_LCC_CRIT
- PH_DEV_MON_HW_STATUS_LCC_WARN
- PH_DEV_MON_HW_STATUS_LINK_CRIT
- PH_DEV_MON_HW_STATUS_LINK_WARN
- PH_DEV_MON_HW_STATUS_MEMBEACON_CRIT
- PH_DEV_MON_HW_STATUS_MEMBEACON_WARN
- PH_DEV_MON_HW_STATUS_MEMORY_CRIT
- PH_DEV_MON_HW_STATUS_MEMORY_WARN
- PH_DEV_MON_HW_STATUS_MEMOUTLET_CRIT
- PH_DEV_MON_HW_STATUS_MEMOUTLET_WARN
- PH_DEV_MON_HW_STATUS_MEMOUTPUT_CRIT
- PH_DEV_MON_HW_STATUS_MEMOUTPUT_WARN
- PH_DEV_MON_HW_STATUS_MEMSENSOR_CRIT
- PH_DEV_MON_HW_STATUS_MEMSENSOR_WARN
- PH_DEV_MON_HW_STATUS_MISC_CRIT
- PH_DEV_MON_HW_STATUS_MISC_WARN
- PH_DEV_MON_HW_STATUS_OUTLET_CRIT
- PH_DEV_MON_HW_STATUS_OUTLET_WARN
- PH_DEV_MON_HW_STATUS_OUTPUTRELAY_CRIT
- PH_DEV_MON_HW_STATUS_OUTPUTRELAY_WARN
- PH_DEV_MON_HW_STATUS_PORT_CRIT
- PH_DEV_MON_HW_STATUS_PORT_WARN
- PH_DEV_MON_HW_STATUS_POWERSUPPLY_CRIT
- PH_DEV_MON_HW_STATUS_POWERSUPPLY_WARN
- PH_DEV_MON_HW_STATUS_POWER_ENCLOSURE_CRIT
- PH_DEV_MON_HW_STATUS_POWER_ENCLOSURE_WARN
- PH_DEV_MON_HW_STATUS_PROBE_CRIT
- PH_DEV_MON_HW_STATUS_PROBE_WARN
- PH_DEV_MON_HW_STATUS_SLOT_CRIT
- PH_DEV_MON_HW_STATUS_SLOT_WARN
- PH_DEV_MON_HW_STATUS_STACKUNIT_CRIT
- PH_DEV_MON_HW_STATUS_STACKUNIT_WARN
- PH_DEV_MON_HW_STATUS_TEMP_CRIT
- PH_DEV_MON_HW_STATUS_TEMP_WARN

- PH_DEV_MON_HW_STATUS_VOLTAGE_CRIT
- PH_DEV_MON_HW_STATUS_VOLTAGE_WARN
- PH_DEV_MON_HW_TEMP
- PH_DEV_MON_HW_VOLTAGE
- PH_DEV_MON_HYPERV_CPU_GUEST_VIRTUAL_PROC
- PH_DEV_MON_HYPERV_CPU_LOGICAL_PROC
- PH_DEV_MON_HYPERV_CPU_ROOT_VIRTUAL_PROC
- PH_DEV_MON_HYPERV_MEM_OVERALL
- PH_DEV_MON_HYPERV_MEM_PARTITION
- PH_DEV_MON_HYPERV_MEM_PARTITION_PER_VM
- PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION
- PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION_ROOT
- PH_DEV_MON_HYPERV_MEM_VID_PARTITION
- PH_DEV_MON_HYPERV_MEM_VID_PARTITION_PER_VM
- PH_DEV_MON_HYPERV_NET_LEGACY_ADAPTER
- PH_DEV_MON_HYPERV_NET_VIRTUAL_ADAPTER
- PH_DEV_MON_HYPERV_NET_VIRTUAL_SWITCH
- PH_DEV_MON_HYPERV_OVERALL_HEALTH
- PH_DEV_MON_HYPERV_OVERALL_SYSINFO
- PH_DEV_MON_HYPERV_STORAGE_LOGICAL_DISK
- PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_IDE_CONTROLLER
- PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_STORAGE
- PH_DEV_MON_INCOMING_EXCEED_GUARANTEED
- PH_DEV_MON_INTF_ADMIN_DOWN_TO_UP
- PH_DEV_MON_INTF_ADMIN_UP_TO_DOWN
- PH_DEV_MON_INTF_OPER_DOWN_TO_UP
- PH_DEV_MON_INTF_OPER_UP_TO_DOWN
- PH_DEV_MON_INTF_USAGE_TOTAL
- PH_DEV_MON_IPSLA_HTTP_MET
- PH_DEV_MON_IPSLA_ICMP_MET
- PH_DEV_MON_IPSLA_MET
- PH_DEV_MON_IPSLA_UDP_MET
- PH_DEV_MON_IPSLA_VOIP_MET
- PH_DEV_MON_IRONPORT_MAIL_USAGE
- PH_DEV_MON_ISILON_CLUSTER_HEALTH
- PH_DEV_MON_ISILON_CLUSTER_MEMBERSHIP_CHANGE
- PH_DEV_MON_ISILON_CLUSTER_QUOTA
- PH_DEV_MON_ISILON_CLUSTER_SNAPSHOT
- PH_DEV_MON_ISILON_NODE_DISK_PERF
- PH_DEV_MON_ISILON_NODE_HEALTH
- PH_DEV_MON_ISILON_NODE_PROTO_PERF
- PH_DEV_MON_JBOSS_APP
- PH_DEV_MON_JBOSS_CPU

- PH_DEV_MON_JBOSS_DB_POOL
- PH_DEV_MON_JBOSS_EJB
- PH_DEV_MON_JBOSS_MEMORY
- PH_DEV_MON_JBOSS_REQUEST_PROCESSOR
- PH_DEV_MON_JBOSS_SERVLET
- PH_DEV_MON_JBOSS_SESSION
- PH_DEV_MON_JBOSS_THREAD_POOL
- PH_DEV_MON_LOG_ALL_DEVICE_DELAY_HIGH
- PH_DEV_MON_LOG_ALL_DEVICE_DELAY_LOW
- PH_DEV_MON_LOG_DEVICE_DELAY_HIGH
- PH_DEV_MON_LOG_DEVICE_DELAY_LOW
- PH_DEV_MON_MANUAL_SVC_START_TO_STOP
- PH_DEV_MON_MANUAL_SVC_STOP
- PH_DEV_MON_MANUAL_SVC_STOP_TO_START
- PH_DEV_MON_NETAPP_AGGR_MET
- PH_DEV_MON_NETAPP_CIFS_MET
- PH_DEV_MON_NETAPP_CP_MET
- PH_DEV_MON_NETAPP_DISK_HEALTH
- PH_DEV_MON_NETAPP_DISK_MET
- PH_DEV_MON_NETAPP_FCP_MET
- PH_DEV_MON_NETAPP_ISCSI_MET
- PH_DEV_MON_NETAPP_LUN_MET
- PH_DEV_MON_NETAPP_NFS3_MET
- PH_DEV_MON_NETAPP_NFS4_MET
- PH_DEV_MON_NETAPP_NFS_MET
- PH_DEV_MON_NETAPP_VOL_MET
- PH_DEV_MON_NETBOTZ_HW_EMS_STATUS
- PH_DEV_MON_NETBOTZ_HW_MODULE_SENSOR
- PH_DEV_MON_NETBOTZ_HW_PROBE
- PH_DEV_MON_NETSCALER_APP_FW
- PH_DEV_MON_NETSCALER_SERVICE
- PH_DEV_MON_NETSCALER_VIRT_SERVER
- PH_DEV_MON_NET_INTF_UTIL
- PH_DEV_MON_NIMBLE_GLOBAL_STAT
- PH_DEV_MON_NUTANIX_CLUSTER_STATUS
- PH_DEV_MON_NUTANIX_CONTAINER_INFO
- PH_DEV_MON_NUTANIX_CTRLR_VM_RESOURCE
- PH_DEV_MON_NUTANIX_DISK_STATUS
- PH_DEV_MON_NUTANIX_DISK_TEMP
- PH_DEV_MON_NUTANIX_SERVICE_STATUS
- PH_DEV_MON_NUTANIX_STORAGE_POOL_INFO
- PH_DEV_MON_OMI_PING_STAT
- PH_DEV_MON OSPF_NBR_STATUS

- [PH_DEV_MON_PANASONIC_AERO_LOG_MON_STATUS](#)
- [PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_HIGH](#)
- [PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_LOW](#)
- [PH_DEV_MON_PERFMON_DEVICE_DELAY_HIGH](#)

EventType: PH_CLICKHOUSE_GET_ONLINE_NODE_FAILED

Description: ClickHouse getting online node failed

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_GET_PARTITIONS_FAILED

Description: Failed to get ClickHouse partitions

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_GET_SHARDS_FAILED

Description: Failed to get ClickHouse shards

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_GET_STORAGE_STATS_FAILED

Description: Failed to get ClickHouse storage stats

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_GET_STORAGE_TIER_FAILED

Description: Failed to get ClickHouse storage tier

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_INSERTION_DROP_EVENTS

Description: FortiSIEM dropped events while failing to insert them to ClickHouse after retries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_INSERTION_EPS

Description: ClickHouse Insertion EPS

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_CLICKHOUSE_JSON_ENCODER_EPS

Description: ClickHouse JSON Encoding EPS

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_CLICKHOUSE_JSON_ENCODER_EPS_PER_THREAD

Description: ClickHouse JSON Encoding EPS per thread

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_ACTIVE_CONSOLIDATION

Description: ClickHouse log integrity active consolidation

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CALCULATE_REQUEST_PARSE_FAILED

Description: Failed to parse log integrity calculate request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CALCULATE_REQUEST_STARTED

Description: ClickHouse partition consolidation request started

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CANDIDATE_PARTITIONS

Description: Clickhouse log integrity candidate partitions

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CONSOLIDATION_DATE

Description: ClickHouse log integrity consolidation target date

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_CONSOLIDATION_STATUS_CHANGE

Description: ClickHouse partition consolidation status change

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_DONE

Description: ClickHouse daily consolidation done

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id				Display name				Type				Description			
validFrom				Valid From				Date							
validTo				Valid To				Date							

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_STARTED

Description: ClickHouse daily consolidation started

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id				Display name				Type				Description			
validFrom				Valid From				Date							
validTo				Valid To				Date							

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_STOPPED

Description: ClickHouse daily consolidation stopped

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DAILY_CONSOLIDATION_TIMER

Description: ClickHouse log integrity daily consolidation timer pops

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_DB_QUERY_FAILED

Description: ClickHouse log integrity failed to execute query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_EMPTY_PARTITION_CHECKSUM

Description: ClickHouse log integrity empty partition checksum

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_EXEC_FAILED

Description: ClickHouse log integrity system command failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	
errorCode	Error Code	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_MIN_MAX_QUERY_FAILED

Description: ClickHouse log integrity failed min max block query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_OPTIMIZE_COMMAND_FAILED

Description: ClickHouse log integrity optimize command failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	

Id	Display name	Type	Description
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_CONSOLIDATION_DONE

Description: ClickHouse partition consolidation done

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	
hashSHA256	SHA256 Hash	string	

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_CONSOLIDATION_STARTED

Description: ClickHouse partition consolidation started

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	

Id	Display name	Type	Description
shard	Shard	string	
dbPartition	DB Partition	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_PARTITION_UPDATED_AFTER_CHECKSUM

Description: ClickHouse log integrity partition data updated after checksum calculation

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	
hashSHA256	SHA256 Hash	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_MISMATCH

Description: ClickHouse log integrity SHA256 response mismatch

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	

Id	Display name	Type	Description
shard	Shard	string	
dbPartition	DB Partition	string	
hashSHA256	SHA256 Hash	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_MISMATCH_REPLICAS

Description: ClickHouse log integrity MD5 response mismatch between replicas

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
validFrom	Valid From	Date	
validTo	Valid To	Date	
shard	Shard	string	
dbPartition	DB Partition	string	
hashSHA256	SHA256 Hash	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_PARTITION_INFO_EMPTY

Description: ClickHouse log integrity sha256 target partition info empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
shard	Shard	string	

Id	Display name	Type	Description
dbPartition	DB Partition	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_REQUEST_PARSE_FAILED

Description: Failed to parse log integrity sha256 validation request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_EMPTY

Description: Received error for log integrity sha256 response empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_ERROR

Description: Received error for log integrity sha256 validation response error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_LOG_INTEGRITY_SHA256_RESPONSE_PARSE_FAILED

Description: Failed to parse log integrity sha256 validation request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_MOVE_PARTITION_FAILED

Description: Failed to move ClickHouse partitions

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
dbPartition	DB Partition	string	
errReason	Reason for Error	string	This is the reason for an error if given.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_MOVE_PARTITION_STARTED

Description: Move ClickHouse partition started

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
dbPartition	DB Partition	string	
command	Command	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_MOVE_PARTITION_SUCCEEDED

Description: Move ClickHouse partition successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
dbPartition	DB Partition	string	
command	Command	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_CLICKHOUSE_NOT_REACHABLE

Description: Failed to reach ClickHouse

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_QUERY_REDIS_CONN_FAILURE

Description: Failed to contact with redis on super

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_QUERY_REDIS_GET_FAILURE

Description: Fail to get values from redis

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_CLICKHOUSE_QUERY_UNCOMPRESS_FAILURE

Description: Failed to uncompress data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_QUERY_ZLIB_INIT_FAILURE

Description: Failed to initialize zlib library

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_QUERY_CHECKIN

Description: ClickHouse query checkin

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_QUERY_CHECKOUT

Description: ClickHouse query checkout

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_THREADS_CHECKIN

Description: ClickHouse query threads checkin

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
replica	Replica	string	
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_CLICKHOUSE_RESOURCE_TRACKER_THREADS_CHECKOUT

Description: ClickHouse query threads checkout

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
replica	Replica	string	
serverIpAddr	Server IP	IP	
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_CLICKHOUSE_ROUND_ROBIN_INSERTION

Description: Insert events to ClickHouse in roundrobin fashion

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_CLICKHOUSE_ROUND_ROBIN_QUERY

Description: Query from ClickHouse in roundrobin fashion

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_CLICKHOUSE_STORAGE_FREE_SPACE_CRITICAL

Description: ClickHouse lowest storage tier free space critical

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_CLICKHOUSE_STORAGE_FREE_SPACE_LOW

Description: ClickHouse lowest storage tier free space low

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_CLICKHOUSE_STORAGE_UTILS_PER_ORG_PER_DAY

Description: ClickHouse disk utils per organization per day

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CLICKHOUSE_WRITE_FAILED

Description: ClickHouse Insertion failed

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_CLIHOUSE_BUILD_QUERY_DIST_SQL_COMMAND_FAILURE

Description: Failed to build query dist sql command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLI_ERROR

Description: FortiSIEM CLI error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_CLUSTER_COLLECT_ALL_IP_FAILED

Description: 670-Cluster: Failed to collect all ips of one node

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_COLLECT_CONFIG_DATA_FAILED

Description: 670-Cluster: Failed to collect config data of one node

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_CONFIG_SSH_KEY_FAILED

Description: 670-Cluster: Failed to configure SSH key

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_CLUSTER_GET_FW_IP_FAILED

Description: 670-Cluster: Failed to get followerIps

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_GET_TASK_FAILED

Description: 670-Cluster: Failed to get task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_CLUSTER_NOT_SUPPORT_TASK

Description: 670-Cluster: This type device doesn't support this task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_NOT_VALID_FELLOWER

Description: 670-Cluster: The node is invalid

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_NO_LICENSE

Description: 670-Cluster: There is no license

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_RELOAD_CONFIG_FAILED

Description: 670-Cluster: Failed to re-load configuration from app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_RM_DB_FAILED

Description: 670-Cluster: Failed to remove DB

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_RUN_COMMAND_FAILED

Description: 670-Cluster: Failed to run command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_CLUSTER_SCRIPT_FAILED

Description: 670-Cluster: Failed to execute script

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_SEND_TASK_FAILED

Description: 670-Cluster: Failed to send task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_CLUSTER_SSH_KEY_IS_WRONG

Description: 670-Cluster: The SSH key is wrong

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_TASK_DATA_EMPTY

Description: 670-Cluster: Task data is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_TASK_INFO_IS_WRONG

Description: 670-Cluster: Task info is not right

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_TASK_NOT_CONTAIN_LIC

Description: 670-Cluster: There is no license in task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_CLUSTER_UPDATE_CONFIG_ERROR

Description: Failed to update config

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propName	Property Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_COLLECTOR_CLOCK_SKEW

Description: Clock skew between Collector and Super

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
collectorId	Collector ID	uint32	This field captures the ID of a FortiSIEM Collector
collectorIp	Collector IP	IP	This field captures the IP address of a FortiSIEM Collector
superTime	Supervisor Time	Date	This field represents SupervisorTime used to determine Clock Skew between Collector and Supervisor. A Clock Skew may develop if NTP is not configured correctly in both Collector and Supervisor.
collectorTime	Collector Time	Date	This field represents Collector Time used to determine Clock Skew between Collector and Supervisor. A Clock Skew may develop if NTP is not configured correctly in both Collector and Supervisor.
timeSkewSec	Time skew	uint32	Time skew between Collector and Supervisor. If there is significant time skew then rules may not trigger, since rules need to be evaluated based on a time window.

EventType: PH_COLLECTOR_DOWN

Description: Collector down

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_COLLECTOR_EVENT_ARRIVAL_DELAYED

Description: Collector event delayed

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_COLLECTOR_EVENT_ARRIVAL_OK

Description: Collector event arrived on time

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_COLLECTOR_EVENT_STORE_DELAYED

Description: Collector event file delayed

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_COLLECTOR_EVENT_STORE_OK

Description: Collector event file on time

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_COLLECTOR_LICENSE_UPDATE

Description: License on collector updated

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_COLLECTOR_UP

Description: Collector up

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_CREATE_TEMP_FILE_FAILURE

Description: FortiSIEM temp file creation error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_CYBERARK_INIT_ERROR

Description: FortiSIEM CyberArk module initialization error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAINTEGRITY_PASSPHRASE_LOAD_ERROR

Description: Data integrity module failed to load passphrase from App Server. Passphrase is needed for signing events

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAINTEGRITY_SIGNER_ERROR

Description: Data integrity module failed to sign event data for message integrity

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAINTEGRITY_UTILS_ERROR

Description: Generic data integrity utilities error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAINTEGRITY_VERIFIER_ERROR

Description: Data integrity module failed to verify event data for message integrity

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAMANAGER_CLICKHOUSE_HTTP_UPLOAD_ERROR

Description: Failed to upload events to ClickHouse

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
serverName	Server Name	string	

EventType: PH_DATAMANAGER_CLUSTER_ENCODE_ERROR

Description: Elasticsearch event encode error while writing events

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_CLUSTER_INIT_ERROR

Description: Elasticsearch client initialization failed

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_CLUSTER_WAIT_ERROR

Description: Elasticsearch client failed tp get event block from sharedstore

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_CLUSTER_WRITER_ERROR

Description: Elasticsearch cluster writer error

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_DASHBOARD_RESPONSE_ERROR

Description: Data Manager failed to respond to Query Master for summary dashboard query requests

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_ELASTICWRITER_ERROR

Description: Elasticsearch client failed to write events to Elasticsearch

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTATTR_ERROR

Description: Data Manager found unknown event attribute while writing to database

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_EVTCACHE_DUPLICATE_ERROR

Description: Data Manager found duplicate event id in event cache for trigger event query

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_EVTCACHE_GET_ERROR

Description: Data Manager failed to get event from event cache for trigger event query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTCACHE_PARSE_ERROR

Description: Data Manager failed to parse trigger event query XML from Query Master

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTDBNOTIFIER_ERROR

Description: Data Manager failed to upload event-file-signature related details to App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTIDX_CORRUPT_ERROR

Description: Data Manager detected event index corruption

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAMANAGER_EVTIDX_MERGE_ERROR

Description: Data Manager failed to merge event index

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.
dirName	Directory Name	string	

EventType: PH_DATAMANAGER_EVTIDX_QUERY_ERROR

Description: Data Manager failed to read event index during query

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTIDX_READ_BLOCK_ERROR

Description: Data Manager failed to read event file block during query or index merge

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTIDX_READ_KEY_ERROR

Description: Data Manager failed to read event file index during query or index merge

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTIDX_READ_POST_ERROR

Description: Data Manager failed to read event index posting file during query or index merge

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTIDX_WRITE_ERROR

Description: Data Manager failed to write event index

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAMANAGER_EVTIDX_WRITE_KEY_ERROR

Description: Data Manager failed to write event index file key

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAMANAGER_EVTIDX_WRITE_POST_ERROR

Description: Data Manager failed to write event index posting file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_EVTLOADER_ERROR

Description: Data Manager failed to load events from shared buffer

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
dirName	Directory Name	string	

EventType: PH_DATAMANAGER_EVTWRITER_ERROR

Description: Data Manager failed to store events to event database

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_DATAMANAGER_EXPORT_ERROR

Description: Data Manager failed to export events from event database

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_FILE_READ_FAILURE

Description: FortiSIEM DataManager failed to read file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_DATAMANAGER_FILE_RENAME_FAILURE

Description: FortiSIEM DataManager failed to rename file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_DATAMANAGER_FILE_SIGN_ERROR

Description: Data Manager failed to sign event files for message integrity

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_DATAMANAGER_FILE_WRITE_FAILURE

Description: FortiSIEM DataManager failed to write file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_DATAMANAGER_GET_SIGN_ERROR

Description: Data Manager failed to read event message integrity signatures

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_DATAMANAGER_GLOBAL_CACHE_MISSING

Description: FortiSIEM DataManager missing global cache

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_HDFSWRITER_ERROR

Description: Data Manager module failed to write to HDFS

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
infoURL	Informational URL	string	This field captures an URL if present in an event
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATAMANAGER_HTTP_UPLOAD_ERROR

Description: Data Manager module failed to upload event database statistics to App server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_DATAMANAGER_INIT_ERROR

Description: Data Manager module initialization error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_INTEGRITY_CHECK_ERROR

Description: Data Manager failed to do integrity check for certain event files

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
fileName	File Name	string	

EventType: PH_DATAMANAGER_INTEGRITY_RESPONSE_ERROR

Description: Data Manager failed to respond to App Server for log integrity check requests

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_INVALID_LOG_FILE

Description: FortiSIEM DataManager invalid log file

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_KAFKAWRITER_CONFIG_ERROR

Description: Data Manager failed to load Kafka configuration from App server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_KAFKAWRITER_ERROR

Description: Data Manager failed to write events to Kafka message bus

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorString	Error String	string	This is the error message, synonymous to attribute errReason
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_DATAMANAGER_LOG_BUFFER_PAUSED_LOW_SPACE

Description: PerCust event buffer is paused because of low free space

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_LOG_BUFFER_PAUSED_STATFS_FAILURE

Description: PerCust event buffer is paused because of statfs failure

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_LOG_BUFFER_RESUMED

Description: PerCust event buffer is resumed

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_PUT_SIGN_ERROR

Description: Data Manager failed to store event file integrity signatures

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_DATAMANAGER_QUERY_EXPR_ERROR

Description: Data Manager failed to parse trigger event query expression

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_QUERY_RESPONSE_ERROR

Description: Data Manager failed to respond to Query Master for incident trigger event query requests

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAMANAGER_REDIS_KEY_NOT_EXIST

Description: redis key not exist

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMANAGER_SUMMARYWRITER_ERROR

Description: Data Manager failed to write inline report results

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_DATAMGR_BAD_EVTBLKIDX_FILE

Description: Bad event block index file

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_BAD_SEGMENT

Description: Bad data segment

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_INDEX_MERGE_FAILED

Description: Failed to merge indices

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_INDEX_MERGE_FAILED_INDEX

Description: Index that failed to merge

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_INDEX_MERGE_FAILED_INDEX_GROUP

Description: Index group that failed to merge

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_SEGMENT_MERGE_ERROR

Description: Datamgr segment merge error

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_SEGMENT_MERGE_FAILED

Description: Failed to merge segments

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_UNABLE_FLUSH_INDEX

Description: Failed to flush index

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAMGR_UNABLE_OPEN_EVTBLK_FILE

Description: Unable to open event block file

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATAPURGER_ARCHIVE_TASK_ERROR

Description: Data Purger failed to archive events but they are purged

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_CMD_FAILURE

Description: Data Purger failed to run command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
errorNoInt	Error Number Int	int32	

EventType: PH_DATAPURGER_DR_ES_RESTORE_FAILED

Description: Data Purger failed to do restore for Disaster Recovery

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_DR_ES_ROLE_UNKNOWN

Description: Elasticsearch Disaster Recovery Role is Unknown

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAPURGER_DR_ES_SNAPSHOTS_GET_FAILED

Description: Data Purger failed to get snapshots for Disaster Recovery

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_DR_ES_SNAPSHOT_DELETION_FAILED

Description: Data Purger failed to delete snapshots for Disaster Recovery

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_DR_ES_SNAPSHOT_FAILED

Description: Data Purger failed to do snapshot for Disaster Recovery

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_DUCHECKER_ERROR

Description: Data Purger failed to check disk usage

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_ENFORCE_ERROR

Description: Data Purger failed to enforce event purging policy

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_EVAL_ERROR

Description: Data Purger failed to evaluate event purging policies for a particular day

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_HTTP_UPLOAD_ERROR

Description: Data Purger failed to upload disk usage to App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_INIT_ERROR

Description: Data Purger module initialization error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_OPEN_FILE_ERROR

Description: Data Purger module failed to open file

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_DATAPURGER_PARSE_XML_ERROR

Description: Data Purger module failed to parse XML containing purging policies received from App server

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_DATAPURGER_POLICY_ERROR

Description: Data Purger failed to implement specific event purging policy

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_RESPONSE_ERROR

Description: Data Purger module failed to handle event database refresh/restore related requests from App server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATAPURGER_STORAGE_POLICY_CLICKHOUSE_NODES_EMPTY

Description: Data Purger failed to retrieve ClickHouse nodes from Redis

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DATA_CLUSTER_ALL_COORDINATOR_DOWN

Description: All Coordinator nodes are down or not reachable or not responsive

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_DATA_CLUSTER_BUSY

Description: Elasticsearch cluster is busy

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_DATA_CLUSTER_CLICKHOUSE_CONFIG_NO_PORT

Description: ClickHouse PORT is not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_COORDINATOR_DOWN

Description: Coordinator is down or not reachable or not responsive

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_DATA_CLUSTER_COORDINATOR_UP

Description: Coordinator is up

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_HTTPPORT

Description: Elasticsearch cluster HTTP PORT is not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_IP

Description: Elasticsearch cluster IP is not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_JAVAPORT

Description: FortiSIEM Elasticsearch configuration missing Java port

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NAME

Description: FortiSIEM Elasticsearch configuration missing cluster name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NUMREPLICAS

Description: FortiSIEM Elasticsearch configuration missing number of replica

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NO_NUMSHARD

Description: FortiSIEM Elasticsearch configuration missing number of shards

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_NULL

Description: Elasticsearch cluster not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_CONFIG_WRONG_FORMAT

Description: Wrng response format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATA_CLUSTER_ELASTIC_EVENTID_NOT_FOUND

Description: Elasticsearch error string doesn't contain enough information

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_HTTP_CLIENT_FAIL

Description: Elasticsearch REST API call to AppSrv failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_ELASTIC_HTTP_CMD_FAIL

Description: Elasticsearch REST API call fails

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
msg	Message	string	

EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_FAIL

Description: Elasticsearch indexing failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
size	Size	uint32	

EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_RESEND_FAIL

Description: Elasticsearch indexing failed 2nd time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
size	Size	uint32	

EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FAIL

Description: Elasticsearch indexing failed at the last time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
size	Size	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_SEND_FIRST_FAIL

Description: Elasticsearch indexing failed at 1st time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
size	Size	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATA_CLUSTER_ELASTIC_INDEX_UPLOAD_FAIL

Description: Elasticsearch event upload via REST API failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATA_CLUSTER_ELASTIC_WRONG_JSON_FORMAT

Description: Elasticsearch "_cat/indices" API response format wrong format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATA_CLUSTER_GET_HOSTNAME_FAIL

Description: Elasticsearch popen hostname failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_PORT

Description: HDFS port in not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_SERVER

Description: HDFS server in not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_YARN_PORT

Description: HDFS yarn port in not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NO_YARN_SERVER

Description: HDFS yarn server in not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_CONFIG_NULL

Description: HDFS cluster is not configured

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_HTTP_CMD_FAIL

Description: HDFS REST API call to AppSrv failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
infoURL	Informational URL	string	This field captures an URL if present in an event
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
msg	Message	string	

EventType: PH_DATA_CLUSTER_HDFS_LISTSTATUS_FAIL

Description: HDFS LISTSTAUTS API failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DATA_CLUSTER_HDFS_SEND_FAIL

Description: HDFS storing events failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_DATA_CLUSTER_HDFS_UPLOAD_FAIL

Description: HDFS event upload via REST API failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_DATA_CLUSTER_JSON_GET_ATTRIBUTE_NAME_FAIL

Description: Elasticsearch Event Attribute name fetch failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DEVICE_NOT_ADDED

Description: Discovered device not added to CMDB because of license restrictions

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DEV_FAIL_TO_PULL_EVENTS

Description: Fail to pull events

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_ACME_PACKET_SESSION_AGENT_STATUS

Description: Acme Packet Controller session status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
sessionAgentHostName	Agent HostName	string	
sessionAgentType	Agent Type	string	
sessionInboundCont	Session Inbound Count	uint32	
sessionInboundRate	Session Inbound Rate	uint32	
sessionOutboundCount	Session Outbound Count	uint32	
sessionOutboundRate	Session Outbound Rate	uint32	
sessionAgentStatus	Session Agent Status	string	

EventType: PH_DEV_MON_ACME_PACKET_SYS_STATUS

Description: Acme Packet Controller system status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
apSysHealthScore	System Health Score	uint32	
apSysRedundancy	System Redundancy	uint32	
apSysGlobalConSess	System Global ConSess	uint32	
apSysGlobalCPS	System Global CPS	uint32	
apSysNATCapacity	System NAT Capacity	uint32	
apSysARPCapacity	System ARP Capacity	uint32	
apSysState	System State	uint32	
apSysLicenseCapacity	System License Capacity	uint32	
apSysSipStatsActiveLocalContacts	System Sip Stats Active Local Contacts	uint32	
apSysMgcpGWEndpoints	System Mgcp GW Endpoints	uint32	
apSysH323Registration	System H323 Registration	uint32	
apSysRegCacheLimit	System Reg Cache Limit	uint32	
apSysApplicationCPULoadRate	System Application CPU Load Rate	uint32	
apSysRejectedMessages	System Rejected Messages	uint32	
apSysSipEndptDemTrustToUntrust	System Sip Endpt Dem Trust To Untrust	uint32	
apSysSipEndptDemUntrustToDeny	System Sip Endpt Dem Untrust To Deny	uint32	
apSysMgcpEndptDemTrustToUntrust	System Mgcp Endpt Dem Trust To Untrust	uint32	
apSysMgcpEndptDemUntrustToDeny	System Mgcp Endpt Dem Untrust To Deny	uint32	
apSysSipTotalCallsRejected	System SIP Total Calls Rejected	uint32	
apSysSipStatsActiveSubscriptions	System SIP Active Subscriptions	uint32	
apSysSipStatsPerMaxSubscriptions	System SIP Per Max Subscriptions	uint32	

Id	Display name	Type	Description
apSysSipStatsPerMaximumActiveSubscriptions	System SIP Per Maximum Active Subscriptions	uint32	
apSysSipStatsTotalSubscriptions	System SIPTotal Subscriptions	uint32	

EventType: PH_DEV_MON_APP_APACHE_MET

Description: Apache Web server performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
httpTotalAccesses	HTTP Connection Count	uint32	
httpTotalKBytes	HTTP Total KBytes	uint32	
apacheCPULoad	Apache CPU Load	double	
apacheUptime	Apache Uptime	uint64	
apacheReqPerSec	Apache Request Rate /sec	double	
apacheBytesPerSec	Apache Transfer Rate Bytes/sec	double	
apacheBytesPerReq	Apache Transfer Rate Bytes/Req	double	
apacheBusyWorkers	Apache Busy Workers	uint32	
apacheldleWorkers	Apache Idle Workers	uint32	

EventType: PH_DEV_MON_APP_ASPNET_MET**Description:** ASP.NET performance metric**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
aspReqExecTimeMs	ASP.NET Request Exec Time ms	uint32	
aspReqCurrent	ASP.NET Curent Requests	uint32	
aspReqDisconnected	ASP.NET Disconn Requests	uint32	
aspReqQueued	ASP.NET Queued Requests	uint32	
aspReqRejected	ASPNET Rejected Requests	uint32	
aspReqWaitTimeMs	ASP.NET Request Wait Time ms	uint32	

EventType: PH_DEV_MON_APP_DHCP_MET**Description:** DHCP performance metrics collected**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
dhcpReqPerSec	DHCP Request Rate /sec	uint32	

Id	Display name	Type	Description
dhcpRelPerSec	DHCP Release Rate /sec	uint32	
dhcpDeclinesPerSec	DHCP Decline Rate /sec	uint32	
dhcpDupsDroppedPerSec	DHCP Duplicate Drop Rate /sec	uint32	
dhcpPktsPerSec	DHCP Packet Rate /sec	uint32	
dhcpActiveQueueLen	DHCP Active Queue Length	uint32	
dhcpConflictQueueLen	DHCP Conflict Queue Length	uint32	
dhcpAvgRespTime	DHCP Average Resp Time	uint32	
dhcpDiscoverPreSec	DHCP Discover Rate /sec	uint32	
dhcOfferPerSec	DHCP Offer Rate /sec	uint32	
dhcpAckPerSec	DHCP Ack Rate /sec	uint32	
dhcpNackPerSec	DHCP Nack Rate /sec	uint32	
dhcpInformPerSec	DHCP Inform Rate /sec	uint32	

EventType: PH_DEV_MON_APP_DNS_MET

Description: DNS performance metrics collected

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
dnsReqRecv	DNS Requests Recvd	uint32	
dnsRespSent	DNS Responses Sent	uint32	
winsReqRecv	WINS Requests Recvd	uint32	

Id	Display name	Type	Description
winsRespSent	WINS Responses Sent	uint32	
dnsRecQueryRecv	Recursive DNS Query Recvd	uint32	
recurDnsQueryFail	Recursive DNS Query Failed	uint32	
recurDnsQueryTimeout	Recursive DNS Query Timeout	uint32	
fullDnsXferSent	Full DNS Zone Transfer Request Sent	uint32	
fullDnsXferRecv	Full DNS Zone Transfer Responses Recvd	uint32	
fullDnsXferSucc	Full DNS Zone Transfer Success	uint32	
incrDnsXferRecv	Incremental DNS Zone Transfer Responses Recvd	uint32	
incrDnsXferSucc	Incremental DNS Zone Transfer Success	uint32	
dnsSecUpdateRecv	Secure DNS Update Recvd	uint32	
dynDnsUpdRej	Dynamic DNS Update Rejected	uint32	
dynDnsUpdTimeout	Dynamic DNS Update Timeout	uint32	
secDnsUpdFail	Secure DNS Update Failed	uint32	

EventType: PH_DEV_MON_APP_ICA_SESS_MET

Description: Citrix ICA IIS session metrics collected

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
user	User	string	
icaLatencyLast	ICA Latency Last Recorded	uint32	

Id	Display name	Type	Description
icaLatencySessAvg	ICA Latency Session Average	uint32	
icaLatencySessDev	ICA Latency Session Deviation	uint32	
icaInSessBw	ICA Input Session Bandwidth	uint32	
icaInSessLineSpeed	ICA Input Session Line Speed	uint32	
icaInSessComp	ICA Input Session Compression	uint32	
icaInDriveBw	ICA Input Drive Bandwidth	uint32	
icaInEchoBw	ICA Input Text Echo Bandwidth	uint32	
icaInAudioBw	ICA Input Audio Bandwidth	uint32	
icaInVFBw	ICA Input VideoFrame Bandwidth	uint32	
icaOutSessBw	ICA Output Session Bandwidth	uint32	
icaOutSessLineSpeed	ICA Output Session Line Speed	uint32	
icaOutSessComp	ICA Output Session Compression	uint32	
icaOutDriveBw	ICA Output Drive Bandwidth	uint32	
icaOutEchoBw	ICA Output Text Echo Bandwidth	uint32	
icaOutAudioBw	ICA Output Audio Bandwidth	uint32	
icaOutVFBw	ICA Output VideoFrame Bandwidth	uint32	

EventType: PH_DEV_MON_APP_IIS_MET

Description: Microsoft IIS performance metrics collected

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
httpCurrConnCount	HTTP Current Connection Count	uint32	
httpMaxConnCount	HTTP Max Connection Count	uint32	
httpSentFiles	HTTP Sent Files	uint32	
httpRecvFiles	HTTP Recv Files	uint32	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.
sysUpTime	System Uptime	uint32	
httpNotFoundErr	HTTP Not Found Errors	uint32	
srvInstName	Web Server Instance	string	

EventType: PH_DEV_MON_APP_MSEXCH_ERR_MET

Description: Microsoft Exchange performance error metrics collected

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	

Id	Display name	Type	Description
exchRPCFailed	Exch RPC Failed Count	uint32	
exchRPCSuccess	Exch RPC Success Count	uint32	
exchRPCCallFailed	Exch RPC Failed - Call Failed	uint32	
exchRPCDenied	Exch RPC Denied Count	uint32	
exchRPCFailedServBusy	Exch RPC Failed - Server Busy	uint32	
exchRPCFailedServUnavail	Exch RPC Failed - Server Unavail	uint32	
exchBgRPCFailed	Exch Background RPC Failed	uint32	
exchFgRPCFailed	Exch Foreground RPC Failed	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_ISDB_INST_MET

Description: Microsoft Exchange Database Instance Metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
dbName	DB Name	string	
logGenCheckptDepth	Log Gen Checkpoint Depth	uint32	
dbReadsAverageLatency	DB Read latency ms	uint32	
dbWritesAverageLatency	DB Write latency ms	uint32	
dbPhysicalWritesPerSec	DB Write Rate /sec	double	

Id	Display name	Type	Description
dbSessionCount	DB Session Count	uint32	
sessPctUsed	Session Used Pct	uint32	
logBytesWritePersec	Log Write Rate Bps	uint32	
versionbucketsallocated	Version Buckets Allocated	uint32	
logThreadsWaiting	Log Threads Waiting	uint32	
tableOpenCacheHitsPersec	Table Open Cache Hit Rate /sec	uint32	
tableOpenCacheMissesPersec	Table Open Cache Miss Rate /sec	uint32	
tableOpenCachePercentHit	Table Open Cache Hit Pct	uint32	
tableOpensPersec	Table Open Rate /sec	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_ISDB_MET

Description: Microsoft Exchange Information Store Database Metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
pageFaultsStallsPersec	Page Fault Stall Rate /sec	uint32	
pageFaultsPersec	Page Fault Rate /sec	uint32	
dbCacheSizeMB	DB Cache Size MB	uint32	
dbCachePercentHit	DB Cache Hit pct	uint32	
logBytesWritePersec	Log Write Rate Bps	uint32	

Id	Display name	Type	Description
dbReadsAverageLatency	DB Read latency ms	uint32	
dbWritesAverageLatency	DB Write latency ms	uint32	
logRecordStallsPersec	Log Record Stall Rate /sec	uint32	
versionbucketsallocated	Version Buckets Allocated	uint32	
logThreadsWaiting	Log Threads Waiting	uint32	
logWritesAverageLatency	Log Write latency ms	uint32	
dbPageFaultsPersec	DB Page Fault Rate /sec	uint32	
dbPageFaultStallsPersec	DB Page Fault Stall Rate /sec	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_MBOX_MET

Description: MS Exchange mailbox utilization metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchMboxName	Exch Mailbox Name	string	
exchMboxSendQueue	Exch Mailbox Send Queue	uint32	
exchMboxRecvQueue	Exch Mailbox Recv Queue	uint32	
exchMboxSentMsg	Exch Mailbox Sent Message	uint32	
exchMboxSubmitMsg	Exch Mailbox Submitted Message	uint32	

Id	Display name	Type	Description
exchMboxDelivMsg	Exch Mailbox Delivered Message	uint32	
exchMboxActiveUserCount	Exch Mailbox Active User Count	uint32	
exchMboxPeakUserCount	Exch Mailbox Peak User Count	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_MET

Description: Microsoft Exchange performance metrics collected

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchVMLargestBlockSize	Exch VM Largest Block Size	uint32	
exchVMTotallLargeFreeBlockBytes	Exch VM Large Free Blocks Bytes	uint32	
exchVMTotallFreeBlocks	Exch VM Free Blocks	uint32	
exchRPCReq	Exch RPC Requests Served	uint32	
exchRPCAvgLatency	Exch Avg RPC Latency ms	uint32	
exchRPCOpsPerSec	Exch RPC Ops Rate /sec	uint32	
exchRPCReqPeak	Exch RPC Request Peak	uint32	
exchUserCount	Exch User Count	uint32	

Id	Display name	Type	Description
exchActiveUserCount	Exch Active User Count	uint32	
exchPeakUserCount	Exch Peak User Count	uint32	
exchActiveConnCount	Exch Active Conn Count	uint32	
exchMaxConn	Exch Max Conn Count	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_REPL_MET

Description: Microsoft Exchange Replication Metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchReplInstName	Exch Replication Instance Name	string	
copyQueueLen	Exch TxLog Copy Queue Length	uint32	
replayQueueLength	Exch TxLog Replay Queue Length	uint32	
avgLogCopyLatencyMs	Exch Log Copy latency ms	uint32	
maxNetworkLatencyMs	Exch Log Copy network Latency ms	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_SMTP_MET

Description: MS Exchange SMTP metric

Severity: 1 (Low)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchCatQueue	Exch Categorization Queue	uint32	
exchSMTPLocalQueue	Exch SMTP Local Queue	uint32	
exchSMTPRemoteQueue	Exch SMTP Remote Queue	uint32	
exchSMTPInConn	Exch SMTP Inbound Conn	uint32	
exchSMTPOutConn	Exch SMTP Outbound Conn	uint32	
sentBytesPerSec	Sent Byte Rate	double	
recvBytesPerSec	Received Byte Rate	double	
exchSMTPRetries	Exch SMTP Retries	uint32	
exchSMTPLocalRetryQueue	Exch SMTP Local Retry Queue	uint32	
exchSMTPRemoteRetryQueue	Exch SMTP Remote Retry Queue	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_STORE_INTF_MET**Description:** Microsoft Exchange Store Interface Metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchStoreIntfName	Exch Store Interface Name	string	
exchRPCAvgLatency	Exch Avg RPC Latency ms	uint32	
RPCReqOutstanding	Exch Outstanding RPC Requests	uint32	
ROPReqOutstanding	Exch Outstanding ROP Requets	uint32	
RPCReqFailedPct	Exch RPC Failed Requests Pct	uint32	
RPCSlowReq	Exch RPC Slow Requests	uint32	
RPCSlowReqLatencyAvgMs	Exch RPC Slow Request Latency ms	uint32	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.

EventType: PH_DEV_MON_APP_MSEXCH_SUBMIT_MET

Description: Microsoft Exchange Mail Submission Metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	

Id	Display name	Type	Description
hubServers	Exch Hub Server Count	uint32	
hubServersInRetry	Exch Hub Servers In Retry	uint32	
failedSubmissions	Exch Failed Submissions	uint32	
successSubmissions	Exch Successful Submissions	uint32	
tempSubmissionFailures	Exch Temp Submission Failures	uint32	
hubTranspServersPrctActive	Exch Active Hub Transport Servers Pct	uint32	
failedSubmissionsPersec	Exch Failed Submission Rate /sec	uint32	
successSubmissionsPersec	Exch Successful Submission Rate /sec	uint32	
tempSubmissionFailuresPersec	Exch Temp Submission Failure Rate /sec	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_TRANS_MET

Description: Microsoft Exchange Transport Queue Metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
aggDeliveryQueueLen	Exch Aggregate Delivery Queue	uint32	
activeRemoteDeliveryQueueLen	Exch Active Remote Delivery Queue	uint32	

Id	Display name	Type	Description
activeMailboxDeliveryQueueLen	Exch Active Mailbox Delivery Queue	uint32	
submissionQueueLen	Exch Submission Queue	uint32	
activeNonSmtplibDeliveryQueueLen	Exch Active Non-SMTP Deelivery Queue	uint32	
retryMailboxDeliveryQueueLen	Exch Retry Mailbox Delivery Queue	uint32	
unreachableQueueLen	Exch Unreachable Queue	uint32	
largestDeliveryQueueLen	Exch Largest Delivery Queue	uint32	
poisonQueueLength	Exch Poison Queue	uint32	

EventType: PH_DEV_MON_APP_MSEXCH_WS_MET

Description: MS Exchange Mailbox whitespace metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
exchMboxName	Exch Mailbox Name	string	
exchMboxWs	Exch Mailbox Whitespace MB	uint32	

EventType: PH_DEV_MON_APP_NTDS_MET

Description: Microsoft directory service performance metrics collected

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
dirSearchesPerSec	NTDS Dir Search Rate /sec	double	
dirReadsPerSec	NTDS Dir Read Rate /sec	double	
dirWritesPerSec	NTDS Dir Write Rate /sec	double	
dirBrowsesPerSec	NTDS Dir Browse Rate /sec	double	
LDAPSearchesPerSec	NTDS LDAP Search Rate /sec	double	
DSClientBindsPerSec	NTDS Client Bind Rate /sec	double	
LDAPNewConnectionsPerSec	NTDS LDAP New Conn Rate /sec	double	
LDAPSuccessfulBindsPerSec	NTDS LDAP Success Bind Rate /sec	double	
LDAPActiveThreads	NTDS LDAP Active Threads	uint32	
LDAPBindTime	NTDS LDAP Bind Time	uint32	
LDAPClientSessions	NTDS LDAP Client Sessions	uint32	

EventType: PH_DEV_MON_ARUBA_WLAN_RADIO_METRIC**Description:** WLAN Radio interface metric**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
wlanChannelId	WLAN Channel Id	uint32	WLAN Channel Id found in SNMP based WLAN monitoring
wlanProtocol	WLAN Protocol	string	WLAN Protocol found in SNMP based WLAN monitoring
wlanUserCount	WLAN User count	uint32	WLAN User count found in SNMP based WLAN monitoring
wlanChannelUtil	WLAN Channel Util	uint32	WLAN Channel Util found in SNMP based WLAN monitoring
ifInteflIdx	WLAN Interface Intereference Index	uint32	WLAN Interface Intereference Index found in SNMP based WLAN monitoring
ifCoverageIdx	WLAN Interface Coverage Index	uint32	WLAN Interface Coverage Index found in SNMP based WLAN monitoring
ifNoiseIdx	WLAN Interface Noise Index	uint32	WLAN Interface Noise Index found in SNMP based WLAN monitoring
totBytesPerSec	Total Byte Rate	double	
totPktsPerSec	Total Packet Rate	double	

EventType: PH_DEV_MON_AUTH_STATS

Description: FortiAuthenticator Authentication status

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
authUserCount	Auth User Count	uint32	
authGroupCount	Auth Group Count	uint32	

Id	Display name	Type	Description
tokenCount	Token Count	uint32	
usersRemaining	User Remaining	uint32	
groupRemaining	Group Remaining	uint32	
tokenRemaining	Token Remaining	uint32	
radiusNasCount	Radius Nas Count	uint32	
radiusNasRemaining	Radius Nas Remaining	uint32	
userCertCount	User Certification Count	uint32	
radiusLoginsTot	Radius Logins Count	uint32	
radiusLogins5Mins	Radius Logins Count 5 Mins	uint32	
radiusFailuresTot	Radius Login Failures Count	uint32	
radiusFailures5Mins	Radius Login Failures Count 5 Mins	uint32	
radiusAccountingTot	Radius Accounting Count	uint32	
radiusAccounting5Mins	Radius Accounting Count 5 Mins	uint32	
ldapLoginsTot	LDAP Logins Count	uint32	
ldapLogins5Mins	LDAP Logins Count 5 Mins	uint32	
ldapFailuresTot	LDAP Failures Count	uint32	
ldapFailures5Mins	LDAP Failures Count 5 Mins	uint32	
authEventsTot	Auth Events Count	uint32	
authEvents5Mins	Auth Events Count 5 Mins	uint32	
authFailure	Auth Failures	uint32	
authFailures5Mins	Auth Failures Count 5 Mins	uint32	
radiusProxyInTot	Radius Proxy Requests Received	uint32	
radiusProxyOutTot	Radius Proxy Requests Sent	uint32	

EventType: PH_DEV_MON_AUTO_SVC_START_TO_STOP

Description: Running Windows Auto Service stopped

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
servicePath	Service Path	string	
serviceDesc	Service Description	string	

EventType: PH_DEV_MON_AUTO_SVC_STOP

Description: Windows Auto Service stopped

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
servicePath	Service Path	string	
serviceDesc	Service Description	string	

EventType: PH_DEV_MON_AUTO_SVC_STOP_TO_START

Description: Stopped Windows Auto Service started

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
servicePath	Service Path	string	
serviceDesc	Service Description	string	

EventType: PH_DEV_MON_BC_PROXY_METRIC

Description: Bluecoat Web-proxy metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
proxyCacheObjCount	Proxy Cache Object Count	uint32	
proxy2ServerHttpErr	Proxy-to-Server HTTP Error	uint32	
proxy2ServerHttpReq	Proxy-to-Server HTTP Requests	uint32	
server2ProxyHttpKBps	Server-to-Proxy HTTP Traffic KBps	double	
proxy2ServerHttpKBps	Proxy-to-Server HTTP Traffic KBps	double	
client2ProxyHttpReq	Client-to-Proxy HTTP Request	uint32	
client2ProxyHttpCacheHit	Client-to-Proxy HTTP Cache Hit	uint32	
client2ProxyHttpError	Client-to-Proxy HTTP Errors	uint32	
client2ProxyHttpKBps	Client-to-Proxy HTTP Traffic KBps	double	

Id	Display name	Type	Description
proxy2ClientHttpKBps	Proxy-to-Client HTTP Traffic KBps	double	

EventType: PH_DEV_MON_BGP_NBR_STATUS

Description: BGP neighbor status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
srcASNum	Source Autonomous System Number	uint16	The Autonomous System Number (ASN) to which Source IP belongs. ASN is a unique identifier that is globally available and allows its autonomous system to exchange routing information with other systems. This attribute is generally present in Netflow.
destASNum	Destination Autonomous System Number	uint16	The Autonomous System Number (ASN) to which Destination IP belongs. ASN is a unique identifier that is globally available and allows its autonomous system to exchange routing information with other systems. This attribute is generally present in Netflow.
bgpState	BGP State	string	

EventType: PH_DEV_MON_BOX_FILE_CREATE

Description: Box.com file created

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
fileType	File Type	string	
targetName	Target Name	string	
fileSize64	File Size64 Bytes	uint64	
filePath	File Path	string	
fileOwner	File Owner	string	
fileDesc	File Description	string	
user	User	string	
userId	User Id	string	
accessTime	Access Time	Date	
accountName	Account Name	string	
fileId	File Id	string	
fileVersion	File Version	string	
targetHashCode	Target Hash Code	string	

EventType: PH_DEV_MON_BOX_FILE_DELETE

Description: Box.com file deleted

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
fileType	File Type	string	
targetName	Target Name	string	
fileSize64	File Size64 Bytes	uint64	
filePath	File Path	string	
fileOwner	File Owner	string	
fileDesc	File Description	string	
user	User	string	

Id	Display name	Type	Description
userId	User Id	string	
accessTime	Access Time	Date	
accountName	Account Name	string	
fileId	File Id	string	
fileVersion	File Version	string	
targetHashCode	Target Hash Code	string	

EventType: PH_DEV_MON_BOX_FILE_MODIFY

Description: Box.com file modified

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
fileType	File Type	string	
targetName	Target Name	string	
fileSize64	File Size64 Bytes	uint64	
filePath	File Path	string	
fileOwner	File Owner	string	
fileDesc	File Description	string	
user	User	string	
userId	User Id	string	
accessTime	Access Time	Date	
accountName	Account Name	string	
fileId	File Id	string	
fileVersion	File Version	string	
targetHashCode	Target Hash Code	string	

EventType: PH_DEV_MON_BOX_FILE_SHARE

Description: Box.com file sharing properties

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
fileType	File Type	string	
targetName	Target Name	string	
fileSize64	File Size64 Bytes	uint64	
filePath	File Path	string	
fileOwner	File Owner	string	
fileDesc	File Description	string	
accountName	Account Name	string	
fileId	File Id	string	
fileVersion	File Version	string	
infoURL	Informational URL	string	This field captures an URL if present in an event
downloadURL	Download URL	string	
filePasswordEnabled	File Password Enabled	string	
filePreviewEnabled	File Preview Enabled	string	
fileDownloadEnabled	File Download Enabled	string	
fileUnshareAtTime	File Unshare At Time	Date	
filePreviewCount	File Preview Count	uint64	
fileDownloadCount	File Download Count	uint64	

EventType: PH_DEV_MON_CBQOS_CMSTAT

Description: Cisco Class-Based QoS ClassMap related metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.
qosPolicy	CBQoS Policy Name	string	Class Based QoS (CSQoS) Policy Name. This parameter is set by CBQoS monitoring.
qosClass	CBQoS Class Name	string	Class Based QoS (CSQoS) Class Name. This parameter is set by CBQoS monitoring.
qosPrePoliceRate	CBQoS PrePolice KBps	double	The rate (in KBytes/sec) of pre-policed Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosPostPoliceRate	CBQoS PostPolice KBps	double	The rate (in KBytes/sec) of post-policed Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosDropRate	CBQoS Drop KBps	double	The rate (in KBytes/sec) of dropped Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosDropPct	CBQoS Drop Pct	double	Dropped traffic percentage of Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.

EventType: PH_DEV_MON_CBQOS_POLICESTAT

Description: Cisco Class-Based QoS Police Action related metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
qosPolicy	CBQoS Policy Name	string	Class Based QoS (CSQoS) Policy Name. This parameter is set by CBQoS monitoring.
qosClass	CBQoS Class Name	string	Class Based QoS (CSQoS) Class Name. This parameter is set by CBQoS monitoring.
qosConformRate	CBQoS Conform KBps	double	The rate (in KBytes/sec) of conforming Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosExceedRate	CBQoS Exceeded KBps	double	The rate (in KBytes/sec) of exceeding Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosViolateRate	CBQoS Violated KBps	double	The rate (in KBytes/sec) of violating Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.

EventType: PH_DEV_MON_CBQOS_QUEUESTAT

Description: Cisco Class-Based QoS Queueing Action related metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.
qosPolicy	CBQoS Policy Name	string	Class Based QoS (CSQoS) Policy Name. This parameter is set by CBQoS monitoring.
qosClass	CBQoS Class Name	string	Class Based QoS (CSQoS) Class Name. This parameter is set by CBQoS monitoring.
qosCurrQueue	CBQoS Curr Queue Length	uint32	Current Queue length in Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.

Id	Display name	Type	Description
qosMaxQueue	CBQoS Max Queue Length	uint32	Maximum Queue length in Class Based QoS (CSQoS) traffic. This parameter is set by CBQoS monitoring.
qosDiscardPkt	CBQoS Discarded Pkt	uint32	

EventType: PH_DEV_MON_CCM_CTI_STAT

Description: Cisco Call Manager CTI device status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	
ccmStatus	CCM Status	string	
errReason	Reason for Error	string	This is the reason for an error if given.
lastRegTime	Last Registered Time	Date	

EventType: PH_DEV_MON_CCM_CTI_STAT_CHANGE

Description: Cisco Call Manager CTI device status changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
prevCCMStatus	Prev CCM Status	string	
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_DEL_CTI

Description: Cisco Call Manager CTI device deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_DEL_GW

Description: Cisco Call Manager Gateway deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_DEL_H323

Description: Cisco Call Manager H323 device deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_DEL_MEDIA

Description: Cisco Call Manager Media device deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_DEL_SIP_TRUNK

Description: Cisco Call Manager SIP Trunk Deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_DEL_VM

Description: Cisco Call Manager Voice mail device deleted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_GLOBAL_INFO

Description: Cisco Call Manager Global Device Info

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
regPhone	Registered Phones	uint32	
unregPhone	Unregistered Phones	uint32	
rejPhone	Rejected Phones	uint32	
regGw	Registered Gateways	uint32	
unregGw	Unregistered Gateways	uint32	
rejGw	Rejected Gateways	uint32	
regMedia	Registered Media	uint32	
unregMedia	Unregistered Media	uint32	
rejMedia	Rejected Media	uint32	
regVM	Registered VMail	uint32	
unregVM	Unregistered VMail	uint32	
rejVM	Rejected VMail	uint32	
sipTrunk	SIP Trunks	uint32	

EventType: PH_DEV_MON_CCM_GW_STAT**Description:** Cisco Call Manager Gateway Status**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	
ccmStatus	CCM Status	string	
errReason	Reason for Error	string	This is the reason for an error if given.
lastRegTime	Last Registered Time	Date	

EventType: PH_DEV_MON_CCM_GW_STAT_CHANGE**Description:** Cisco Call Manager Gateway Status Change**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
prevCCMStatus	Prev CCM Status	string	
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_H323_STAT

Description: Cisco Call Manager H323 Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	
ccmStatus	CCM Status	string	
lastRegTime	Last Registered Time	Date	

EventType: PH_DEV_MON_CCM_H323_STAT_CHANGE

Description: Cisco Call Manager H323 Status Change

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
prevCCMStatus	Prev CCM Status	string	
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_MEDIA_STAT

Description: Cisco Call Manager Media device Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	

Id	Display name	Type	Description
ccmStatus	CCM Status	string	
errReason	Reason for Error	string	This is the reason for an error if given.
lastRegTime	Last Registered Time	Date	

EventType: PH_DEV_MON_CCM_MEDIA_STAT_CHANGE

Description: Cisco Call Manager Media device status change

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
prevCCMStatus	Prev CCM Status	string	
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_NEW_CTI

Description: Cisco Call Manager CTI device added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_NEW_GW

Description: Cisco Call Manager Gateway added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_NEW_H323

Description: Cisco Call Manager H323 device added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_NEW_MEDIA

Description: Cisco Call Manager Media device added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_NEW_SIP_TRUNK

Description: Cisco Call Manager SIP Trunk Added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_NEW_VM

Description: Cisco Call Manager Voice Mail device added

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CCM_SIP_TRUNK_STAT

Description: Cisco Call Manager SIP Trunk Statistics

Severity: 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	
srcProto	Source Application Protocol	string	
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destProto	Destination Application Protocol	string	
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_DEV_MON_CCM_VM_STAT

Description: Cisco Call Manager Voice Mail Status**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
description	Description	string	
type	Type	string	
ccmStatus	CCM Status	string	
errReason	Reason for Error	string	This is the reason for an error if given.
lastRegTime	Last Registered Time	Date	

EventType: PH_DEV_MON_CCM_VM_STAT_CHANGE

Description: Cisco Call Manager Voice Mail Status Change

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
prevCCMStatus	Prev CCM Status	string	
ccmStatus	CCM Status	string	
description	Description	string	
type	Type	string	

EventType: PH_DEV_MON_CHANGE_CUST_CONFIG

Description: Config Change detected by custom script

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oldSVNVersion	Old SVN Version	uint32	
newSVNVersion	New SVN Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_CHANGE_INST_SW

Description: New software (un)installed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oldSVNVersion	Old SVN Version	uint32	
newSVNVersion	New SVN Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_CHANGE_RUN_CONFIG**Description:** Running config changed**Severity:** 5 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oldSVNVersion	Old SVN Version	uint32	
newSVNVersion	New SVN Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_CHANGE_RUN_SW**Description:** Running apps changed**Severity:** 5 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_CHANGE_STARTUP_CONFIG**Description:** Startup config changed**Severity:** 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oldSVNVersion	Old SVN Version	uint32	
newSVNVersion	New SVN Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_CISCO_NBAR_STAT

Description: Cisco NBAR statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.
appTransportProto	Application Protocol	string	
totFlows	Total Flows	uint32	Total number of Total (Sent plus Received) Flows. Used in Netflow.
recvFlows	Received Flows	uint32	Total number of Received Flows. Used in Netflow.
sentFlows	Sent Flows	uint32	Total number of Sent Flows. Used in Netflow.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.

Id	Display name	Type	Description
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
totBitsPerSec	Total Bit Rate	double	Total (Sent plus Received) bits/sec through an interface
recvBitsPerSec	Received Bit Rate	double	
sentBitsPerSec	Sent Bit Rate	double	

EventType: PH_DEV_MON_CISCO_RAS_VPN_MET

Description: Remote Access VPN metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
localVpnIpAddr	Local VPN Tunnel IP	IP	
ispVpnIpAddr	ISP VPN IP	IP	
user	User	string	
userGrp	User Group	string	
tunnelStatus	Tunnel Status	string	
tunnelUpTime	Tunnel Uptime	uint64	
rasSessProto	RAS Session Protocol	string	
authenMethod	Authentication Method	string	
authorMethod	Authorization Method	string	
encryptAlgo	Encryption Algorithm	string	

Id	Display name	Type	Description
authenAlgo	Authentication Algorithm	string	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.
sentPktDrop	Sent Packet Drop	uint64	
recvPktDrop	Recv Packet Drop	uint64	

EventType: PH_DEV_MON_CISCO_VPN_P1_TUNNEL_MET

Description: IPSec P1 Tunnel metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
localVpnIpAddr	Local VPN Tunnel IP	IP	
remoteVpnIpAddr	Remote VPN Tunnel IP	IP	
tunnelStatus	Tunnel Status	string	

Id	Display name	Type	Description
tunnelUpTime	Tunnel Uptime	uint64	
sentBitsPerSec	Sent Bit Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
recvBitsPerSec	Received Bit Rate	double	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPktDrop	Sent Packet Drop	uint64	
sentExchReject	Sent Exch Reject	uint64	
sentExchInvalid	Sent Exch Invalid	uint64	
recvPktDrop	Recv Packet Drop	uint64	
recvExchReject	Recv Exch Reject	uint64	
recvExchInvalid	Recv Exch Invalid	uint64	

EventType: PH_DEV_MON_CISCO_VPN_P2_TUNNEL_MET

Description: IPSec P2 Tunnel metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
localVpnIpAddr	Local VPN Tunnel IP	IP	

Id	Display name	Type	Description
remoteVpnIpAddr	Remote VPN Tunnel IP	IP	
tunnelStatus	Tunnel Status	string	
tunnelUpTime	Tunnel Uptime	uint64	
sentBitsPerSec	Sent Bit Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
recvBitsPerSec	Received Bit Rate	double	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPktDrop	Sent Packet Drop	uint64	
sentAuthFail	Sent Auth Fail	uint64	
sentEncryptFail	Sent Encrypt Fail	uint64	
recvPktDrop	Recv Packet Drop	uint64	
recvAuthFail	Recv Auth Fail	uint64	
recvDecryptFail	Recv Decrypt Fail	uint64	
recvReplayFail	Recv Replay Fail	uint64	

EventType: PH_DEV_MON_CISCO_WLAN_RADIO_METRIC

Description: WLAN Radio interface metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
devPort	Device Port	string	Name of the physical network port a device
wlanProtocol	WLAN Protocol	string	WLAN Protocol found in SNMP based WLAN monitoring
ifOperStatus	Interface Oper Status	string	
wlanUserCount	WLAN User count	uint32	WLAN User count found in SNMP based WLAN monitoring
wlanSuppChannels	WLAN Supported Channels	string	WLAN Supported Channels found in SNMP based WLAN monitoring
wlanChannelId	WLAN Channel Id	uint32	WLAN Channel Id found in SNMP based WLAN monitoring
wlanSendUtil	WLAN Transmit Util	uint32	WLAN Transmit Util found in SNMP based WLAN monitoring
wlanRecvUtil	WLAN Receive Util	uint32	WLAN Receive Util found in SNMP based WLAN monitoring
wlanChannelUtil	WLAN Channel Util	uint32	WLAN Channel Util found in SNMP based WLAN monitoring
wlanPoorSNRUserCount	WLAN Poor SNR User count	uint32	WLAN Poor SNR User count found in SNMP based WLAN monitoring
ifLoadProfile	WLAN Interface Load Profile	string	WLAN Interface Load Profile found in SNMP based WLAN monitoring
ifIntefProfile	WLAN Interface Intereference Profile	string	WLAN Interface Intereference Profile found in SNMP based WLAN monitoring
ifCoverageProfile	WLAN Interface Coverage Profile	string	WLAN Interface Coverage Profile found in SNMP based WLAN monitoring
ifNoiseProfile	WLAN Interface Noise Profile	string	WLAN Interface Noise Profile found in SNMP based WLAN monitoring

EventType: PH_DEV_MON_CITRIX_SDWAN_INTF

Description: Citrix SD-WAN Interface metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
ifInteflndx	WLAN Interface Intereference Index	uint32	WLAN Interface Intereference Index found in SNMP based WLAN monitoring
intfName	Host Interface Name	string	Name of a network interface in a host.
sentBytes	Sent Bytes	uint32	Number of bytes sent by a host. This has 32bit resolution.
sentPkts	Sent Packets	uint32	Number of packets sent by a host. This is 32bit version.
recvBytes	Received Bytes	uint32	Number of bytes received by a host. This has 32bit resolution.
recvPkts	Received Packets	uint32	Number of packets received by a host. This is 32bit version.
droppedBytes	Dropped Bytes	uint32	
totPktDrop	Dropped Packets	uint64	Packets dropped

EventType: PH_DEV_MON_CITRIX_SDWAN_LINK

Description: Citrix SD-WAN Link metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
wanLinkId	Wan link ID	uint32	
wanLinkName	Wan link Name	string	
wanLinkState	Wan link State	uint32	
sentBytes	Sent Bytes	uint32	Number of bytes sent by a host. This has 32bit resolution.

Id	Display name	Type	Description
sentPkts	Sent Packets	uint32	Number of packets sent by a host. This is 32bit version.
recvBytes	Received Bytes	uint32	Number of bytes received by a host. This has 32bit resolution.
recvPkts	Received Packets	uint32	Number of packets received by a host. This is 32bit version.
droppedBytes	Dropped Bytes	uint32	
totPktDrop	Dropped Packets	uint64	Packets dropped
addressType	Address Type	string	
serverIpAddr	Server IP	IP	
lanToWanRate	Lan To Wan Rate	uint64	
wanToLanRate	Wan To Lan Rate	uint64	
lanToWanAllowedRate	Lan To Wan Allowed Rate	uint64	
wanToLanAllowedRate	Wan To Lan Allowed Rate	uint64	

EventType: PH_DEV_MON_CLARION_ARRAY_UTIL

Description: Clarion/VNX Storage Array utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	

Id	Display name	Type	Description
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
availDiskMB	Available Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
hwHotSpareDiskCount	Hot Spare Disk Count	uint32	

EventType: PH_DEV_MON_CLARION_DISK_HEALTH

Description: Clarion/VNX Disk health

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
totDisk	Total Disk Count	uint32	Total number of Disks
totalDiskMB	Total Disk MB	uint32	
activeDisk	Active Disk Count	uint32	Total number of Active Disks
failedDisk	Failed Disk Count	uint32	Total number of Failed Disks
spareDisk	Spare Disk Count	uint32	Total number of Spare Disks

EventType: PH_DEV_MON_CLARION_HOST_CONN

Description: Host to Clarion/VNX Fiber channel Connections

Severity: 1 (Low)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcWWN	Source FiberChannel WWN Id	string	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
spPortName	SAN Storage Port Name	string	
fcLoginStatus	SAN FC Login Status	uint32	
fcRegStatus	SAN FC Registration Status	uint32	
lunNameList	SAN LUN Name List	string	
sgName	SAN Storage Group Name	string	

EventType: PH_DEV_MON_CLARION_LUN_UTIL**Description:** Clarion/VNX LUN utilization metric**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
lunName	LUN Name	string	
lunNumber	LUN Number	uint32	

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	

EventType: PH_DEV_MON_CLARION_PER_HOST_LUN_UTIL

Description: Per host Clarion/VNX LUN utilization metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
lunName	LUN Name	string	
lunNumber	LUN Number	uint32	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
pollIntv	Polling Interval	uint32	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	

EventType: PH_DEV_MON_CLARION_PORT_UTIL

Description: Clarion/VNX Storage Port utilization metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
spPortName	SAN Storage Port Name	string	

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	

EventType: PH_DEV_MON_CLARION_RG_UTIL

Description: Clarion/VNX RAID Group utilization metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
raidGrpId	RAID Group Id	uint32	
raidType	RAID Type	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	

Id	Display name	Type	Description
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	

EventType: PH_DEV_MON_CLARION_SP_UTIL

Description: Clarion/VNX Storage Processor utilization metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
spName	SAN Storage Processor Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
cpuUtil	CPU Util	double	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	

EventType: PH_DEV_MON_CLARION_STORAGE_USAGE

Description: Clarion/VNX Storage space utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
usageType	Usage Type	string	
diskUsage	Disk Used MB	uint64	

EventType: PH_DEV_MON_CLARION_STORE_POOL_UTIL

Description: Clarion/VNX Storage pool utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
spoolName	Storage Pool Name	string	
raidType	RAID Type	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
diskReadReqPerSec	Disk Read Rate req/sec	double	

Id	Display name	Type	Description
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskRWReqPerSec	Disk RW Rate req/sec	double	
diskRWKBytesPerSec	Disk RW Rate KBps	double	

EventType: PH_DEV_MON_CLARION_UNREG_HOST

Description: Logged in but not yet registered Host at EMC CLarion

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcWWN	Source FiberChannel WWN Id	string	
spPortName	SAN Storage Port Name	string	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DEV_MON_CLOUD_SERVICE_HEARTBEAT

Description: Cloud service heartbeat

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
reptVendor	Reporting Vendor	string	This field captures the vendor of the reported event
reptModel	Reporting Model	string	This field captures the model of the reported event
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
version	Version	string	
domain	Domain	string	

EventType: PH_DEV_MON_CMDB_DISK_PRUNE_FAILED

Description: CMDB free Disk fell below the low threshold and inspite of pruning older incidents and identity / location data, CMDB free Disk stays below high threshold. User need to reduce the number of months of incidents and identity / location data in CMDB.

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CMDB_DISK_PRUNE_SUCCESS

Description: CMDB free Disk fell below the low threshold and old incidents and identity / location data were pruned to bring the CMDB free Disk above high threshold

Severity: 4 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CUST_FILE_CHANGE_ATTRIB

Description: File or directory ownership or access permission changed

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CUST_FILE_CHANGE_CONTENT

Description: File or directory content hash changed

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CUST_FILE_CREATE

Description: New file or directory created

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CUST_FILE_DELETE

Description: New file or directory deleted

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CUST_FILE_SCAN

Description: Files scanned with hashes

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_CUST_TARGET_FILE_CHANGE

Description: Target file content changed from gold standard

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_DATASTORE_UTIL

Description: Datastore utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_DC DIAG

Description: Windows Active Directory DC DIAG command output

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_DD NS_UPDATE_STAT

Description: InfoBlox DDNS Update performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
ddnsUpdateSuccess	DDNS Successful Updates	uint32	
ddnsUpdateFail	DDNS Failed Updates	uint32	
dynDnsUpdRej	Dynamic DNS Update Rejected	uint32	
ddnsUpdatePrereqRej	DDNS Prereq Rejected Updates	uint32	
ddnsUpdateLatency	DDNS Update latency	uint32	
dynDnsUpdTimeout	Dynamic DNS Update Timeout	uint32	

EventType: PH_DEV_MON_DELLFORCE10_EXT_INTF_UTIL

Description: Network Interface extended utilization stats for Dell Force10 device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
intfAlias	Host Interface Alias	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
inVlanPktsPerSec	Recv Valid VLAN Tagged Frame Rate	double	
inOverrunsPerSec	Recv Buffer Overrun Rate	double	
outVlanPktsPerSec	Sent Valid VLAN Tagged Frame rate	double	
outUnderrunsPerSec	Sent Buffer Underrun Rate	double	
outUnicastsPerSec	Sent Unicast Frames rate	double	
outCollisionsPerSec	Sent Frame Collision rate	double	
outWredDropsPerSec	Sent WRED Drop Rate	double	

EventType: PH_DEV_MON_DELL_BLADE_POWER_STATUS

Description: Dell Blade Server Chassis Power Utilization metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
maxSpecEnvPower	Max Spec Power Watt	double	
potentialEnvPower	Potential Power Watt	double	
idleEnvPower	Idle Power Watt	double	

Id	Display name	Type	Description
surplusEnvPower	Surplus Power Watt	double	
peakEnvPower	Peak Power Watt	double	
minEnvPower	Minimum Power Watt	double	
envPower	Power Watt	double	
envCurrentAmp	Current Amp	double	

EventType: PH_DEV_MON_DELL_BLADE_PSU_STATUS

Description: Dell Blade Server Power Supply Utilization metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorLoc	Sensor Location	string	
envPower	Power Watt	double	
envCurrentAmp	Current Amp	double	
envVoltage	Voltage	double	

EventType: PH_DEV_MON_DELTA_CONFIG

Description: Running config different than startup config

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
startUpConfVer	StartUp Config Version	uint32	
runningConfVer	Running Config Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_DGA_DETECTED

Description: FortiSIEM detected host names created via Domain Generation Algorithm

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
relayDevIpAddr	Relaying IP	IP	Relaying IP is most commonly used to specify the log relay appliance, usually a collector.
relayDevName	Relaying Device	string	This is the hostname of the relaying device, a log relay, which is most typically a FortiSIEM collector.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
domainEntropy	Domain Name Entropy	double	

EventType: PH_DEV_MON_DHCP_SUBNET_USAGE

Description: InfoBlox DHCP subnet usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
dhcpSubnetAddr	DHCP Subnet Address	IP	
dhcpSubnetMask	DHCP Subnet Mask	IP	
dhcpSubnetUsed	DHCP Subnet Usage pct	uint32	

EventType: PH_DEV_MON_DISK_IO_UTIL

Description: Disk IO Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskIOUtil	Disk IO Util	double	
devDiskRWLatency	Disk Read/Write Latency	double	

Id	Display name	Type	Description
appDiskRWLatency	Disk Appl Read/Write Latency	double	
diskTfrKBytesPerSec	Disk Transfer Rate KBps	double	
diskNumofSeeksPerSec	Disk Number of Seeks	double	
diskType	Disk Type	string	
pollIntv	Polling Interval	uint32	
devDiskRdLatency	Disk Read Latency ms	double	
devDiskWrLatency	Disk Write Latency ms	double	
diskQLen	Disk Queue Length	uint32	

EventType: PH_DEV_MON_DISK_MON_SKIP

Description: Disk/Volume Monitoring skipped by policy

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	

EventType: PH_DEV_MON_DNS_CLUST_REPL_STAT

Description: InfoBlox DNS CLuster replication metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
dnsReplQueueStatus	DNS Replication Queue Status	string	
dnsSentQueueFromMaster	DNS Sent Queue From Master	uint32	
dnsLastSentTimeFromMaster	DNS Sent Time From Master	string	
dnsSentQueueToMaster	DNS Sent Queue To Master	uint32	
dnsLastSentTimeToMaster	DNS Sent Time To Master	string	

EventType: PH_DEV_MON_DNS_PERF_STAT

Description: InfoBlox DNS Performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
nonAuthDNSQueryCount	NonAuth DNS Query Count	uint32	
nonAuthDNSAvgLatency	Avg NonAuth DNS Latency ms	uint32	
authDNSQueryCount	Auth DNS Query Count	uint32	

Id	Display name	Type	Description
authDNSAvgLatency	Avg Auth DNS Latency ms	uint32	
dnsInvalidPort	Invalid DNS Port Response	uint32	
dnsInvalidTxId	Invalid DNS TXID Response	uint32	

EventType: PH_DEV_MON_DNS_ZONETX_MET

Description: InfoBlox DNS Zone Transfer metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
dnsZone	DNS Zone Name	string	
dnsRespSent	DNS Responses Sent	uint32	
dnsFailedQuery	DNS Failed Queries	uint32	
dnsReferral	DNS Referrals	uint32	
dnsQueryNxRecord	DNS Non-existent Record Queries	uint32	
dnsQueryNxDomain	DNS Non-existent Domain Queries	uint32	
dnsRecQueryRecv	Recursive DNS Query Recvd	uint32	

EventType: PH_DEV_MON_DST_AD_REPL_STAT

Description: Windows Active Directory Destination REPLSTAT command output

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_EBS_METRIC

Description: AWS EBS metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
volumeId	AWS Volume Id	string	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
ioReadsPerSec	Total Read I/Os Rate	double	
ioWritesPerSec	Total Write I/Os Rate	double	
diskQLen	Disk Queue Length	uint32	

EventType: PH_DEV_MON_EC2_INSTANCE_DOWN

Description: AWS EC2 instance went down

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
ec2InstanceId	EC2 Instance Id	string	
accountId	Account Id	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_EC2_INSTANCE_UP

Description: AWS EC2 instance came back up

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
ec2InstanceId	EC2 Instance Id	string	
accountId	Account Id	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_EC2_METRIC

Description: Amazon Web Services EC2 status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cpuUtil	CPU Util	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	

EventType: PH_DEV_MON EMC_DATADOMAIN_DISK_PERF

Description: EMC Data Domain disk performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
diskSectorsReadPerSec	Disk Sector Reads/sec	double	

Id	Display name	Type	Description
diskSectorsWrittenPerSec	Disk Sector Writes/sec	double	
diskTfrKBytesPerSec	Disk Transfer Rate KBps	double	
diskIOUtil	Disk IO Util	double	
hwDiskStatus	Hardware Disk Status	uint16	Hardware Disk Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)

EventType: PH_DEV_MON EMC_DATADOMAIN_OVERALL_PERF

Description: EMC Data Domain overall performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskIOUtil	Disk IO Util	double	
nvrReadKBytesPerSec	NVRAM Reads KBps	double	
nvrWriteKBytesPerSec	NVRAM Writes KBps	double	
replInKBytesPerSec	Replication Recvd KBps	double	
replOutKBytesPerSec	Replication Writes KBps	double	
nfsOpsPerSec	NFS Request Rate	double	
nfsProcPercentage	NFS Processing Pct	double	
nfsSendPercentage	NFS Send Pct	double	
nfsReceivePercentage	NFS Recv Pct	double	
cifsOpsPerSec	CIFS Request Rate	double	

EventType: PH_DEV_MON_EQL_CONN_MET

Description: EqualLogic connection performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
sanConnCount	SAN Connection Count	uint32	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
devDiskRdLatency	Disk Read Latency ms	double	
devDiskWrLatency	Disk Write Latency ms	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	

EventType: PH_DEV_MON_EQL_DISK_HEALTH

Description: EqualLogic disk status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
totDisk	Total Disk Count	uint32	Total number of Disks
activeDisk	Active Disk Count	uint32	Total number of Active Disks
failedDisk	Failed Disk Count	uint32	Total number of Failed Disks
spareDisk	Spare Disk Count	uint32	Total number of Spare Disks

EventType: PH_DEV_MON_EQL_DISK_MET

Description: EqualLogic disk level performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
diskIOUtil	Disk IO Util	double	
ioQueue	Disk IO Queue	uint32	
diskTransferRate	Disk Transfer Rate/sec	double	

EventType: PH_DEV_MON_EQL_GROUP_MET

Description: EqualLogic group level performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
totalStorageMB	Total Storage MB	uint32	
usedStorageMB	Used Storage MB	uint32	
resvStorageMB	Reserved Storage MB	uint32	
resvUsedStorageMB	Reserved Used Disk MB	uint32	
totalVolume	Total Volumes	uint32	
usedVolume	Used Volumes	uint32	
onlineVolume	Online Volumes	uint32	
totalSnapshot	Total Snapshots	uint32	
usedSnapshot	Used Snapshots	uint32	
onlineSnapshot	Online Snapshots	uint32	

EventType: PH_DEV_MON_ESX_DATASTORE_IO

Description: ESX Datastore IO stats

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_ESX_DISK_IO

Description: ESX Disk IO stats

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_ESX_DISK_UTIL

Description: ESX datastore utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_ESX_STATE

Description: Physical Machine State

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_ESX_UPTIME

Description: ESX server's up time

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_EUM_FAIL

Description: Synthetic transaction monitor failed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
appPort	Application Port	string	This field represents the port that an application uses.
appTransportProto	Application Protocol	string	
endUserMonitorName	Synthetic Transaction Monitor Name	string	This is the name of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI
endUserMonitorStep	Synthetic Transaction Monitor Step	string	This is the step of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI. An STM job can have many steps, and an event is generated for every step.

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
srcProto	Source Application Protocol	string	
srcUser	Source User	string	
destUser	Destination User	string	
mailSubject	Mail Subject	string	

EventType: PH_DEV_MON_EUM_INTERNAL_ERR

Description: Synthetic transaction monitoring failed because of internal error

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
appPort	Application Port	string	This field represents the port that an application uses.
appTransportProto	Application Protocol	string	
endUserMonitorName	Synthetic Transaction Monitor Name	string	This is the name of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
srcProto	Source Application Protocol	string	
srcUser	Source User	string	
destUser	Destination User	string	
mailSubject	Mail Subject	string	

EventType: PH_DEV_MON_EUM_STATUS

Description: Synthetic transaction monitor status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
appPort	Application Port	string	This field represents the port that an application uses.
appTransportProto	Application Protocol	string	
endUserMonitorName	Synthetic Transaction Monitor Name	string	This is the name of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI

Id	Display name	Type	Description
endUserMonitorStep	Synthetic Transaction Monitor Step	string	This is the step of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI. An STM job can have many steps, and an event is generated for every step.
newStatus	New Status	string	
sysDownTime	System Downtime	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_EUM_SUCCESS

Description: Synthetic transaction monitor succeeded

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appGroupName	Application Group Name	string	
appPort	Application Port	string	This field represents the port that an application uses.
appTransportProto	Application Protocol	string	
endUserMonitorName	Synthetic Transaction Monitor Name	string	This is the name of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI
endUserMonitorStep	Synthetic Transaction Monitor Step	string	This is the step of the Synthetic Transaction Monitor (STM) performance job defined in FortiSIEM GUI. An STM job can have many steps, and an event is generated for every step.
appResponseTimeMSec	Application Response Time	uint32	

Id	Display name	Type	Description
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
srcProto	Source Application Protocol	string	
srcUser	Source User	string	
destUser	Destination User	string	
mailSubject	Mail Subject	string	

EventType: PH_DEV_MON_F5_ACTIVE_CONN

Description: F5 Active Connection Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
clientConns	Client Connections	uint64	
serverConns	Server Connections	uint64	
pvaClientConns	PVA Client Connections	uint32	
pvaServerConns	PVA Server Connections	uint32	
sslClientConns	SSL Client Connections	uint32	
sslServerConns	SSL Server Connections	uint32	

EventType: PH_DEV_MON_F5_LTM_NODE_STAT**Description:** F5 LTM Node Statistics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serverIpAddr	Server IP	IP	
statusDetailedReason	Status Detail Reason	string	
ratio	Ratio	double	
monitorState	Monitor State	string	
monitorStatus	Monitor Status	string	
sessionStatus	Session Status	string	
availState	Availability State	string	
enabledState	Enabled State	string	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
recvPktsPerSec	Received Packet Rate	double	Received Packet rate (packets/sec)
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
recvBytesPerSec	Received Byte Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
sentPktsPerSec	Sent Packet Rate	double	Sent Packet rate (packets/sec)
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
sentBytesPerSec	Sent Byte Rate	double	
peakConns	Peak Connections	uint64	
totConns	Total Connections	uint64	
totConnsPerSec	Total Connections/sec	double	

Id	Display name	Type	Description
activeConns	Active Connection	uint64	
pvaRecvPkts	Received PVA Packets	uint64	
pvaRecvPktsPerSec	Received PVA Pkts/sec	double	
pvaRecvBytes	Received PVA Bytes	uint64	
pvaRecvBytesPerSec	Received PVA Bps	double	
pvaSentPkts	Sent PVA Packets	uint64	
pvaSentPktsPerSec	Sent PVA Pkts/sec	double	
pvaSentBytes	Sent PVA Bytes	uint64	
pvaSentBytesPerSec	Sent PVA Bps	double	
pvaMaxConns	Max PVA Connections	uint64	
pvaTotConns	Total PVA Connections	uint64	
pvaTotConnsPerSec	PVA Connections/sec	double	
pvaCurrConns	Current PVA Connections	uint64	
totRequests	Total Requests	uint64	
totRequestsPerSec	Requests/sec	double	
pvaAssistTotConns	Total PVA Assisted Connections	uint64	
pvaAssistTotConnsPerSec	PVA Assisted Connections/sec	double	
pvaAssistCurrConns	Assisted PVA Connections	uint64	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_LTM_POOL_MEMBER_STAT

Description: F5 LTM Pool Member Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serverIpAddr	Server IP	IP	
poolName	Pool Name	string	
statusDetailedReason	Status Detail Reason	string	
memberPort	Member Port	uint16	
ratio	Ratio	double	
monitorState	Monitor State	string	
monitorStatus	Monitor Status	string	
sessionStatus	Session Status	string	
availState	Availability State	string	
enabledState	Enabled State	string	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
recvPktsPerSec	Received Packet Rate	double	Received Packet rate (packets/sec)
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
recvBytesPerSec	Received Byte Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
sentPktsPerSec	Sent Packet Rate	double	Sent Packet rate (packets/sec)
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
sentBytesPerSec	Sent Byte Rate	double	
peakConns	Peak Connections	uint64	
totConns	Total Connections	uint64	
totConnsPerSec	Total Connections/sec	double	
activeConns	Active Connection	uint64	
pvaRecvPkts	Received PVA Packets	uint64	
pvaRecvPktsPerSec	Received PVA Pkts/sec	double	

Id	Display name	Type	Description
pvaRecvBytes	Received PVA Bytes	uint64	
pvaRecvBytesPerSec	Received PVA Bps	double	
pvaSentPkts	Sent PVA Packets	uint64	
pvaSentPktsPerSec	Sent PVA Pkts/sec	double	
pvaSentBytes	Sent PVA Bytes	uint64	
pvaSentBytesPerSec	Sent PVA Bps	double	
pvaMaxConns	Max PVA Connections	uint64	
pvaTotConns	Total PVA Connections	uint64	
pvaTotConnsPerSec	PVA Connections/sec	double	
pvaCurrConns	Current PVA Connections	uint64	
totRequests	Total Requests	uint64	
totRequestsPerSec	Requests/sec	double	
pvaAssistTotConns	Total PVA Assisted Connections	uint64	
pvaAssistTotConnsPerSec	PVA Assisted Connections/sec	double	
pvaAssistCurrConns	Assisted PVA Connections	uint64	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_LTM_POOL_STAT

Description: F5 LTM Pool Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
poolName	Pool Name	string	
poolLbMode	Pool Loadbalance Mode	string	
poolMemberCount	Pool Member Count	uint64	
availState	Availability State	string	
enabledState	Enabled State	string	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
recvPktsPerSec	Received Packet Rate	double	Received Packet rate (packets/sec)
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
recvBytesPerSec	Received Byte Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
sentPktsPerSec	Sent Packet Rate	double	Sent Packet rate (packets/sec)
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
sentBytesPerSec	Sent Byte Rate	double	
peakConns	Peak Connections	uint64	
totConns	Total Connections	uint64	
totConnsPerSec	Total Connections/sec	double	
activeConns	Active Connection	uint64	
pvaRecvPkts	Received PVA Packets	uint64	
pvaRecvPktsPerSec	Received PVA Pkts/sec	double	
pvaRecvBytes	Received PVA Bytes	uint64	
pvaRecvBytesPerSec	Received PVA Bps	double	
pvaSentPkts	Sent PVA Packets	uint64	
pvaSentPktsPerSec	Sent PVA Pkts/sec	double	
pvaSentBytes	Sent PVA Bytes	uint64	
pvaSentBytesPerSec	Sent PVA Bps	double	
pvaMaxConns	Max PVA Connections	uint64	
pvaTotConns	Total PVA Connections	uint64	
pvaTotConnsPerSec	PVA Connections/sec	double	

Id	Display name	Type	Description
pvaCurrConns	Current PVA Connections	uint64	
pvaAssistTotConns	Total PVA Assisted Connections	uint64	
pvaAssistTotConnsPerSec	PVA Assisted Connections/sec	double	
pvaAssistCurrConns	Assisted PVA Connections	uint64	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_LTM_VIRT_ADDR_STAT

Description: F5 LTM Virtual Address Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serverIpAddr	Server IP	IP	
availState	Availability State	string	
enabledState	Enabled State	string	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
recvPktsPerSec	Received Packet Rate	double	Received Packet rate (packets/sec)
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
recvBytesPerSec	Received Byte Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
sentPktsPerSec	Sent Packet Rate	double	Sent Packet rate (packets/sec)

Id	Display name	Type	Description
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
sentBytesPerSec	Sent Byte Rate	double	
peakConns	Peak Connections	uint64	
totConns	Total Connections	uint64	
totConnsPerSec	Total Connections/sec	double	
activeConns	Active Connection	uint64	
pvaRecvPkts	Received PVA Packets	uint64	
pvaRecvPktsPerSec	Received PVA Pkts/sec	double	
pvaRecvBytes	Received PVA Bytes	uint64	
pvaRecvBytesPerSec	Received PVA Bps	double	
pvaSentPkts	Sent PVA Packets	uint64	
pvaSentPktsPerSec	Sent PVA Pkts/sec	double	
pvaSentBytes	Sent PVA Bytes	uint64	
pvaSentBytesPerSec	Sent PVA Bps	double	
pvaMaxConns	Max PVA Connections	uint64	
pvaTotConns	Total PVA Connections	uint64	
pvaTotConnsPerSec	PVA Connections/sec	double	
pvaCurrConns	Current PVA Connections	uint64	
pvaAssistTotConns	Total PVA Assisted Connections	uint64	
pvaAssistTotConnsPerSec	PVA Assisted Connections/sec	double	
pvaAssistCurrConns	Assisted PVA Connections	uint64	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_LTM_VIRT_SERVER_STAT

Description: F5 LTM Virtual Server Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
virtServerName	Virtual Server name	string	
statusDetailedReason	Status Detail Reason	string	
virtServerPort	Virtual Server Port	uint16	
availState	Availability State	string	
enabledState	Enabled State	string	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
recvPktsPerSec	Received Packet Rate	double	Received Packet rate (packets/sec)
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
recvBytesPerSec	Received Byte Rate	double	
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
sentPktsPerSec	Sent Packet Rate	double	Sent Packet rate (packets/sec)
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
sentBytesPerSec	Sent Byte Rate	double	
peakConns	Peak Connections	uint64	
totConns	Total Connections	uint64	
totConnsPerSec	Total Connections/sec	double	
activeConns	Active Connection	uint64	
pvaRecvPkts	Received PVA Packets	uint64	
pvaRecvPktsPerSec	Received PVA Pkts/sec	double	
pvaRecvBytes	Received PVA Bytes	uint64	
pvaRecvBytesPerSec	Received PVA Bps	double	
pvaSentPkts	Sent PVA Packets	uint64	
pvaSentPktsPerSec	Sent PVA Pkts/sec	double	
pvaSentBytes	Sent PVA Bytes	uint64	

Id	Display name	Type	Description
pvaSentBytesPerSec	Sent PVA Bps	double	
pvaMaxConns	Max PVA Connections	uint64	
pvaTotConns	Total PVA Connections	uint64	
pvaTotConnsPerSec	PVA Connections/sec	double	
pvaCurrConns	Current PVA Connections	uint64	
totRequests	Total Requests	uint64	
totRequestsPerSec	Requests/sec	double	
pvaAssistTotConns	Total PVA Assisted Connections	uint64	
pvaAssistTotConnsPerSec	PVA Assisted Connections/sec	double	
pvaAssistCurrConns	Assisted PVA Connections	uint64	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_NEW_CONN

Description: F5 New Connnection Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
tcpClientAcceptsPerSec	TCP Client Connection Accept Rate	double	
tcpClientConnsPerSec	TCP Client Connection Rate	double	
serverConnsPerSec	Server Connection Rate	double	
clientConnsPerSec	Client Connection Rate	double	

Id	Display name	Type	Description
pvaClientConnsPerSec	PVA Client Connection Rate	double	
pvaServerConnsPerSec	PVA Server Connection Rate	double	
sslClientConnsPerSec	SSL Client Connection Rate	double	
sslServerConnsPerSec	SSL Server Connection Rate	double	
httpRequestsPerSec	HTTP Request Rate	double	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_RAM_CACHE

Description: F5 RAM Cache Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
httpRAMCacheHitRate	HTTP Cache Hit Rate	double	
httpRAMCacheHitByteRate	HTTP Cache Byte Hit Rate	double	
httpRAMCacheEvictionRate	HTTP cache Eviction Rate	double	

EventType: PH_DEV_MON_F5_THROUGHPUT

Description: F5 Throughput Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
clientTotBitsPerSec	Client Total bps	double	
serverTotBitsPerSec	Server Total bps	double	
httpCompressionBitsPerSec	HTTP Compression bps	double	
clientInBitsPerSec	Client Recv bps	double	
clientOutBitsPerSec	Client Sent bps	double	
serverInBitsPerSec	Server Recv bps	double	
serverOutBitsPerSec	Server Sent bps	double	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_F5_TMM_MEM_UTIL

Description: F5 per TMM memory utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
tmmName	F5 TMM Name	string	
memUtil	Memory Util	double	
totalMemKB	Total Memory	uint32	
freeMemKB	Free Memory	uint32	
usedMemKB	Used Memory	uint32	

EventType: PH_DEV_MON_FGT_SEC_POSTURE_DETAILS

Description: FortiGate Security Posture - Per device audit details

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
type	Type	string	
subtype	Subtype	string	
eventSeverityCat	Event Severity Category	string	It takes 3 values - High, Medium and Low based on Event Severity. (1-4 : Low, 5-8 : Medium, 9-10 : High)
deviceType	Device Type	string	
serialNumber	Serial Number	string	
auditScore	Audit Score	double	
status	Status	string	

EventType: PH_DEV_MON_FGT_SEC_POSTURE_DETECTED_ENDPOINTS

Description: FortiGate Security Posture - Detected Endpoint Types

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
totGenericDevs	Total Generic Devices	uint32	
totFortigateDevs	Total FortiGates	uint32	
totFortimgrDevs	Total FortiManager	uint32	

Id	Display name	Type	Description
totFortisandboxDevs	Total FortiSandbox Devices	uint32	
totWindowsDevs	Total Windows Devices	uint32	
totLinuxDevs	Total Linux Devices	uint32	
totAppleDevs	Total Apple Devices	uint32	
totMobileDevs	Total Mobile Devices	uint32	

EventType: PH_DEV_MON_FGT_SEC_POSTURE_FABRIC_GRADE

Description: FortiGate Security Posture - Overall Fabric Grade

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
letterGrade	Letter Grade	string	

EventType: PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_GRADE

Description: FortiGate Security Posture - Per category grade

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
type	Type	string	
gradePercent	Grade Percentage	uint32	
letterGrade	Letter Grade	string	
eventSeverityCat	Event Severity Category	string	It takes 3 values - High, Medium and Low based on Event Severity. (1-4 : Low, 5-8 : Medium, 9-10 : High)
totalNum	Total Number of Items	uint32	

EventType: PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_STATS

Description: FortiGate Security Posture - Per category summary

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
type	Type	string	
totalChecks	Total Checks	uint32	
totalFailedChecks	Total Failed Checks	uint32	
totalExemptChecks	Total Exempt Checks	uint32	
totalPassedChecks	Total Passed Checks	uint32	
totalRecommendations	Total Recommendations	uint32	
auditScore	Audit Score	double	
lowSevCount	Low Severity Count	uint32	
mediumSevCount	Medium Severity Count	uint32	
highSevCount	High Severity Count	uint32	

Id	Display name	Type	Description
criticalSevCount	Critical Severity Count	uint32	

EventType: PH_DEV_MON_FGT_SEC_POSTURE_PER_DEVICE_STATS

Description: FortiGate Security Posture - Per device summary

Severity: 4 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
serialNumber	Serial Number	string	
totalChecks	Total Checks	uint32	
totalFailedChecks	Total Failed Checks	uint32	
totalExemptChecks	Total Exempt Checks	uint32	
totalPassedChecks	Total Passed Checks	uint32	
totalRecommendations	Total Recommendations	uint32	
auditScore	Audit Score	double	
lowSevCount	Low Severity Count	uint32	
mediumSevCount	Medium Severity Count	uint32	
highSevCount	High Severity Count	uint32	
criticalSevCount	Critical Severity Count	uint32	

EventType: PH_DEV_MON_FGT_USER_INFO

Description: FortiGate User Device Informational Event

Severity: 4 (Low)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostVendor	Host Vendor	string	This field captures the vendor of the reported event
hostMACAddr	Host MAC	string	Host Layer 2 MAC Address in the log
vdom	Virtual Domain	string	
osName	Operating System Name	string	
osVersion	Operating System Version	string	
userFullName	User Full Name	string	
lastSeenTime	Last Seen Time	Date	
appName	Application Name	string	
user	User	string	
firstSeenTime	First Seen Time	Date	
tagName	Tag Name	string	
emsSerialNumber	FortiEMS Serial Number	string	
srcAppVersion	Source App Version	string	
discoveryDomain	Discovery Domain	string	
purdueLevel	Purdue Level	double	
vulnCount	Vulnerability Count	uint64	
vulnCountCritical	Vulnerability Count Critical	uint16	
vulnCountHigh	Vulnerability Count High	uint16	
vulnCountMedium	Vulnerability Count Medium	uint16	

Id	Display name	Type	Description
vulnCountLow	Vulnerability Count Low	uint16	
vulnCountInfo	Vulnerability Count Info	uint16	

EventType: PH_DEV_MON_FILE_CONTENT_CHANGE

Description: Monitored file modified

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
fileName	File Name	string	
hashCode	Hash Code	string	
oldSVNVersion	Old SVN Version	uint32	
newSVNVersion	New SVN Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	
user	User	string	
hashAlgo	Hash Algorithm	string	

EventType: PH_DEV_MON_FIREAMP_DISCOVERY_CLIENT_APP

Description: FireAMP Client App discovery event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
clientAppId	Client App Id	uint32	
appName	Application Name	string	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_DISCOVERY_NETWORK_PROTOCOL

Description: FireAMP Network App discovery event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_DISCOVERY_OS_FINGERPRINT

Description: FireAMP OS discovery event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
fingerprintId	Fingerprint	string	
osType	Operating System	string	
hostVendor	Host Vendor	string	This field captures the vendor of the reported event
osVersion	Operating System Version	string	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_DISCOVERY_SERVER

Description: FireAMP Server discovery event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
applicationId	Application Id	uint32	
appTransportProto	Application Protocol	string	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_FILE

Description: FireAMP File Analysis event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
envSensorId	Env Sensor Id	string	
deviceTime	Device Time	Date	This is the timestamp as seen in the raw log. This is converted and stored as epoch milliseconds. Note that the deviceTime, or event occur time, is different than the event receive time by the SIEM.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
fileName	File Name	string	
hashAlgo	Hash Algorithm	string	
hashCode	Hash Code	string	
fileSize64	File Size64 Bytes	uint64	
fileDirection	File Direction	uint16	
fireAmpDisposition	FireAmp Disposition	uint16	
fireAmpSperoDisposition	FireAmp Spero Disposition	uint16	
fireAmpFileStorageStatus	FireAmp File Storage Status	uint16	
fireAmpFileAnalysisStatus	FireAmp File Analysis Status	uint16	
threatScore	Threat Score	uint16	
fireAmpFileAction	FireAmp File Action	uint16	
fileType	File Type	string	
applicationId	Application Id	uint32	

Id	Display name	Type	Description
destUserId	Destination User Id	uint32	
infoURL	Informational URL	string	This field captures an URL if present in an event
signatureName	Signature Name	string	
accessCtlPolicyId	Access Control Policy Id	uint32	
srcGeoCountryCode	Source Country Number	uint32	
destGeoCountryCode	Destination Country Number	uint32	
webAppId	Web App Id	uint32	
clientAppId	Client App Id	uint32	
connCounter	Connection Counter	uint64	
connEventTime	Connection Event Time	Date	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_IMPACT_FLAG

Description: FireAMP Impact Flag event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
envSensorId	Env Sensor Id	string	
snortEventId	Snort Event ID	uint64	Event ID of a Snort IPS Device

Id	Display name	Type	Description
deviceTime	Device Time	Date	This is the timestamp as seen in the raw log. This is converted and stored as epoch milliseconds. Note that the deviceTime, or event occur time, is different than the event receive time by the SIEM.
eventType	Event Type	string	This is the unique log name, identifying the product and type of log. This is a key attribute for most queries.
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.
ipsGeneratorId	IPS Generator Id	uint64	
ipsSignatureId	Signature Id	uint64	
ipsClassificationId	IPS Classification Id	uint64	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
fireAmpImpactFlag	FireAmp Impact Flag	uint16	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_INTRUSION

Description: FireAMP Intrusion event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
envSensorId	Env Sensor Id	string	
snortEventId	Snort Event ID	uint64	Event ID of a Snort IPS Device
deviceTime	Device Time	Date	This is the timestamp as seen in the raw log. This is converted and stored as epoch milliseconds. Note that the deviceTime, or event occur time, is different than the event receive time by the SIEM.
eventType	Event Type	string	This is the unique log name, identifying the product and type of log. This is a key attribute for most queries.
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.
ipsGeneratorId	IPS Generator Id	uint64	
ipsSignatureId	Signature Id	uint64	
ipsClassificationId	IPS Classification Id	uint64	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
iocNum	IOC Number	uint32	
fireAmpImpactFlag	FireAmp Impact Flag	uint16	
fireAmpImpact	FireAmp Impact	uint16	
eventAction	Event Action	uint16	This is an unsigned integer boolean. 0 means permitted, 1 means blocked. It is used by various parsers to indicate success / failure or permit/deny.
mplsLabel	MPLS Label	uint32	
hostVLAN	Host VLAN	uint16	Host VLAN Number
userId	User Id	string	

Id	Display name	Type	Description
webAppId	Web App Id	uint32	
clientAppId	Client App Id	uint32	
appProtold	App Proto Id	uint32	
fwRule	Firewall Rule	string	Firewall Rule Name
policyName	Policy Name	string	
srcIntfName	Source Interface Name	string	Name of the network interface through which a packet enters a network device. This information is typically present in Firewall logs.
destIntfName	Destination Interface Name	string	Name of the network interface through which a packet exits a network device. This information is typically present in Firewall logs.
srcFwZone	Source Firewall Zone	string	Source Firewall Zone found in Firewall logs
destFwZone	Destination Firewall Zone	string	Destination Firewall Zone found in Firewall logs
connEventTime	Connection Event Time	Date	
connCounter	Connection Counter	uint64	
srcGeoCountryCode	Source Country Number	uint32	
destGeoCountryCode	Destination Country Number	uint32	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_MALWARE

Description: FireAMP Malware event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
envSensorId	Env Sensor Id	string	
deviceTime	Device Time	Date	This is the timestamp as seen in the raw log. This is converted and stored as epoch milliseconds. Note that the deviceTime, or event occur time, is different than the event receive time by the SIEM.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
fileName	File Name	string	
filePath	File Path	string	
fileSize64	File Size64 Bytes	uint64	
fileType	File Type	string	
fileTimestamp	File Timestamp	Date	
hashAlgo	Hash Algorithm	string	
hashCode	Hash Code	string	
fileDirection	File Direction	uint16	
fireAmpFileAction	FireAmp File Action	uint16	
parentFileName	Parent File Name	string	
parentFileHashCode	Parent File Hash Code	string	
infoURL	Informational URL	string	This field captures an URL if present in an event
threatScore	Threat Score	uint16	

Id	Display name	Type	Description
fireAmpDisposition	FireAmp Disposition	uint16	
fireAmpRetrospectiveDisposition	FireAmp Retrospective Disposition	uint16	
iocNum	IOC Number	uint32	
accessCtlPolicyId	Access Control Policy Id	uint32	
srcGeoCountryCode	Source Country Number	uint32	
destGeoCountryCode	Destination Country Number	uint32	
webAppId	Web App Id	uint32	
clientAppId	Client App Id	uint32	
applicationId	Application Id	uint32	
connEventTime	Connection Event Time	Date	
connCounter	Connection Counter	uint64	
cloudSecIntelId	Cloud Security Intel Id	uint32	
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FIREAMP_USER_LOGIN

Description: FireAMP user login event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
deviceTime	Device Time	Date	This is the timestamp as seen in the raw log. This is converted and stored as epoch milliseconds. Note that the deviceTime, or event occur time, is different than the event receive time by the SIEM.
user	User	string	
userId	User Id	string	
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
emailId	Email Id	string	
loginType	Login Type	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
extEventRecvProto	External Event Receive Protocol	string	

EventType: PH_DEV_MON_FORTIAP_INTF_UTIL

Description: FortiAP interface performance

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_FORTIAP_PERF

Description: FortiAP performance

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_FORTIAP_STAT

Description: FortiAP Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
sysUpTime	System Uptime	uint32	
wtpDaemonUpTime	WLAN AP Daemon Uptime	uint32	WLAN AP Daemon Uptime found in SNMP based WLAN monitoring
wtpSessionUpTime	WLAN AP Session Uptime	uint32	WLAN AP Session Uptime found in SNMP based WLAN monitoring
numWlanClient	WLAN Station Count	uint32	WLAN Station Count found in SNMP based WLAN monitoring
ftntWtpSessionStatus	WLAN AP Session Status	uint32	WLAN AP Session Status found in SNMP based WLAN monitoring
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_FORTIGATE_INTF_UTIL

Description: Fortigate interface performance

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_FORTIGATE_PERF

Description: Fortigate performance

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_FORTIMAIL_SESSION_COUNT**Description:** FortiMail session count**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_DEV_MON_FORTIMAIL_SYS_LOAD**Description:** FortiMail system load**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
numJob	Average System Job	uint32	

EventType: PH_DEV_MON_FORTINET_PROCESSOR_USAGE**Description:** FortiGate Firewall Processor Usage**Severity:** 1 (Low)**Event Category:** 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cpuName	CPU Name	string	
sysCpuUtil	System CPU Util	double	
userCpuUtil	User CPU Util	double	
cpuUtil	CPU Util	double	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
recvPktsPerSec	Received Packet Rate	double	Received Packet rate (packets/sec)
sentPktsPerSec	Sent Packet Rate	double	Sent Packet rate (packets/sec)
totPktDrop	Dropped Packets	uint64	Packets dropped
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_FORTINET_QOS**Description:** Fortinet QoS metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.
qosClassId	QoS Class Id	uint32	
direction	Direction	string	
guaranteedBandwidth	Guaranteed Bandwidth	double	

Id	Display name	Type	Description
allocatedBandwidth	Allocated Bandwidth	double	
peakBandwidth	Peak Bandwidth	double	
currentBandwidth	Current Bandwidth	double	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.
totPktDrop	Dropped Packets	uint64	Packets dropped

EventType: PH_DEV_MON_FORTISWITCH_PERF

Description: FortiSwitch performance

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_FORTIWLC_QOS_STAT

Description: FortiWLC QoS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
qosSessionCount	QoS Session Count	uint32	
qosH323SessionCount	QoS H.323 Session Count	uint32	
qosSipSessionCount	QoS SIP Session Count	uint32	

Id	Display name	Type	Description
qosSccpSessionCount	QoS SCCP Session Count	uint32	
qosRejectedSessionCount	QoS Rejected Session Count	uint32	
qosRejectedH323SessionCount	QoS Rejected H.323 Session Count	uint32	
qosRejectedSipSessionCount	QoS Rejected SIP Session Count	uint32	
qosRejectedSccpSessionCount	QoS Rejected SCCP Session Count	uint32	
qosPendingSessionCount	QoS Pending Session Count	uint32	
qosH323PendingSessionCount	QoS H.323 Pending Session Count	uint32	
qoSsipPendingSessionCount	QoS SIP Pending Session Count	uint32	
qoSsccpPendingSessionCount	QoS SCCP Pending Session Count	uint32	
qosActiveFlowCount	QoS Active Flow Count	uint32	
qosPendingFlowCount	QoS Pending Flow Count	uint32	

EventType: PH_DEV_MON_FORTIWLC_STATIONS

Description: FortiWLC Station Count

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
station11a	802.11a Station Count	uint32	
station11b	802.11b Station Count	uint32	

Id	Display name	Type	Description
station11bg	802.11bg Station Count	uint32	
stationData	Data Station Copunt	uint32	
stationPhone	Phone Station Count	uint32	
stationWired	Wired Station Count	uint32	
stationUnknown	Unknown Station Count	uint32	

EventType: PH_DEV_MON_FORTIWLC_SYS_THRUPUT

Description: FortiWLC system throughput

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBitsPerSec	Received Bit Rate	double	
sentBitsPerSec	Sent Bit Rate	double	
wlanRecvBitsPerSec	WLAN Recv Rate bps	double	WLAN Recv Rate (in bits/sec)s found in SNMP based WLAN monitoring
wlanSentBitsPerSec	WLAN Sent Rate bps	double	WLAN Sent Rate (in bits/sec) found in SNMP based WLAN monitoring

EventType: PH_DEV_MON_FPC_LIEBERT_METRIC

Description: Liebert FPC metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
outputVoltageXNVolts	Output Voltage X-N	uint32	
outputVoltageYNVolts	Output Voltage Y-N	uint32	
outputVoltageZNVolts	Output Voltage Z-N	uint32	
outputCurrentXAmps	Output Current X Amps	uint32	
outputCurrentYAmps	Output Current Y Amps	uint32	
outputCurrentZAmps	Output Current Z Amps	uint32	
neutralCurrentAmps	Neutral Current Amps	uint32	
groundCurrentAmps	Ground Current Amps	double	
outputPowerWatts	Output Power Watts	uint32	
powerFactor	Power Factor	uint32	
outputFrequency	Output Frequency Hz	uint32	
outputVxTHD	Output Vx THD	double	
outputVyTHD	Output Vy THD	double	
outputVzTHD	Output Vz THD	double	
outputLxTHD	Output lx THD	double	
outputLyTHD	Output ly THD	double	
outputLzTHD	Output lz THD	double	
outputKWh	Output kWh	double	
outputLxCrestFactor	Output lx Crest Factor	double	
outputLyCrestFactor	Output ly Crest Factor	double	
outputLzCrestFactor	Output lz Crest Factor	double	
outputLxKFactor	Output lx K-Factor	double	
outputLyKFactor	Output ly K-Factor	double	
outputLzKFactor	Output lz K-Factor	double	
outputLxCapacity	Output lx Capacity	uint32	
outputLyCapacity	Output ly Capacity	uint32	

Id	Display name	Type	Description
outputLzCapacity	Output lz Capacity	uint32	

EventType: PH_DEV_MON_FW_CONN_UTIL

Description: Firewall connection count stats for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
fwConnCount	Firewall Session	uint32	Number of concurrent sessions, typically found in Stateful Firewall performance statistic log
fwConnPct	Firewall Session Utilization	double	Concurrent sessions utilization defined as the ratio of concurrent sessions and max allowed concurrent sessions, typically found in Stateful Firewall performance statistic log
pollIntv	Polling Interval	uint32	
fwConnMax	Max Firewall Conn	uint32	Maximum number of Firewall Connections reported by Firewalls.
tcpFwConnCount	TCP Connection	uint32	Total number of TCP Connections reported by Firewalls.
udpFwConnCount	UDP Connection	uint32	Total number of UDP Connections reported by Firewalls.
icmpFwConnCount	ICMP Connection	uint32	Total number of ICMP Connections reported by Firewalls.
fwConnRate	Firewall Session Rate	uint32	

EventType: PH_DEV_MON_GITHUB_BRANCH_EVENT

Description: GitHub Branch Create/Delete Event

Severity: 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
branchName	Branch Name	string	
actionName	Notification Action Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_COMMIT

Description: User committed code to a GitHub repository**Severity:** 1 (Low)**Event Category:** 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
comment	Comment	string	
srcFileName	Source File Name	string	
actionName	Notification Action Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_EVENT**Description:** GitHub event**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_FORK_REPOSITORY_EVENT

Description: GitHub Repository Fork Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
newRepoName	New Repository Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_ISSUE_EVENT

Description: GitHub Issue Action Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
title	Title	string	
issueBody	Issue Body	string	
status	Status	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_MEMBER_EVENT

Description: GitHub user membership and permission change event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
memberName	Member Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_ORG_EVENT

Description: GitHub Organization User Block/Unblock Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_PROJECT_EVENT

Description: GitHub Project Action Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
projectName	Project Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_PULL_REQUEST_EVENT

Description: GitHub Pull Request Action Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
title	Title	string	
requestBody	Request Body	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_PULL_REQUEST_REVIEW_EVENT

Description: GitHub Pull Request Review Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
title	Title	string	
requestBody	Request Body	string	
reviewBody	Review Body	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_REPOSITORY_EVENT

Description: GitHub Repository Create/Delete Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
actionName	Notification Action Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GITHUB_TAG_EVENT

Description: GitHub Tag Create/Delete Event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
uuid	UUID	string	
type	Type	string	
user	User	string	
repoName	Repository Name	string	
repoURL	Repository URL	string	
reptGeoOrg	Reporting Organization	string	The Organization to which the Reporting IP in event belongs. This information is collected by doing a IP GeoDB lookup for external IPs, and CMDB lookup for internal IPs. The latter requires users to add CMDB Device location information in FortiSIEM GUI.
actionTime	Notification Action Time	Date	
tagName	Tag Name	string	
actionName	Notification Action Name	string	
extEventRecvProto	External Event Receive Protocol	string	
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_DEV_MON_GLASSFISH_APP

Description: Glassfish application server settings and metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_CONN_STAT

Description: Glassfish http connection statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_CPU

Description: Glassfish CPU usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_DB_POOL

Description: Glassfish database pool metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_EJB

Description: Glassfish EJB metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_JMS

Description: Glassfish JMS usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_MEMORY

Description: Glassfish memory usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_REQUEST_PROCESSOR

Description: Glassfish request processor metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_SERVLET

Description: Glassfish servlet metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_SESSION

Description: Glassfish session metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_GLASSFISH_THREAD_POOL

Description: Glassfish thread pool usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HARDWARE_STATUS

Description: Overall hardware Health status for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HOST_PERF_STATE

Description: Host performance monitoring state

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
durationHostNormal	Duration Normal	uint32	
durationHostWarn	Duration Warning	uint32	
durationHostCrit	Duration Critical	uint32	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.

EventType: PH_DEV_MON_HVAC_LIEBERT_METRIC

Description: Liebert HVAC metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envTempDegC	Temperature Celsius	uint32	

Id	Display name	Type	Description
envTempHighThreshDegC	High Temperature Threshold Celsius	uint32	
envTempLowThreshDegC	Low Temperature Threshold Celsius	uint32	
envTempOffHighDegC	Temp Offset High Celsius	uint32	
envTempOffLowDegC	Temp Offset Low Celsius	uint32	
envTempDegF	Temperature Fahrenheit	uint32	
envTempHighThreshDegF	High Temperature Threshold Fahrenheit	uint32	
envTempLowThreshDegF	Low Temperature Threshold Fahrenheit	uint32	
envTempOffHighDegF	Temp Offset High Fahrenheit	uint32	
envTempOffLowDegF	Temp Offset Low Fahrenheit	uint32	
envHumidityRel	Relative Humidity	uint32	
envHumidityRelHighThresh	High Relative Humidity Threshold	uint32	
envHumidityRelLowThresh	Low Relative Humidity Threshold	uint32	
envHumidityOffHigh	Humidity Offset High	uint32	
envHumidityOffLow	Humidity Offset Low	uint32	
lgpSystemState	Liebert HVAC System State	uint16	
lgpDehumidState	Liebert HVAC Dehumidifying State	uint16	

EventType: PH_DEV_MON_HW_AIRFLOW

Description: Airflow measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
envAirFlow	Air Flow 0.1meter/min	uint32	

EventType: PH_DEV_MON_HW_AMP

Description: Current measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
envCurrentAmp	Current Amp	double	

EventType: PH_DEV_MON_HW_AUDIO

Description: Audio sensor measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
envAudioLevel	Audio sensor level	uint32	

EventType: PH_DEV_MON_HW_CAMERA_MOTION

Description: Camera motion sensor measurement**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
cameraMotionSensorVal	Camera Motion Sensor Value	string	

EventType: PH_DEV_MON_HW_CHASSIS_COMP_STAT

Description: Chassis component environmental measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwCompAdminStateStr	Chassis Com Admin State	string	
hwCompOperStateStr	Chassis Comp Operational State	string	
hwCompSwStateStr	Chassis Comp Software State	string	
envTempDegF	Temperature Fahrenheit	uint32	
envTempHighThreshDegF	High Temperature Threshold Fahrenheit	uint32	

EventType: PH_DEV_MON_HW_CURRENT

Description: Current measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HW_DEWPPT**Description:** Dew point measurement**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
envTempDegC	Temperature Celsius	uint32	
envTempDegF	Temperature Fahrenheit	uint32	

EventType: PH_DEV_MON_HW_DOOR_SWITCH**Description:** Door switch sensor measurement**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device

Id	Display name	Type	Description
doorSwitchSensorVal	Door Switch Sensor Value	string	

EventType: PH_DEV_MON_HW_DRY_CONTACT

Description: Dry contact sensor measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
dryContactSensorVal	Dry Contact Sensor Value	string	

EventType: PH_DEV_MON_HW_FAN_SPEED

Description: Fan Speed measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
fanSpeed	Fan Speed	double	

EventType: PH_DEV_MON_HW_HUMIDITY

Description: Relative humidity measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
envHumidityRel	Relative Humidity	uint32	
envSensorLoc	Sensor Location	string	
envHumidityRelHighThresh	High Relative Humidity Threshold	uint32	
envHumidityRelLowThresh	Low Relative Humidity Threshold	uint32	

EventType: PH_DEV_MON_HW_POWER

Description: Power measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HW_PS_STAT

Description: Power supply environmental measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envPSTrayId	Power Supply Tray Id	string	
hwPowerSupply1StatusStr	Power Supply 1 State	string	
hwPowerSupply2StatusStr	Power Supply 2 State	string	
hwTempSensorStatusStr	Power Supply Temp Sensor State	string	
envTempHighThreshDegF	High Temperature Threshold Fahrenheit	uint32	
envPSInputStateStr	Power Supply Input State	string	
envPSOutputStateStr	Power Supply Output State	string	
envPSACStateStr	Power Supply AC State	string	
envPSDCStateStr	Power Supply DC State	string	

EventType: PH_DEV_MON_HW_STACK_UNIT

Description: Stack unit status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
envTempDegF	Temperature Fahrenheit	uint32	
cpuUtil	CPU Util	double	
memUtil	Memory Util	double	

EventType: PH_DEV_MON_HW_STATUS

Description: Hardware health status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwBatteryStatus	Hardware Battery Status	uint16	Hardware Battery Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwDiskStatus	Hardware Disk Status	uint16	Hardware Disk Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwMemoryStatus	Hardware Memory Status	uint16	Hardware Memory Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)

Id	Display name	Type	Description
hwPowerSupplyStatus	Hardware Power Supply Status	uint16	Hardware Power Supply Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwTempSensorStatus	Hardware Temperature Sensor Status	uint16	Hardware Temperature Sensor Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwFanStatus	Hardware Fan Status	uint16	Hardware Fan Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwAmpStatus	Hardware Amp Status	uint16	Hardware Amp Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwVoltageStatus	Hardware Voltage Status	uint16	Hardware Voltage Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwFailedPowerSupplyCount	Failed Power Supply Count	uint16	Failed Power Supply Count from SNMP based hardware monitoring
hwFailedFanCount	Failed Fan Count	uint16	Failed Fan Count from SNMP based hardware monitoring
hwLCCStatus	Storage LCC Status	uint16	
hwLinkStatus	Storage Link Status	uint16	
hwPortStatus	Storage Port Status	uint16	
hwHotSpareDiskCount	Hot Spare Disk Count	uint32	
hwMiscCompStatus	Misc Component Status	uint16	
hwRaidStatus	Hardware Raid Status	uint16	Hardware Raid Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwRelHumidStatus	Relative Humidity Status	uint16	
hwDewPtStatus	Dew Point Status	uint16	

Id	Display name	Type	Description
hwAudioStatus	Audio Sensor Status	uint16	
hwAirFlowStatus	Air Flow Status	uint16	
hwGenNumericSensorStatus	Generic Numeric Sensor Status	uint16	
hwDryContactStatus	Dry Contact Status	uint16	
hwDoorSwitchStatus	Door Switch Status	uint16	
hwCameraMotionStatus	Camera Motion Status	uint16	
hwGenStateSensorStatus	Generic State Sensor Status	uint16	
hwPowerEnclosureStatus	Hardware Power Enclosure Status	uint16	Hardware Power Enclosure Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwChassisStatus	Hardware Chassis Status	uint16	Hardware Chassis Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwIOMStatus	Hardware IO Module Status	uint16	Hardware IO Module Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwKVMStatus	Hardware KVM Status	uint16	Hardware KVM Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwRedundantStatus	Hardware Redundancy Status	uint16	Hardware Redundancy Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwBladeStatus	Hardware Blade Status	uint16	Hardware Blade Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwDellCMCStatus	Hardware Dell CMC Status	uint16	Hardware Dell CMC Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwFileSystemStatus	File System Status	uint16	

Id	Display name	Type	Description
hwStackUnitStatus	Hardware Stack Unit Status	uint16	Hardware Stack Unit Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwProbeStatus	Hardware Probe Status	uint16	Hardware Probe Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwInputContactStatus	Hardware Input Contact Status	uint16	Hardware Input Contact Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwOutputRelayStatus	Hardware Output Relay Status	uint16	Hardware Output Relay Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwOutletStatus	Hardware Outlet Status	uint16	Hardware Outlet Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwAlarmDeviceStatus	Hardware Alarm Device Status	uint16	Hardware Alarm Device Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwMemSensorStatus	Hardware Mem Sensor Status	uint16	Hardware Mem Sensor Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwMemOutputStatus	Hardware Mem Output Status	uint16	Hardware Mem Output Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwMemOutletStatus	Hardware Outlet Status	uint16	Hardware Outlet Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwMemBeaconStatus	Hardware Mem Beacon Status	uint16	Hardware Mem Beacon Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
hwSlotStatus	Hardware Slot Status	uint16	Hardware Slot Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)

EventType: PH_DEV_MON_HW_STATUS_AIRFLOW_CRIT

Description: Airflow critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_AIRFLOW_WARN**Description:** Airflow warning**Severity:** 5 (Medium)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_ALARMDEVICE_CRIT

Description: Alarm Device hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_ALARMDEVICE_WARN

Description: Alarm Device hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_AMP_CRIT

Description: Amp hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_AMP_WARN

Description: Amp hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_AUDIO_CRIT

Description: Audio sensor critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_AUDIO_WARN

Description: Audio sensor warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_BATTERY_CRIT

Description: Battery hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_BATTERY_WARN

Description: Battery hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_CAMERA_MOTION_CRIT

Description: Camera motion critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_CAMERA_MOTION_WARN

Description: Camera motion warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DEWPT_CRIT

Description: Dew Point temperature critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DEWPT_WARN

Description: Dew Point temperature warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DISK_CRIT

Description: Disk hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DISK_WARN

Description: Disk hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DOOR_SWITCH_CRIT

Description: Door switch critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DOOR_SWITCH_WARN

Description: Door switch warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DRY_CONTACT_CRIT

Description: Dry Contact sensor critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_DRY_CONTACT_WARN

Description: Dry Contact Sensor warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_FAN_CRIT

Description: Fan hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_FAN_WARN

Description: Fan hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_FILESYSTEM_CRIT

Description: File system hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_FILESYSTEM_WARN

Description: File system hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_GEN_NUMERIC_SENSOR_CRIT

Description: Generic Numeric Sensor critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_GEN_NUMERIC_SENSOR_WARN

Description: Generic Numeric Sensor warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_GEN_STATE_SENSOR_CRIT

Description: Generic state sensor critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_GEN_STATE_SENSOR_WARN

Description: Generic state sensor warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_HUMIDITY_CRIT

Description: Relative humidity critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_HUMIDITY_WARN

Description: Relative humidity warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_INPUTCONTACT_CRIT

Description: Input Contact hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_INPUTCONTACT_WARN

Description: Input Contact hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_LCC_CRIT

Description: SAN Link Control Card hardware critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_LCC_WARN

Description: SAN Link Control Card hardware warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_LINK_CRIT

Description: SAN host link critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_LINK_WARN

Description: SAN host link warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMBEACON_CRIT

Description: Memory Beacon hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMBEACON_WARN

Description: Memory Beacon hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMORY_CRIT

Description: Memory hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMORY_WARN

Description: Memory hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMOUTLET_CRIT

Description: Memory Outlet hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMOUTLET_WARN

Description: Memory Outlet hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMOUTPUT_CRIT

Description: Memory Output hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMOUTPUT_WARN

Description: Memory Output hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMSENSOR_CRIT

Description: Memory Sensor hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MEMSENSOR_WARN

Description: Memory Sensor hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MISC_CRIT

Description: Miscellaneous hardware critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_MISC_WARN

Description: Miscellaneous hardware warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_OUTLET_CRIT

Description: Outlet hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_OUTLET_WARN

Description: Outlet hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_OUTPUTRELAY_CRIT

Description: Output relay hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_OUTPUTRELAY_WARN

Description: Output relay hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_PORT_CRIT

Description: SAN storage port hardware critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_PORT_WARN

Description: SAN storage port hardware warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_POWERSUPPLY_CRIT

Description: Power supply hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_POWERSUPPLY_WARN

Description: Power supply hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_POWER_ENCLOSURE_CRIT

Description: Power enclosure health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_POWER_ENCLOSURE_WARN

Description: Power enclosure health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_PROBE_CRIT

Description: Probe hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_PROBE_WARN

Description: Probe hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_SLOT_CRIT

Description: Hardware Status Critical

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_SLOT_WARN

Description: Hardware Status Warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_STACKUNIT_CRIT

Description: Stackunit critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_STACKUNIT_WARN

Description: Stackunit warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_TEMP_CRIT

Description: Temperature sensor hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_TEMP_WARN

Description: Temperature sensor hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_VOLTAGE_CRIT

Description: Voltage hardware health: Critical

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_STATUS_VOLTAGE_WARN

Description: Voltage hardware health: Warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwStatusCode	Hardware Status	uint16	This attribute represents hardware status of a device
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
hwComponentStatus	Hardware Component Status	string	This field represents the specific issue with the component in hwComponentName field, when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), hwComponentName specifies a specific disk, say disk1 and this field states the specific issue with disk1

EventType: PH_DEV_MON_HW_TEMP**Description:** Temperature measurement**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
envTempDegC	Temperature Celsius	uint32	
envTempDegF	Temperature Fahrenheit	uint32	
envTempHighThreshDegC	High Temperature Threshold Celsius	uint32	
envTempOffHighDegC	Temp Offset High Celsius	uint32	
envTempHighThreshDegF	High Temperature Threshold Fahrenheit	uint32	
envTempOffHighDegF	Temp Offset High Fahrenheit	uint32	
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorEnclosureId	Sensor Enclosure Id	string	
devPort	Device Port	string	Name of the physical network port a device
envSensorLoc	Sensor Location	string	

Id	Display name	Type	Description
envTempLowThreshDegF	Low Temperature Threshold Fahrenheit	uint32	
envTempLowThreshDegC	Low Temperature Threshold Celsius	uint32	

EventType: PH_DEV_MON_HW_VOLTAGE

Description: Voltage measurement

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
envVoltage	Voltage	double	

EventType: PH_DEV_MON_HYPERV_CPU_GUEST_VIRTUAL_PROC

Description: HyperV Guest Virtual Processor Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_CPU_LOGICAL_PROC

Description: HyperV Logical Processor Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_CPU_ROOT_VIRTUAL_PROC

Description: HyperV Root Virtual Processor Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_OVERALL

Description: HyperV Root Memory Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_PARTITION

Description: HyperV Memory Partition usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_PARTITION_PER_VM

Description: HyperV per-VM Memory Partition usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION

Description: HyperV Root Partition Total Memory Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION_ROOT

Description: HyperV Root Partition Root Memory Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_VID_PARTITION

Description: HyperV VID Partition Memory Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_MEM_VID_PARTITION_PER_VM

Description: HyperV per-VM VID Partition Memory Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_NET_LEGACY_ADAPTER

Description: HyperV Virtual Switch Per Adapter Network Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_NET_VIRTUAL_ADAPTER

Description: HyperV Virtual Switch Per Adapter Network Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_NET_VIRTUAL_SWITCH

Description: HyperV Virtual Switch Network Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_OVERALL_HEALTH

Description: HyperV Machine Health Summary

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_OVERALL_SYSINFO

Description: HyperV System Information

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_STORAGE_LOGICAL_DISK

Description: HyperV Logical Disk Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_IDE_CONTROLLER

Description: HyperV IDE Controller Storage Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_STORAGE

Description: HyperV Virtual Storage Usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_INCOMING_EXCEED_GUARANTEED

Description: Incoming eps exceeded Guaranteed eps at a collector

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
collectorId	Collector ID	uint32	This field captures the ID of a FortiSIEM Collector
phCollectorName	Collector Name	string	Name of the FortiSIEM Collector. The name is set in GUI.
incomingEventsPerSec	Incoming Event Rate	double	This is a FortiSIEM event ingestion rate calculated every 3 minutes, divided by 180 to generate a rolling EPS (Events Per Second) interval.
guaranteedEventsPerSec	Guaranteed EPS	uint64	

EventType: PH_DEV_MON_INTF_ADMIN_DOWN_TO_UP

Description: Network Interface administratively came back up

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
intfAlias	Host Interface Alias	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_INTF_ADMIN_UP_TO_DOWN

Description: Network Interface administratively went down

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
intfAlias	Host Interface Alias	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_INTF_OPER_DOWN_TO_UP

Description: Network Interface operationally came back up

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
intfAlias	Host Interface Alias	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_INTF_OPER_UP_TO_DOWN

Description: Network Interface operationally went down

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
intfAlias	Host Interface Alias	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DEV_MON_INTF_USAGE_TOTAL**Description:** Aggregate Interface Usage**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
recvBitsPerSec	Received Bit Rate	double	
sentBitsPerSec	Sent Bit Rate	double	
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.

EventType: PH_DEV_MON_IPSLA_HTTP_MET**Description:** IP SLA HTTP Performance metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipSLAProto	IP SLA Protocol	string	Name of the IP Service Level Agreement (SLA) protocol. This parameter is set during IPSLA monitoring
httpResponseTimeMs	HTTP Response Time ms	uint32	
dnsResponseTimeMs	DNS Response Time ms	uint32	
tcpConnectResponseTimeMs	TCP Connect Response Time ms	uint32	
httpTransactResponseTimeMs	HTTP Transaction Response Time ms	uint32	
ipslaHttpStatus	IPSLA HTTP Status	uint32	
ipslaHttpStatusDesc	IPSLA HTTP Status Description	string	
httpStatusCode	HTTP Status	string	

EventType: PH_DEV_MON_IPSLA_ICMP_MET

Description: ICMP performance metrics collected via IP SLA

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
ipslaTestName	IP SLA Test Name	string	
icmpResponseTimeMs	ICMP Response Time ms	uint32	

EventType: PH_DEV_MON_IPSLA_MET

Description: IP SLA performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

Id	Display name	Type	Description
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipSLAProto	IP SLA Protocol	string	Name of the IP Service Level Agreement (SLA) protocol. This parameter is set during IPSLA monitoring
tos	IP Type of Service	uchar	The type of service (ToS) field present in the IPv4 header. Typically present in Netflow.
dscp	DSCP	uchar	
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
avgJitterMs	Avg Jitter	uint32	Average Jitter (msec)
maxJitterMs	Max Jitter	uint32	Maximum Jitter (msec)
minJitterMs	Min Jitter	uint32	Minimum Jitter (msec)
avgJitterSDMs	Avg SD Jitter	uint32	Average Source to Destination Jitter (msec)
maxJitterSDMs	Max SD Jitter	uint32	Maximum Source to Destination Jitter (msec)
minJitterSDMs	Min SD Jitter	uint32	Minimum Source to Destination Jitter (msec)
avgJitterDSMs	Avg DS Jitter	uint32	Average Destination to Source Jitter (msec)
maxJitterDSMs	Max DS Jitter	uint32	Maximum Destination to Source Jitter (msec)
minJitterDSMs	Min DS Jitter	uint32	Minimum Destination to Source Jitter (msec)
pktLost	Packets Lost	uint32	Total Packets lost (includes Source to Destination and reverse)
pktLostSD	SD Packets Lost	uint32	Packets lost from Source to Destination
pktLostDS	DS Packets Lost	uint32	Packets lost from Destination to Source
pktMIA	Packets Missing	uint32	Packets missing
pktLate	Packets Late	uint32	Packets late

Id	Display name	Type	Description
pktOutSeq	Pkt Out-of-Seq	uint32	

EventType: PH_DEV_MON_IPSLA_UDP_MET

Description: IP SLA UDP Performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
udpResponseTimeMs	UDP Response Time ms	uint32	
ipslaUdpStatus	IPSLA UDP Status	uint32	
ipslaUdpStatusDesc	IPSLA UDP Status Description	string	

EventType: PH_DEV_MON_IPSLA_VOIP_MET

Description: VOIP performance metrics collected via IP SLA

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
ipSLAProto	IP SLA Protocol	string	Name of the IP Service Level Agreement (SLA) protocol. This parameter is set during IPSLA monitoring
codec	VoIP Codec	string	
tos	IP Type of Service	uchar	The type of service (ToS) field present in the IPv4 header. Typically present in Netflow.
dscp	DSCP	uchar	
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
avgJitterMs	Avg Jitter	uint32	Average Jitter (msec)

Id	Display name	Type	Description
maxJitterMs	Max Jitter	uint32	Maximum Jitter (msec)
minJitterMs	Min Jitter	uint32	Minimum Jitter (msec)
avgJitterSDMs	Avg SD Jitter	uint32	Average Source to Destination Jitter (msec)
maxJitterSDMs	Max SD Jitter	uint32	Maximum Source to Destination Jitter (msec)
minJitterSDMs	Min SD Jitter	uint32	Minimum Source to Destination Jitter (msec)
avgJitterDSMs	Avg DS Jitter	uint32	Average Destination to Source Jitter (msec)
maxJitterDSMs	Max DS Jitter	uint32	Maximum Destination to Source Jitter (msec)
minJitterDSMs	Min DS Jitter	uint32	Minimum Destination to Source Jitter (msec)
pktLost	Packets Lost	uint32	Total Packets lost (includes Source to Destination and reverse)
pktLostSD	SD Packets Lost	uint32	Packets lost from Source to Destination
pktLostDS	DS Packets Lost	uint32	Packets lost from Destination to Source
pktMIA	Packets Missing	uint32	Packets missing
pktLate	Packets Late	uint32	Packets late
pktOutSeq	Pkt Out-of-Seq	uint32	
mosScore	MOS Score	double	MOS (Mean Opinion Score) measures the perceived quality of VoIP audio on a scale from 1 to 5, with 5 being the best possible score. A high MOS rate indicates that the audio quality is good, while a low MOS rate indicates poor audio quality.
icpifScore	ICPIF Score	uint32	ICPIF (Impairment/Calculated Planning Impairment Factor) quantifies the key impairments to voice quality that are encountered in the network. ICPIF values are expressed in a typical range of 5 (very low impairment) to 55 (very high impairment).

EventType: PH_DEV_MON_IRONPORT_MAIL_USAGE

Description: Cisco Ironport Mail Usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
workQueueMsgCount	Mail Work Queue Count	uint32	
diskIOUtil	Disk IO Util	double	
mailQueueUtil	Mail Queue Util	double	
msgAge	Oldest Message Age sec	uint32	
outstandingDNS	Outstanding DNS Req	uint32	
pendingDNS	Pending DNS Req	uint32	
openFile	Open File Count	uint32	
mtaThreadCount	MTA Thread Count	uint32	
queueAvailStatus	Mail Queue Avail Status	string	

EventType: PH_DEV_MON_ISILON_CLUSTER_HEALTH

Description: Isilon Cluster health and performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
svcStatus	Service Health	string	
clusterOnlineMember	Cluster Online Members	string	
clusterOfflineMember	Cluster Offline Members	string	

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
cpuUtil	CPU Util	double	
userCpuUtil	User CPU Util	double	
kernCpuUtil	Kernel CPU Util	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
netSentKBytesPerSec	Net Sent Rate KBps	double	
netRecvdKBytesPerSec	Net Received Rate KBps	double	

EventType: PH_DEV_MON_ISILON_CLUSTER_MEMBERSHIP_CHANGE

Description: Isilon cluster membership change

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
addedItem	Added Item	string	
deletedItem	Deleted Item	string	

EventType: PH_DEV_MON_ISILON_CLUSTER_QUOTA

Description: Isilon quota utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
quotaName	Quota Name	string	
quotaType	Quota Type	string	
quotaSoftThresholdBytes	Quota Soft Threshold Bytes	uint64	
quotaHardThresholdBytes	Quota Hard Threshold Bytes	uint64	
quotaAdvThresholdBytes	Quota Advisory Threshold Bytes	uint64	
quotaUsageBytes	Quota Usage Bytes	uint64	
quotaUsageWithOverheadBytes	Quota Usage With Overhead Bytes	uint64	
quotaInodeUsage	Quota Inode Usage	uint64	
gracePeriod	Quota Grace Period	uint64	

EventType: PH_DEV_MON_ISILON_CLUSTER_SNAPSHOT**Description:** Isilon snapshot usage**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
snapshotName	Snapshot Name	string	

Id	Display name	Type	Description
snapshotDescription	Snapshot Description	string	
snapshotPath	Snapshot Path	string	
snapshotCreateTime	Snapshot Create Time	Date	
snapshotExpiryTime	Snapshot Expiry Time	Date	
fileSize64	File Size64 Bytes	uint64	

EventType: PH_DEV_MON_ISILON_NODE_DISK_PERF

Description: Isilon disk performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
opsPerSec	Operations/sec	uint32	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	

EventType: PH_DEV_MON_ISILON_NODE_HEALTH

Description: Isilon node health and performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
svcStatus	Service Health	string	
cluster	Cluster	string	
cpuUtil	CPU Util	double	
userCpuUtil	User CPU Util	double	
kernCpuUtil	Kernel CPU Util	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
netSentKBytesPerSec	Net Sent Rate KBps	double	
netRecvdKBytesPerSec	Net Received Rate KBps	double	

EventType: PH_DEV_MON_ISILON_NODE_PROTO_PERF

Description: Isilon protocol performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appName	Application Name	string	
opsPerSec	Operations/sec	uint32	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
minSentBytes	Min Sent Bytes	uint64	Minimum of Sent Bytes over the report window. Used in Profile Reports only.
maxSentBytes	Max Sent Bytes	uint64	Maximum of Sent Bytes over the report window. Used in Profile Reports only.

Id	Display name	Type	Description
avgSentBytes	Avg Sent Bytes	double	Average of Sent Bytes over the report window. Used in Profile Reports only.
sdevSentBytes	Std Dev Sent Bytes	double	Standard Deviation of Sent Bytes over the report window. Used in Profile Reports only.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
minRecvBytes	Min Received Bytes	uint64	Minimum of Received Bytes over the report window. Used in Profile Reports only.
maxRecvBytes	Max Received Bytes	uint64	Maximum of Received Bytes over the report window. Used in Profile Reports only.
avgRecvBytes	Avg Received Bytes	double	Average of Received Bytes over the report window. Used in Profile Reports only.
sdevRecvBytes	Std Dev Received Bytes	double	Standard Deviation of Received Bytes over the report window. Used in Profile Reports only.
latency	Latency	double	
minLatency	Min Latency	double	
maxLatency	Max Latency	double	
avgLatency	Avg Latency	double	
sdevLatency	Std Dev Latency	double	
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	

EventType: PH_DEV_MON_JBOSS_APP

Description: JBOSS application server settings and metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_CPU

Description: JBOSS CPU metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_DB_POOL

Description: JBOSS database pool metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_EJB

Description: JBOSS EJB metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_MEMORY

Description: JBOSS memory usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_REQUEST_PROCESSOR

Description: Weblogic request processor metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_SERVLET

Description: JBOSS servlet metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_SESSION

Description: JBOSS session metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_JBOSS_THREAD_POOL

Description: JBOSS thread pool usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_LOG_ALL_DEVICE_DELAY_HIGH

Description: Log receipt delay for all devices from a collection point crossed high water mark

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_LOG_ALL_DEVICE_DELAY_LOW

Description: Log receipt delay for all devices from a collection point fell below low water mark

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_LOG_DEVICE_DELAY_HIGH

Description: Log receipt delay for a single device crossed high water mark

Notes: This event is generated by FortiSIEM Supervisor node when no events are received from a single source IP (Reporting IP) within a (high threshold) time window. The time period can be set in two ways:

- Global Setting: Set the EventRecvTimeGapHigh attribute in Admin > Device Support > Custom Properties. By default it is set to 10 minutes
- Per device Setting: Set the "Event Receive Time Gap High Threshold minutes" attribute in CMDB > Choose a Device > Edit > Device Properties

An event is generated for each jobType, e.g. Syslog, Windows Agent Log Collection, Linux Agent Log Collection, Cloud Service Log Collection etc.

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_LOG_DEVICE_DELAY_LOW

Description: Log receipt delay for a single device fell below water mark

Notes: This event is generated by FortiSIEM Supervisor node when no events are received from a single source IP (Reporting IP) within a (low threshold) time window. The time period can be set in two ways:

- Global Setting: Set the EventRecvTimeGapLow attribute in Admin > Device Support > Custom Properties. By default it is set to 5 minutes
- Per device Setting: Set the "Event Receive Time Gap Low Threshold minutes" attribute in CMDB > Choose a Device > Edit > Device Properties

An event is generated for each jobType, e.g. Syslog, Windows Agent Log Collection, Linux Agent Log Collection, Cloud Service Log Collection etc.

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_MANUAL_SVC_START_TO_STOP

Description: Running Windows Manual service stopped

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
servicePath	Service Path	string	
serviceDesc	Service Description	string	

EventType: PH_DEV_MON_MANUAL_SVC_STOP

Description: Windows Manual Windows Service stopped

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
servicePath	Service Path	string	
serviceDesc	Service Description	string	

EventType: PH_DEV_MON_MANUAL_SVC_STOP_TO_START

Description: Stopped Windows Manual Service started

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
servicePath	Service Path	string	
serviceDesc	Service Description	string	

EventType: PH_DEV_MON_NETAPP_AGGR_MET

Description: NETAPP aggregate performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
aggrName	NetApp Aggregate Name	string	
aggrReadOpsPerSec	Aggregate Read Request /sec	double	
aggrWriteOpsPerSec	Aggregate Write Request /sec	double	
aggrTxfrPerSec	Aggregate Transfer /sec	double	
aggrCpReadPerSec	Aggregate CP Read /sec	double	

EventType: PH_DEV_MON_NETAPP_CIFS_MET

Description: NETAPP CIFS performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cifsOpsPerSec	CIFS Request Rate	double	
cifsLatency	CIFS Latency ms	double	Overall Latency (ms) using CIFS storage protocol.

EventType: PH_DEV_MON_NETAPP_CP_MET

Description: NetApp consistency point metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cpFromTimer	Timer Consistency Point	uint32	
cpFromSnapshot	Snapshot Consistency Point	uint32	
cpFromLowWater	Low Water Consistency Point	uint32	
cpFromHiWater	High Water Consistency Point	uint32	
cpFromLogFull	Log Full Consistency Point	uint32	
backtobackCp	Back-to-back Consistency Point	uint32	
totalCp	Total Consistency Point	uint32	
deferredBacktobackCp	Deferred Back-to-back Consistency Point	uint32	

EventType: PH_DEV_MON_NETAPP_DISK_HEALTH

Description: NetApp disk status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
totDisk	Total Disk Count	uint32	Total number of Disks
activeDisk	Active Disk Count	uint32	Total number of Active Disks
failedDisk	Failed Disk Count	uint32	Total number of Failed Disks
spareDisk	Spare Disk Count	uint32	Total number of Spare Disks
reconstDisk	Reconstructing Disk Count	uint32	Total number of Reconstructing Disks
scrubbDisk	Scrubbing Disk Count	uint32	
addSpareDisk	Add Spare Disk Count	uint32	

EventType: PH_DEV_MON_NETAPP_DISK_MET

Description: NETAPP disk level performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
diskUtil	Disk Capacity Util	double	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
devDiskRdLatency	Disk Read Latency ms	double	
devDiskWrLatency	Disk Write Latency ms	double	
diskTfrOpsPerSec	Disk Transfer Ops/s	double	

EventType: PH_DEV_MON_NETAPP_FCP_MET

Description: NETAPP FCP performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
fcReadOpsPerSec	FCP Read Request /sec	double	Read Request Rate (operations/sec) using FCP storage protocol.
fcWriteOpsPerSec	FCP Write Request /sec	double	Write Request Rate (operations/sec) using FCP storage protocol.

Id	Display name	Type	Description
fcReadLatency	FCP Read Latency ms	double	Read Latency (ms) using FCP storage protocol.
fcWriteLatency	FCP Write Latency ms	double	Write Latency (ms) using FCP storage protocol.
fcReadKBytesPerSec	FCP Read Volume KBps	double	Read throughput (KBytes/sec) using FCP storage protocol.
fcWriteKBytesPerSec	FCP Write Volume KBps	double	Write throughput (KBytes/sec) using FCP storage protocol.

EventType: PH_DEV_MON_NETAPP_ISCSI_MET

Description: NETAPP ISCSI performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
iscsiReadOpsPerSec	ISCSI Read Request Rate	double	Read Request Rate (operations/sec) using ISCSI storage protocol.
iscsiWriteOpsPerSec	ISCSI Write Request Rate	double	Write Request Rate (operations/sec) using ISCSI storage protocol.
iscsiReadLatency	ISCSI Read Latency ms	double	Read Latency (ms) using ISCSI storage protocol.
iscsiWriteLatency	ISCSI Write Latency ms	double	Write Latency (ms) using ISCSI storage protocol.
iscsiReadKBytesPerSec	ISCSI Read Volume KBps	double	Read throughput (KBytes/sec) using ISCSI storage protocol.
iscsiWriteKBytesPerSec	ISCSI Write Volume KBps	double	Write throughput (KBytes/sec) using ISCSI storage protocol.

EventType: PH_DEV_MON_NETAPP_LUN_MET**Description:** NETAPP lun level performance metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
lunName	LUN Name	string	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
devDiskRWLatency	Disk Read/Write Latency	double	
diskQueueFull	Disk Queue Full /sec	double	

EventType: PH_DEV_MON_NETAPP_NFS3_MET**Description:** NETAPP detailed NFS V3 performance metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
nfsReadOpsPerSec	NFS Read Request Rate	double	Read Request Rate (operations/sec) using NFS storage protocol.

Id	Display name	Type	Description
nfsWriteOpsPerSec	NFS Write Request Rate	double	Write Request Rate (operations/sec) using NFS storage protocol.
nfsOpsPerSec	NFS Request Rate	double	
nfsReadLatency	NFS Read Latency	double	Read Latency (ms) using NFS storage protocol.
nfsWriteLatency	NFS Write Latency	double	Write Latency (ms) using NFS storage protocol.
nfsReadKBytesPerSec	NFS Read Volume KBps	double	Read throughput (KBytes/sec) using NFS storage protocol.
nfsWriteKBytesPerSec	NFS Write Volume KBps	double	Write throughput (KBytes/sec) using NFS storage protocol.

EventType: PH_DEV_MON_NETAPP_NFS4_MET

Description: NETAPP detailed NFS V4 performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
nfsReadOpsPerSec	NFS Read Request Rate	double	Read Request Rate (operations/sec) using NFS storage protocol.
nfsWriteOpsPerSec	NFS Write Request Rate	double	Write Request Rate (operations/sec) using NFS storage protocol.
nfsOpsPerSec	NFS Request Rate	double	
nfsReadLatency	NFS Read Latency	double	Read Latency (ms) using NFS storage protocol.
nfsWriteLatency	NFS Write Latency	double	Write Latency (ms) using NFS storage protocol.
nfsReadKBytesPerSec	NFS Read Volume KBps	double	Read throughput (KBytes/sec) using NFS storage protocol.
nfsWriteKBytesPerSec	NFS Write Volume KBps	double	Write throughput (KBytes/sec) using NFS storage protocol.

EventType: PH_DEV_MON_NETAPP_NFS_MET**Description:** NETAPP NFS performance metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cacheAgeMin	Cache Age Min	uint64	
cifsOpsPerSec	CIFS Request Rate	double	
nfsOpsPerSec	NFS Request Rate	double	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
netSentKBytesPerSec	Net Sent Rate KBps	double	
netRecvdKBytesPerSec	Net Received Rate KBps	double	
rpcBadCallsDelta	RPC Bad Calls	uint64	
nfsBadCallsDelta	NFS Bad Calls	uint64	
cifsBadCallsDelta	CIFS Bad Calls	uint64	

EventType: PH_DEV_MON_NETAPP_VOL_MET**Description:** NETAPP volume performance metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
volName	NetApp Volume Name	string	
diskReadReqPerSec	Disk Read Rate req/sec	double	
diskWriteReqPerSec	Disk Write Rate req/sec	double	
nfsWriteOpsPerSec	NFS Write Request Rate	double	Write Request Rate (operations/sec) using NFS storage protocol.
nfsReadLatency	NFS Read Latency	double	Read Latency (ms) using NFS storage protocol.
nfsWriteLatency	NFS Write Latency	double	Write Latency (ms) using NFS storage protocol.
cifsReadOpsPerSec	CIFS Read Request /sec	double	Read Request Rate (operations/sec) using CIFS storage protocol.
cifsWriteOpsPerSec	CIFS Write Request /sec	double	Write Request Rate (operations/sec) using CIFS storage protocol.
cifsReadLatency	CIFS Read Latency ms	double	Read Latency (ms) using CIFS storage protocol.
cifsWriteLatency	CIFS Write Latency ms	double	Write Latency (ms) using CIFS storage protocol.
sanReadOpsPerSec	SAN Read Request /sec	double	
sanWriteOpsPerSec	SAN Write Request /sec	double	
sanReadLatency	SAN Read Latency ms	double	
sanWriteLatency	SAN Write Latency ms	double	

EventType: PH_DEV_MON_NETBOTZ_HW_EMS_STATUS

Description: NetBotz EMS Hardware Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
emsHwStatus	EMS Hardware Status	uint16	EMS Hardware Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
phyMachConnectionStateCode	Physical Machine Connection State	uint16	
hwLogStatus	Hardware Log Status	uint16	Hardware Log Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)

EventType: PH_DEV_MON_NETBOTZ_HW_MODULE_SENSOR

Description: NetBotz Module Sensor Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
moduleNumber	Module Number	uint32	
envSensorId	Env Sensor Id	string	
envSensorLabel	Sensor Label	string	
envSensorLoc	Sensor Location	string	
envTempDegC	Temperature Celsius	uint32	

Id	Display name	Type	Description
envHumidityRel	Relative Humidity	uint32	
phyMachConnectionStateCode	Physical Machine Connection State	uint16	
hwAlarmDeviceStatus	Hardware Alarm Device Status	uint16	Hardware Alarm Device Status determined from SNMP based hardware monitoring (0: Normal, 1: Warning, 2: Critical)
envTempDegF	Temperature Fahrenheit	uint32	

EventType: PH_DEV_MON_NETBOTZ_HW_PROBE

Description: NetBotz Probe Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
envSensorLabel	Sensor Label	string	
envTempDegC	Temperature Celsius	uint32	
envTempHighThreshDegC	High Temperature Threshold Celsius	uint32	
envHumidityRel	Relative Humidity	uint32	
envHumidityRelHighThresh	High Relative Humidity Threshold	uint32	
envHumidityRelLowThresh	Low Relative Humidity Threshold	uint32	
serialNumber	Serial Number	string	

Id	Display name	Type	Description
phyMachConnectionStateCode	Physical Machine Connection State	uint16	
envTempDegF	Temperature Fahrenheit	uint32	
envTempHighThreshDegF	High Temperature Threshold Fahrenheit	uint32	

EventType: PH_DEV_MON_NETSCALER_APP_FW

Description: NetScaler Application Firewall metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
totalRequests	Total Requests	uint64	
totalResponses	Total Responses	uint64	
totalAborts	Total Aborts	uint64	
totalRedirects	Total Redirects	uint64	
startURLViol	Start URL Violations	uint32	
denyURLViol	Deny URL Violations	uint32	
bufOverflowViol	Buffer Overflow Violations	uint32	
cookieViol	Cookie Violations	uint32	
xssViol	XSS Violations	uint32	
sqlViol	SQL Violations	uint32	
fieldFormatViol	Field Format Violations	uint32	
fieldConsistViol	Field Consistency Violations	uint32	
creditCardViol	Credit Card Violations	uint32	

Id	Display name	Type	Description
safeObjViol	Safe Object Violations	uint32	
totViol	Total Violations	uint32	

EventType: PH_DEV_MON_NETSCALER_SERVICE

Description: NetScaler Service metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
serviceName	Service Name	string	
serverIpAddr	Server IP	IP	
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
appTransportProto	Application Protocol	string	
svcStatus	Service Health	string	
averageTransactionTime	Average Transaction Time ms	uint32	
createdConn	Created Connections	uint64	
activeConns	Active Connection	uint64	
surgeQueue	Surge Queue	uint32	
totalRequests	Total Requests	uint64	
totalResponses	Total Responses	uint64	
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.

Id	Display name	Type	Description
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.

EventType: PH_DEV_MON_NETSCALER_VIRT_SERVER

Description: NetScaler Virtual Server metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
serverName	Server Name	string	
serverIpAddr	Server IP	IP	
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
appTransportProto	Application Protocol	string	
svcStatus	Service Health	string	
clientConns	Client Connections	uint64	
serverConns	Server Connections	uint64	
surgeQueue	Surge Queue	uint32	
totalRequests	Total Requests	uint64	
totalResponses	Total Responses	uint64	
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.

Id	Display name	Type	Description
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
totHits	Total Hits	uint64	
serviceUp	Services Up	uint32	
serviceDown	Services Down	uint32	
serviceUnknown	Services Unknown	uint32	
serviceOOS	Services OutOfService	uint32	
serviceTransitOOS	Services Transit OutOfService	uint32	

EventType: PH_DEV_MON_NET_INTF_UTIL

Description: Network Interface utilization stats for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
intfName	Host Interface Name	string	Name of a network interface in a host.
intfAlias	Host Interface Alias	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pollIntv	Polling Interval	uint32	
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
recvBitsPerSec	Received Bit Rate	double	
inIntfUtil	Recv Interface Util	double	Ratio of Received Bits per second (derived from recvBytes) to the received network interface speed

Id	Display name	Type	Description
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
sentBitsPerSec	Sent Bit Rate	double	
outIntfUtil	Sent Interface Util	double	Ratio of Sent Bits per second (derived from sentBytes) to the sent network interface speed
recvPkts64	Received Packets64	uint64	Number of packets received by a host. This is 64bit version.
sentPkts64	Sent Packets64	uint64	Number of packets sent by a host. This is 64bit version.
inIntfPktErr	Recv Packet Errors	uint32	Number of received packets that had errors. The networking stack discards these packets.
inIntfPktErrPct	Recv Packet Error Pct	double	Ratio of inIntfPktErr and the total number of received packets in an onterval
outIntfPktErr	Sent Packet Errors	uint32	Number of sent packets that had errors. he networking stack discards these packets.
outIntfPktErrPct	Sent Packet Error Pct	double	Ratio of outIntfPktErr and the total number of received packets in an onterval
outQLen64	Interface Sent Queue Length64	uint64	
intfInSpeed64	Recv Interface Speed bps	uint64	Received bits/sec through an interface
intfOutSpeed64	Sent Interface Speed bps	uint64	Sent bits/sec through an interface
intfAdminStatus	Interface Admin Status	string	
intfOperStatus	Interface Operational Status	string	
daysSinceLastUse	Days Since Last Use	uint32	
totIntfPktErr	Total Packet Errors	uint32	
totBitsPerSec	Total Bit Rate	double	Total (Sent plus Received) bits/sec through an interface
linkDuplexStatus	Link Duplex Status	string	
alignError	Frame Align Error	uint32	
fcsError	Frame FCS Error	uint32	
defTransmit	Frame Deferred Transmission	uint32	

Id	Display name	Type	Description
multiCollision	Frame Multi Collision	uint32	
lateCollision	Frame Late Collision	uint32	
excessCollisionAbort	Frame Excess Collision Abort	uint32	
macTxmitError	Frame MAC Transmit Error	uint32	
carrierSenseError	Frame Carrier Sense Error	uint32	
framesTooLong	Frame Too Long	uint32	
symbolError	Frame Symbol Error	uint32	
intMacRecvError	Frame Internal MAC Receive Error	uint32	
vdom	Virtual Domain	string	
latency	Latency	double	
jitterMs	Jitter	uint32	
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.
availSentBitsPerSec	Available Sent Rate	double	
availRecvBitsPerSec	Available Received Rate	double	
realtimeLinkCost	Real-time Link Cost	uint32	
transactionalLinkCost	Transactional Link Cost	uint32	
backgroundLinkCost	Background Link Cost	uint32	
relayDevIpAddr	Relaying IP	IP	Relaying IP is most commonly used to specify the log relay appliance, usually a collector.
relayDevName	Relaying Device	string	This is the hostname of the relaying device, a log relay, which is most typically a FortiSIEM collector.

EventType: PH_DEV_MON_NIMBLE_GLOBAL_STAT**Description:** Nimble Storage global stats**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
ioReadsPerSec	Total Read I/Os Rate	double	
ioSeqReadsPerSec	Total Sequential Read I/Os Rate	double	
ioWritesPerSec	Total Write I/Os Rate	double	
ioSeqWritesPerSec	Total Sequential Write I/Os Rate	double	
ioReadLatency	IO Read Latency	uint64	
ioWriteLatency	IO Write Latency	uint64	
ioReadKBytesPerSec	Total Read I/O Rate KBps	double	
ioSeqReadKBytesPerSec	Total Sequential Read I/O Rate KBps	double	
ioWriteKBytesPerSec	Total Write I/O Rate KBps	double	
ioSeqWriteKBytesPerSec	Total Sequential Write I/O Rate KBps	double	
usedVolMB	Used Volumes MB	uint64	
usedSnapMB	Used Snapshots MB	uint64	
ioNonSeqCacheHitRatio	Non-Sequential Read I/Os Hit Ratio	double	

EventType: PH_DEV_MON_NUTANIX_CLUSTER_STATUS**Description:** Nutanix Cluster Status**Severity:** 1 (Low)**Event Category:** 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
clusterVersion	Cluster Version	string	
clusterStatus	Cluster Status	string	
diskUtil	Disk Capacity Util	double	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
diskRWReqPerSec	Disk RW Rate req/sec	double	
devDiskRWLatency	Disk Read/Write Latency	double	

EventType: PH_DEV_MON_NUTANIX_CONTAINER_INFO**Description:** Nutanix Storage Container Info**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
ntxContainerId	Nutanix Container Id	uint64	
ntxContainerName	Nutanix Container Name	string	
diskUtil	Disk Capacity Util	double	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	

Id	Display name	Type	Description
diskRWReqPerSec	Disk RW Rate req/sec	double	
devDiskRWLatency	Disk Read/Write Latency	double	

EventType: PH_DEV_MON_NUTANIX_CTRLR_VM_RESOURCE

Description: Nutanix Controller VM Resource Info

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
ntxControllerVMId	Nutanix Controller VM Id	uint64	
memTotalIMB	Total Memory MB	uint32	
procCount	System Process Count	uint32	

EventType: PH_DEV_MON_NUTANIX_DISK_STATUS

Description: Nutanix Disk Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	

Id	Display name	Type	Description
diskId	Disk Id	uint64	
ntxControllerVMId	Nutanix Controller VM Id	uint64	
hwDiskSerial	Disk Serial	string	
diskUtil	Disk Capacity Util	double	
totalDiskMB	Total Disk MB	uint32	
freeDiskMBNonRoot	Free Disk MB NonRoot	uint32	
inodeUsedPct	Inode Util	double	
inodeMax	Max Inodes	uint32	
inodeFreeNonRoot	Free Inodes NonRoot	uint32	

EventType: PH_DEV_MON_NUTANIX_DISK_TEMP

Description: Nutanix Disk temperature event

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskId	Disk Id	uint64	
ntxControllerVMId	Nutanix Controller VM Id	uint64	
hwDiskSerial	Disk Serial	string	
envTempdDegC	Temperature Celsius Detailed	double	

EventType: PH_DEV_MON_NUTANIX_SERVICE_STATUS

Description: Nutanix Service Status

Severity: 1 (Low)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
ntxControllerVMId	Nutanix Controller VM Id	uint64	
ntxClusterVMStatus	Cluster VM Status	string	
ntxZeusStatus	Nutanix Zeus Status	string	
ntxStargateStatus	Nutanix Stargate Status	string	

EventType: PH_DEV_MON_NUTANIX_STORAGE_POOL_INFO**Description:** Nutanix Storage Pool Info**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cluster	Cluster	string	
spoolId	Storage Pool Id	uint64	
spoolName	Storage Pool Name	string	
diskUtil	Disk Capacity Util	double	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
diskRWReqPerSec	Disk RW Rate req/sec	double	
devDiskRWLatency	Disk Read/Write Latency	double	

EventType: PH_DEV_MON_OMI_PING_STAT

Description: OMI Ping Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.
sysDownTime	System Downtime	uint32	
sysDegradedTime	System Degraded Time	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_OSPF_NBR_STATUS

Description: OSPF neighbor status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
ospfAreaId	OSPF Area Id	uint32	
ospfState	OSPF State	string	

EventType: PH_DEV_MON_PANASONIC_AERO_LOG_MON_STATUS

Description: Panasonic Aero Log Monitoring Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
collectorId	Collector ID	uint32	This field captures the ID of a FortiSIEM Collector
phCollectorName	Collector Name	string	Name of the FortiSIEM Collector. The name is set in GUI.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.
airlineName	Airline Name	string	
airlineTail	Airline Tail Number	string	
airlineDevName	Airline Device	string	
filePath	File Path	string	
scannedFiles	Scanned File Count	uint32	
totEventCount	Total Event Count	uint32	

EventType: PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_HIGH

Description: Performance monitoring delay for all devices from a collection point crossed high water mark

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_LOW

Description: Performance monitoring delay for all devices from a collection point fell below low water mark

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERFMON_DEVICE_DELAY_HIGH

Description: All performance metrics delay for a single device crossed high water mark

Severity: 9 (High)

Event Category: 3 (System Logs)

All Logs Page 3

Every FortiSIEM internally generated event log regardless of category

- PH_DEV_MON_PERFMON_DEVICE_DELAY_LOW
- PH_DEV_MON_PERFMON_JOB_DELAY_HIGH
- PH_DEV_MON_PERFMON_JOB_DELAY_LOW
- PH_DEV_MON_PERF_MSSQL_BACKUP_INFO
- PH_DEV_MON_PERF_MSSQL_BLOCKBY_INFO
- PH_DEV_MON_PERF_MSSQL_CONFIG_INFO
- PH_DEV_MON_PERF_MSSQL_ERROR_LOG_INFO
- PH_DEV_MON_PERF_MSSQL_GEN_INFO
- PH_DEV_MON_PERF_MSSQL_LOCK_INFO
- PH_DEV_MON_PERF_MSSQL_PERDB
- PH_DEV_MON_PERF_MSSQL_SYS
- PH_DEV_MON_PERF_MSSQL_TOP_QUERIES
- PH_DEV_MON_PERF_MYSQLDB
- PH_DEV_MON_PERF_MYSQLDB_TABLESPACE
- PH_DEV_MON_PERF_ORADB
- PH_DEV_MON_PERF_ORADB_CLUSTER
- PH_DEV_MON_PERF_ORADB_TABLESPACE
- PH_DEV_MON_PERF_ORADB_TOP_QUERIES
- PH_DEV_MON_PING_STAT
- PH_DEV_MON_PING_STAT_SUPPRESSED
- PH_DEV_MON_PORT_CLOSE
- PH_DEV_MON_PORT_OPEN
- PH_DEV_MON_PRINTER_OUTPUT_STATUS
- PH_DEV_MON_PRINTER_SUPPLY_STATUS
- PH_DEV_MON_PROC_CPU_UTIL
- PH_DEV_MON_PROC_MEM_UTIL
- PH_DEV_MON_PROC_RESOURCE_UTIL
- PH_DEV_MON_PROC_START
- PH_DEV_MON_PROC_STOP
- PH_DEV_MON_QUALYS_WEB_APP_FW
- PH_DEV_MON_RBD_BW
- PH_DEV_MON_RBD_CONN
- PH_DEV_MON_RBD_PEER_STAT
- PH_DEV_MON_RBD_PER_PORT_BW
- PH_DEV_MON_RBD_TOP_APP
- PH_DEV_MON_RBD_TOP_DEST
- PH_DEV_MON_RBD_TOP_SRC

- PH_DEV_MON_RBD_TOP_TALKER
- PH_DEV_MON_RDS_METRIC
- PH_DEV_MON_RUCKUS_ACCESS_POINT_STAT
- PH_DEV_MON_RUCKUS_CONTROLLER_STAT
- PH_DEV_MON_RUCKUS_SSID_PERF
- PH_DEV_MON_SERVERIRON_REAL_SERVER_STAT
- PH_DEV_MON_SLB_METRIC
- PH_DEV_MON_SNMP_PING_STAT
- PH_DEV_MON_SRC_AD_REPL_STAT
- PH_DEV_MON_STATUS
- PH_DEV_MON_STORAGE_PORT_DOWN_TO_UP
- PH_DEV_MON_STORAGE_PORT_UP_TO_DOWN
- PH_DEV_MON_SYS_CPU_UTIL
- PH_DEV_MON_SYS_DISK_FREE
- PH_DEV_MON_SYS_DISK_TREND_DAY
- PH_DEV_MON_SYS_DISK_TREND_MONTH
- PH_DEV_MON_SYS_DISK_TREND_WEEK
- PH_DEV_MON_SYS_DISK_UTIL
- PH_DEV_MON_SYS_EXT_CMD
- PH_DEV_MON_SYS_MEM_FREE
- PH_DEV_MON_SYS_MEM_UTIL
- PH_DEV_MON_SYS_PAGEFILE_USAGE
- PH_DEV_MON_SYS_PER_CPU_UTIL
- PH_DEV_MON_SYS_PROC_COUNT
- PH_DEV_MON_SYS_RESTART
- PH_DEV_MON_SYS_STAT
- PH_DEV_MON_SYS_STATUS
- PH_DEV_MON_SYS_SWAP_MEM_ERROR_MSG
- PH_DEV_MON_SYS_UPTIME
- PH_DEV_MON_SYS_VIRT_MEM_UTIL
- PH_DEV_MON_TARGET_FILE_CONTENT_CHANGE
- PH_DEV_MON_TOMCAT_CPU
- PH_DEV_MON_TOMCAT_DB
- PH_DEV_MON_TOMCAT_MEMORY
- PH_DEV_MON_TOMCAT_REQUEST_PROCESSOR
- PH_DEV_MON_TOMCAT_SERVLET
- PH_DEV_MON_TOMCAT_SESSION
- PH_DEV_MON_TOMCAT_THREAD_POOL
- PH_DEV_MON_TRACEROUTE_STAT
- PH_DEV_MON_UCS_HW_CHASSIS_STAT
- PH_DEV_MON_UCS_HW_FAN_STAT
- PH_DEV_MON_UCS_HW_MEMORY_STAT
- PH_DEV_MON_UCS_HW_PROCESSOR_STAT

- PH_DEV_MON_UCS_HW_PSU_STAT
- PH_DEV_MON_UPS_METRIC
- PH_DEV_MON_VMCLUSTER_CPU_UTIL
- PH_DEV_MON_VMCLUSTER_DATASTORE_IO
- PH_DEV_MON_VMCLUSTER_MEM_UTIL
- PH_DEV_MON_VMCLUSTER_STATUS
- PH_DEV_MON_VMRESPOOL_CPU_UTIL
- PH_DEV_MON_VMRESPOOL_MEM_UTIL
- PH_DEV_MON_VM_CPU_UTIL
- PH_DEV_MON_VM_DATASTORE_IO
- PH_DEV_MON_VM_DISK_IO
- PH_DEV_MON_VM_DISK_UTIL
- PH_DEV_MON_VM_MEM_UTIL
- PH_DEV_MON_VM_NET_INTF_UTIL
- PH_DEV_MON_VM_PER_CPU_UTIL
- PH_DEV_MON_VM_SNAPSHOT
- PH_DEV_MON_VM_STATE
- PH_DEV_MON_VM_TOOLS_STATUS
- PH_DEV_MON_VM_UPTIME
- PH_DEV_MON_VPN_CONN
- PH_DEV_MON_VPN_STATUS
- PH_DEV_MON_WATCHGUARD_POLICY_STAT
- PH_DEV_MON_WEBLOGIC_APP
- PH_DEV_MON_WEBLOGIC_DB_POOL
- PH_DEV_MON_WEBLOGIC_EJB
- PH_DEV_MON_WEBLOGIC_GEN
- PH_DEV_MON_WEBLOGIC_MEMORY
- PH_DEV_MON_WEBLOGIC_SERVLET
- PH_DEV_MON_WEBLOGIC_SESSION
- PH_DEV_MON_WEBLOGIC_THREAD_POOL
- PH_DEV_MON_WEBSPHERE_APP
- PH_DEV_MON_WEBSPHERE_AUTHENTICATION
- PH_DEV_MON_WEBSPHERE_CPU
- PH_DEV_MON_WEBSPHERE_DB_POOL
- PH_DEV_MON_WEBSPHERE_EJB
- PH_DEV_MON_WEBSPHERE_MEMORY
- PH_DEV_MON_WEBSPHERE_SERVLET
- PH_DEV_MON_WEBSPHERE_THREAD_POOL
- PH_DEV_MON_WEBSPHERE_TRANSACTION
- PH_DEV_MON_WMI_PING_STAT
- PH_DISCOVERY_COMPLETE
- PH_DISCOVERY_RESULT_SENT
- PH_DISCOV_ACCESS_IP_PARSE_ERROR

- PH_DISCOV_ADS_ACCOUNT_TO_EXPIRE
- PH_DISCOV_ADS_ACCT_DISABLED
- PH_DISCOV_ADS_DORMANT_ACCT
- PH_DISCOV_ADS_PASSWORD_NEVER_EXPIRES
- PH_DISCOV_ADS_PASSWORD_NOT_REQD
- PH_DISCOV_ADS_PASSWORD_STALE
- PH_DISCOV_ADS_PASSWORD_TO_EXPIRE
- PH_DISCOV_ARUBA_WLAN_HOST_LOCATION
- PH_DISCOV_AWS_DEVICE_DELETED
- PH_DISCOV_AWS_DEVICE_UNKNOWN
- PH_DISCOV_AWS_DISCOV_FAILED
- PH_DISCOV_AZURE_DISCOV_FAILED
- PH_DISCOV_BASIC_FAILED
- PH_DISCOV_BASIC_SKIPPED
- PH_DISCOV_BASIC_SNMP_DETAIL
- PH_DISCOV_BASIC_SNMP_ERROR
- PH_DISCOV_BASIC_SNMP_FAILED
- PH_DISCOV_BASIC_SNMP_STARTED
- PH_DISCOV_BASIC_SNMP_SUCCESS
- PH_DISCOV_BASIC_SSH_DETAIL
- PH_DISCOV_BASIC_SSH_ERROR
- PH_DISCOV_BASIC_SSH_FAILED
- PH_DISCOV_BASIC_SSH_STARTED
- PH_DISCOV_BASIC_SSH_SUCCESS
- PH_DISCOV_BASIC_STARTED
- PH_DISCOV_BGP_OSPF_FAILED
- PH_DISCOV_BROCADE_SERVER_IRON_HW_INFO_WARNING
- PH_DISCOV_CANCEL_UNKNOWN_REQ
- PH_DISCOV_CERT_FILE_DOWNLOAD_FAILURE
- PH_DISCOV_CHECKPOINT_TEST_CONN_FAILED
- PH_DISCOV_CISCO_ASA_GET_CONTEXT_FAILED
- PH_DISCOV_CISCO_ASA_IPSEC_VPN_FAILED
- PH_DISCOV_CISCO_ASA_RAS_VPN_FAILED
- PH_DISCOV_CISCO_ASA_RUN_CONFIG_FAILED
- PH_DISCOV_CISCO_ASA_SET_CONTEXT_FAILED
- PH_DISCOV_CISCO_ASA_STARTUP_CONFIG_FAILED
- PH_DISCOV_CISCO_CALL_MANAGER_WARNING
- PH_DISCOV_CISCO_CATOS_INTF_FAILED
- PH_DISCOV_CISCO_CDP_ERROR
- PH_DISCOV_CISCO_IOS_L2_WARNING
- PH_DISCOV_CISCO_IOS_TRUNK_PORT_ERROR
- PH_DISCOV_CISCO_JUNOS_L2_WARNING
- PH_DISCOV_CISCO_NXOS_HW_STATUS_WARNING

- PH_DISCOV_CISCO_NXOS_INTF_SHORT_NAME_NOT_FOUND
- PH_DISCOV_CISCO_NXOS_L2_WARNING
- PH_DISCOV_CISCO_WLAN_HOST_LOCATION
- PH_DISCOV_CLOCK_ROLLS_BACK
- PH_DISCOV_CONTACT_APP_SERVER
- PH_DISCOV_CREDEN_INSERT_ERROR
- PH_DISCOV_CUSTOM_MAP_LOAD_FAILED
- PH_DISCOV_DATA_DOMAIN_HW_STATUS_WARNING
- PH_DISCOV_DELL_BLADE_CHASSIS_WARNING
- PH_DISCOV_DELL_COMPELLENT_STORAGE_WARNING
- PH_DISCOV_DISCOV_REQ_GET_FAILED
- PH_DISCOV_DISCOV_RESULT_SENDER_THREADS_SPAWN_FAILED
- PH_DISCOV_DISCOV_THREADS_SPAWN_FAILED
- PH_DISCOV_EC2_INSTANCE_PARSE_FAILED
- PH_DISCOV EMC_CLARION_ERROR
- PH_DISCOV EMC_VNX_DISCOV_FAILED
- PH_DISCOV EMC_VNX_PING_FAILED
- PH_DISCOV_EQLOGIC_CONN_FAILED
- PH_DISCOV_EQLOGIC_HW_INFO_FAILED
- PH_DISCOV_ESX_HOST_PING_ONLY_DISCOV_ERROR
- PH_DISCOV_FAILED_INVALID_REQUEST
- PH_DISCOV_FAILED_INVALID_REQUEST_XML
- PH_DISCOV_FAILED_XML_ERROR
- PH_DISCOV_FAIL_CMDB_DEV
- PH_DISCOV_FILE_BASED_DISCOV_DIR_NOT_CONFIGURED
- PH_DISCOV_FILE_BASED_DISCOV_FAILED
- PH_DISCOV_FORTINET_CPU_INFO_WARNING
- PH_DISCOV_FORTINET_LINK_STAT_WARNING
- PH_DISCOV_FORTINET_SYS_UPDATE_VERSION_WARNING
- PH_DISCOV_GENERIC_ERROR
- PH_DISCOV_GEN_WLAN_HOST_LOCATION
- PH_DISCOV_GET_SNMP_ENGINE_ID_FAILED
- PH_DISCOV_HOST_CONVERT_PROCESS_UPTIME_ERROR
- PH_DISCOV_HOST_ERROR
- PH_DISCOV_HOST_INSTALL_SW_WARNING
- PH_DISCOV_HOST_LOCATE_PROCESS_ERROR
- PH_DISCOV_HOST_LOCATION
- PH_DISCOV_HOST_NET_INTF
- PH_DISCOV_HOST_STARTED
- PH_DISCOV_HOST_SUCCESS
- PH_DISCOV_HOST_SUCCESS_DETAIL
- PH_DISCOV_HOST_WARNING
- PH_DISCOV_HP3COM_HW_WARNING

- PH_DISCOV_HP_BLADE_HW_STATUS_WARNING
- PH_DISCOV_INIT_MODULE_FAILED
- PH_DISCOV_INTERFACE_VIA_SNMP_FAILED
- PH_DISCOV_IP_TYPE_INVALID
- PH_DISCOV_ISILON_HW_STATUS_WARNING
- PH_DISCOV_JMX_TEST_CONN_FAILED
- PH_DISCOV_JUNIPER_SSG_HW_INFO_WARNING
- PH_DISCOV_L2_FAILED
- PH_DISCOV_L2_STARTED
- PH_DISCOV_L2_SUCCESS
- PH_DISCOV_LDAP_ERROR
- PH_DISCOV_LDAP_OU_ERROR
- PH_DISCOV_LINUX_DSKTABLE_NOT_CONFIG
- PH_DISCOV_LOGIN_ERROR
- PH_DISCOV_NEXT_HOP_VIA_SNMP_FAILED
- PH_DISCOV_NIMBLE_VOLUME_WARNING
- PH_DISCOV_NOZOMI_DISCOV_FAILED
- PH_DISCOV_PARAM_PARSE_FAILED
- PH_DISCOV_PARSER_MSG_EXCEEDS_THRESHOLD
- PH_DISCOV_PARSER_MSG_THREAD_SPAWN_FAILED
- PH_DISCOV_PERF_TEMPLATE_LOAD_FAILED
- PH_DISCOV_PING_ONLY_LIST_NOT_MATCH
- PH_DISCOV_READ_COMPRESS_THRESHOLD_FAILED
- PH_DISCOV_RECVD_VALID_REQUEST
- PH_DISCOV_RESULT_SEND_FAILED
- PH_DISCOV_RESULT_SEND_WARNING
- PH_DISCOV_RESULT_XML_WRITE_FAILURE
- PH_DISCOV_RUNNING_SERVICE
- PH_DISCOV_RUN_JAVA_PROBE_ERROR
- PH_DISCOV_RUN_SW_FILTER_LOAD_FAILED
- PH_DISCOV_RUN_SW_FILTER_PARSE_FAILED
- PH_DISCOV_RUN_VM_TEST_CONN_ERROR
- PH_DISCOV_SKIPPED
- PH_DISCOV_SKIP_DEV
- PH_DISCOV_SNMP_ERROR
- PH_DISCOV_SSH_ERROR
- PH_DISCOV_START
- PH_DISCOV_TELNET_ERROR
- PH_DISCOV_TEST_CONN_GET_REQ_FAILED
- PH_DISCOV_TEST_CONN_MSRPC_ERROR
- PH_DISCOV_TEST_CONN_NO_UCSAPI_CRED
- PH_DISCOV_TEST_CONN_RESULT_SENDER_THREADS_SPAWN_FAILED
- PH_DISCOV_TEST_CONN_RESULT_SEND_ERROR

- PH_DISCOV_TEST_CONN_RESULT_SEND_WARNING
- PH_DISCOV_TEST_CONN_THREADS_SPAWN_FAILED
- PH_DISCOV_TEST_CONN_VMSDK_ERROR
- PH_DISCOV_TRIPP_UPS_HW_STATUS_WARNING
- PH_DISCOV_TRUNK_PORTS_ERROR
- PH_DISCOV_UNHANDLED_ACCESS_PROTO
- PH_DISCOV_UPLOAD_DATA_FAILED
- PH_DISCOV_VMWARE_DUP_DEV_ID
- PH_DISCOV_VMWARE_ERROR
- PH_DISCOV_VOIP_PHONE_ID
- PH_DISCOV_WMI_PULL_ERROR
- PH_DISC_DATA_PROCESS_ERROR
- PH_DIVIDE_BY_ZERO
- PH_DROP_EVENT_FROM_SHARED_BUFFER
- PH_DROP_INCIDENT
- PH_DROP_INCIDENT_COUNT
- PH_ES_ARCHIVE_STORAGE_CHECK_ERROR
- PH_ES_ARCHIVE_STORAGE_LOW
- PH_ES_ARCHIVE_STORAGE_PURGING_FAILED
- PH_ES_ARCHIVE_STORAGE_PURGING_FINISHED
- PH_ES_ARCHIVE_STORAGE_PURGING_STARTED
- PH_ES_ARCHIVE_STORAGE_PURGING_SUCCESS
- PH_ES_ARCHIVE_STORAGE_USAGE
- PH_ES_CCR_DELAY
- PH_ES_COLD_STORAGE_ARCHIVING_FAILED
- PH_ES_COLD_STORAGE_ARCHIVING_FINISHED
- PH_ES_COLD_STORAGE_ARCHIVING_STARTED
- PH_ES_COLD_STORAGE_ARCHIVING_SUCCESS
- PH_ES_COLD_STORAGE_CHECK_ERROR
- PH_ES_COLD_STORAGE_LOW
- PH_ES_COLD_STORAGE_PURGING_FAILED
- PH_ES_COLD_STORAGE_PURGING_FINISHED
- PH_ES_COLD_STORAGE_PURGING_STARTED
- PH_ES_COLD_STORAGE_PURGING_SUCCESS
- PH_ES_COLD_STORAGE_USAGE
- PH_ES_HOTCOLD_STORAGE_MOVING_FAILED
- PH_ES_HOTCOLD_STORAGE_MOVING_FINISHED
- PH_ES_HOTCOLD_STORAGE_MOVING_STARTED
- PH_ES_HOTCOLD_STORAGE_MOVING_SUCCESS
- PH_ES_HOT_STORAGE_ARCHIVING_FAILED
- PH_ES_HOT_STORAGE_ARCHIVING_FINISHED
- PH_ES_HOT_STORAGE_ARCHIVING_STARTED
- PH_ES_HOT_STORAGE_ARCHIVING_SUCCESS

- PH_ES_HOT_STORAGE_CHECK_ERROR
- PH_ES_HOT_STORAGE_LOW
- PH_ES_HOT_STORAGE_MOVING_FAILED
- PH_ES_HOT_STORAGE_MOVING_FINISHED
- PH_ES_HOT_STORAGE_MOVING_STARTED
- PH_ES_HOT_STORAGE_MOVING_SUCCESS
- PH_ES_HOT_STORAGE_PURGING_FAILED
- PH_ES_HOT_STORAGE_PURGING_FINISHED
- PH_ES_HOT_STORAGE_PURGING_STARTED
- PH_ES_HOT_STORAGE_PURGING_SUCCESS
- PH_ES_HOT_STORAGE_USAGE
- PH_ES_INDEX_SEGMENT_MERGE_FAILED
- PH_ES_REST_FAILED
- PH_ES_SM_ADD_INDEX_FAILED
- PH_ES_SM_HOURLCHECK_FAILED
- PH_ES_SM_INIT_FAILED
- PH_ES_SM_INIT_INDEX_FAILED
- PH_ES_SNAPSHOT_FAILED
- PH_ES_TO_NFS_ARCHIVE_FAILED_ADD_INDEX
- PH_ES_WARM_STORAGE_ARCHIVING_FAILED
- PH_ES_WARM_STORAGE_ARCHIVING_FINISHED
- PH_ES_WARM_STORAGE_ARCHIVING_STARTED
- PH_ES_WARM_STORAGE_ARCHIVING_SUCCESS
- PH_ES_WARM_STORAGE_CHECK_ERROR
- PH_ES_WARM_STORAGE_LOW
- PH_ES_WARM_STORAGE_MOVING_FAILED
- PH_ES_WARM_STORAGE_MOVING_FINISHED
- PH_ES_WARM_STORAGE_MOVING_STARTED
- PH_ES_WARM_STORAGE_MOVING_SUCCESS
- PH_ES_WARM_STORAGE_PURGING_FAILED
- PH_ES_WARM_STORAGE_PURGING_FINISHED
- PH_ES_WARM_STORAGE_PURGING_STARTED
- PH_ES_WARM_STORAGE_PURGING_SUCCESS
- PH_ES_WARM_STORAGE_USAGE
- PH_EVENT_ATTR_XML_ISSUE
- PH_EVENT_FORWARDER_CHECKSUM_MISMATCH
- PH_EVENT_FORWARDER_CONNECT_ERROR
- PH_EVENT_FORWARDER_DIR_OPEN_FAILURE
- PH_EVENT_FORWARDER_FILE_OPEN_FAILURE
- PH_EVENT_FORWARDER_FILE_RENAME_FAILURE
- PH_EVENT_FORWARDER_INIT_FAILURE
- PH_EVENT_FORWARDER_INVALID_GZIP_FILE
- PH_EVENT_FORWARDER_INVALID_PHOENIX_CONFIG

- PH_EVENT_FORWARDER_INVALID_PROTOCOL
- PH_EVENT_FORWARDER_KAFKA_ERROR
- PH_EVENT_FORWARDER_KAFKA_INIT_FAILURE
- PH_EVENT_FORWARDER_KAFKA_PRODUCE_ERROR
- PH_EVENT_FORWARDER_MKDIR_FAILURE
- PH_EVENT_FORWARDER_RUN_PROCESS_ERROR
- PH_EVENT_FORWARDER_SOCKET_ERROR
- PH_EVENT_FORWARDER_SOCKET_WRITE_ERROR
- PH_EVENT_FORWARDER_SSL_CERT_ERROR
- PH_EVENT_FORWARDER_SSL_ERROR
- PH_EVENT_FWD_CERT_LOAD_FAILED
- PH_EVENT_FWD_CERT_UNPAIRED
- PH_EVENT_FWD_DIR_MAKE_FAILED
- PH_EVENT_FWD_DIR_OPEN_FAILED
- PH_EVENT_FWD_FILE_RENAME_FAILED
- PH_EVENT_FWD_FULL_FORWARDING_FAILED
- PH_EVENT_FWD_GET_FILE_NUM_FAILURE
- PH_EVENT_FWD_GZ_CLOSE_ERROR
- PH_EVENT_FWD_GZ_FILE_OPEN_ERROR
- PH_EVENT_FWD_GZ_MD5_ERROR
- PH_EVENT_FWD_GZ_RENAME_ERROR
- PH_EVENT_FWD_GZ_SIZE_MISMATCH
- PH_EVENT_FWD_KAFKA_WARNING
- PH_EVENT_FWD_MD5_CHECKSUM_MISMATCH
- PH_EVENT_FWD_NETFLOW_REGEX_IGNORED
- PH_EVENT_FWD_PARTIAL_FORWARDING_FAILED
- PH_EVENT_FWD_PARTIAL_FORWARDING_WARNING
- PH_EVENT_FWD_PCRE_ERROR
- PH_EVENT_FWD_PROCESS_INIT_FAILED
- PH_EVENT_FWD_PROCESS_START_FAILED
- PH_EVENT_FWD_PROTO_FORWARDED_WRONG
- PH_EVENT_FWD_RENAME_GZ_ERROR
- PH_EVENT_FWD_RULE_PARSE_ERROR
- PH_EVENT_FWD_SOCKET_CONNECT_FAILED
- PH_EVENT_FWD_SOCKET_GET_FAILED
- PH_EVENT_FWD_SOCKET_WRITE_FAILED
- PH_EVENT_FWD_SSL_CREATE_FAILED
- PH_EVENT_FWD_SSL_SESSION_BUILD_FAILED
- PH_EVENT_FWD_UNEXPECTED_FILE_REMOVED
- PH_EVENT_PKG_ATTR_NOT_FOUND
- PH_EVENT_PKG_EMPTY_FILE_REMOVED
- PH_EVENT_PKG_FILE_ADD_TO_SVN_FAILED
- PH_EVENT_PKG_FILE_REMOVED_ERROR

- PH_EVENT_PKG_FILE_RENAME_FAILED
- PH_EVENT_PKG_FILE_STAT_FAILED
- PH_EVENT_PKG_FILE_UPLOAD_FAILED
- PH_EVENT_PKG_FILE_UPLOAD_SUCCESS_HIGH
- PH_EVENT_PKG_FILE_UPLOAD_SUCCESS_LOW
- PH_EVENT_PKG_GZ_CLOSE_FAILED
- PH_EVENT_PKG_GZ_FILE_OPEN_ERROR
- PH_EVENT_PKG_HTTP_FAILED
- PH_EVENT_PKG_HTTP_INIT_FAILED
- PH_EVENT_PKG_INSERT_TASK_FAILED
- PH_EVENT_PKG_NO_EVENT
- PH_EVENT_PKG_OPEN_DIR_FAILED
- PH_EVENT_PKG_PROCESS_INIT_FAILED
- PH_EVENT_PKG_PROCESS_START_FAILED
- PH_EVENT_PKG_QUEUE_GET_FAILED
- PH_EVENT_PKG_SERVER_LIST_UPLOAD_FAILED
- PH_EVENT_PKG_SERVICE_LIST_EMPTY
- PH_EVENT_PKG_TASK_ADD_TO_QUEUE_FAILED
- PH_EVENT_PKG_XML_PARSE_FAILED
- PH_EVTPKGGER_FILE_UPLOAD_FAILED
- PH_EVT_HANDLER_DBG
- PH_EVT_HANDLER_ERR
- PH_EVT_HANDLER_EVT_QUEUE_LARGE
- PH_EVT_HANDLER_EVT_QUEUE_WARNING
- PH_EVT_HANDLER_INFO
- PH_EVT_HANDLER_SVN_QUEUE_LARGE
- PH_EVT_HANDLER_SVN_QUEUE_WARNING
- PH_EVT_PACKAGER_COND_WAIT_ERROR
- PH_EVT_PACKAGER_FILE_CLOSE_FAILURE
- PH_EVT_PACKAGER_FILE_OPEN_FAILURE
- PH_EVT_PACKAGER_FILE_REMOVE_FAILURE
- PH_EVT_PACKAGER_FILE_RENAME_FAILURE
- PH_EVT_PACKAGER_FILE_STAT_FAILURE
- PH_EVT_PACKAGER_FILE_UPLOAD_FAILURE
- PH_EVT_PACKAGER_HTTP_RESPONSE_ERROR
- PH_EVT_PACKAGER_INIT_FAILURE
- PH_EVT_PACKAGER_REST_PARSE_ERROR
- PH_EVT_PACKAGER_RUN_PROCESS_ERROR
- PH_FAILED_TO_EXEC
- PH_FILE_NOT_FOUND
- PH_GCS_BUCKET_ACCESS_FAILURE
- PH_GENERIC_CRITICAL
- PH_GENERIC_DEBUG

- PH_GENERIC_ERROR
- PH_GENERIC_INFO
- PH_GENERIC_WARNING
- PH_GET_CURL_HANDLE_FAILED
- PH_GET_SUPER_LEADER_FAILURE
- PH_GRPC_CERT_CREATE_SUCCESS
- PH_GRPC_CERT_ERROR
- PH_GRPC_CERT_LOADED_FAILED
- PH_GRPC_CERT_UPDATE_FAILED
- PH_GRPC_CERT_UPDATE_SUCCESS
- PH_GRPC_FORTMAT_JSON_FAILED
- PH_GRPC_INIT_SSL_CONTEXT
- PH_GRPC_TASK_DATA_EMPTY
- PH_HDFS_ARCHIVE_STORAGE_LOW
- PH_HDFS_ARCHIVE_STORAGE_USAGE
- PH_HDFS_PURGING_FAILED
- PH_HDFS_PURGING_FINISHED
- PH_HDFS_PURGING_STARTED
- PH_HDFS_PURGING_SUCCESS
- PH_HTTP_CLIENT_COMPRESS_FAILED
- PH_HTTP_CLIENT_CURL_ERROR
- PH_HTTP_CLIENT_GET_CACHE_FROM_MONITOR_FAILED
- PH_HTTP_CLIENT_GET_DATA_FROM_CACHE_FAILED
- PH_HTTP_CLIENT_GET_INIT_RESPONSE_FAILED
- PH_HTTP_CLIENT_GET_INIT_RESPONSE_WARNING
- PH_HTTP_CLIENT_GET_RESPONSE_WARNING
- PH_HTTP_CLIENT_HOST_IS_NULL
- PH_HTTP_CLIENT_INIT_FAILURE
- PH_HTTP_CLIENT_INIT_WARNING
- PH_HTTP_CLIENT_INVALID_FILE_SIZE
- PH_HTTP_CLIENT_MKSTEMP_FAILED
- PH_HTTP_CLIENT_NO_FILE_PARAM
- PH_HTTP_CLIENT_PICK_SUPER_FAILED
- PH_HTTP_CLIENT_PREP_REQUEST_ERROR
- PH_HTTP_CLIENT_PUT_REDIRECT_FAILURE
- PH_HTTP_CLIENT_SETOPT_FAILED
- PH_HTTP_CLIENT_SET_HOST_WARNING
- PH_HTTP_CLIENT_UPLOAD_FILE_FAILED
- PH_HTTP_CLIENT_WRITE_CACHE_NULL
- PH_HTTP_INIT_FAILURE
- PH_HTTP_RESPONSE_FAILURE
- PH_IDENTITYMASTER_HTTP_UPLOAD_ERROR
- PH_IDENTITYMASTER_INIT_ERROR

- PH_IDENTITYWORKER_ATTRIB_ERROR
- PH_IDENTITYWORKER_EVT_LOAD_ERROR
- PH_IDENTITYWORKER_EVT_SEND_ERROR
- PH_IDENTITYWORKER_INIT_ERROR
- PH_IDENTITYWORKER_PARAM_ERROR
- PH_IDENTITYWORKER_PROCESSING_EPS
- PH_IDENTITYWORKER_SS_OBTAIN_ERROR
- PH_INCIDENT_ACTION_STATUS
- PH_INVALID_IP_ADDR
- PH_INVALID_PARAM
- PH_INVALID_PARAM_CNT
- PH_INVALID_PARAM_VAL_EMPTY
- PH_JAVA_AGENT_APPSERVER_CONN_ERROR
- PH_JAVA_AGENT_APPSERVER_EXECUTE_ERROR
- PH_JAVA_AGENT_CONTROLLER_CMD_PARSE_ERROR
- PH_JAVA_AGENT_CONTROLLER_CMD_READ_ERROR
- PH_JAVA_AGENT_CONTROLLER_GENERIC_ERROR
- PH_JAVA_AGENT_CONTROLLER_LINE_READ_ERROR
- PH_JAVA_AGENT_CONTROLLER_XML_READ_ERROR
- PH_JAVA_AGENT_CUSTOM_JDBC_CONN_ERROR
- PH_JAVA_AGENT_CUSTOM_JDBC_EXEC_ERROR
- PH_JAVA_AGENT_DISCOVERY_TEST_ERROR
- PH_JAVA_AGENT_ERROR
- PH_JAVA_AGENT_GLASSFISH_MONITOR_ERROR
- PH_JAVA_AGENT_GLASS_FISH_WARNING
- PH_JAVA_AGENT_GOOGLEAPPS_EXEC_ERROR
- PH_JAVA_AGENT_IBMDB2_AUDIT_CONN_ERROR
- PH_JAVA_AGENT_IBMDB2_AUDIT_EXEC_ERROR
- PH_JAVA_AGENT_IBM_DB2_CAT_READ_ERROR
- PH_JAVA_AGENT_IBM_DB2_CONN_ERROR
- PH_JAVA_AGENT_IBM_DB2_INTERNAL_ERROR
- PH_JAVA_AGENT_INFO
- PH_JAVA_AGENT_JBOSS_CONN_ERROR
- PH_JAVA_AGENT_JBOSS_EXEC_ERROR
- PH_JAVA_AGENT_JBOSS_MONITOR_ERROR
- PH_JAVA_AGENT_JDBC_PULL_UNSUPP_ERROR
- PH_JAVA_AGENT_JDBC_SQL_NOT_SUPPORT_ERROR
- PH_JAVA_AGENT_JMX_CONN_ERROR
- PH_JAVA_AGENT_JMX_EXEC_ERROR
- PH_JAVA_AGENT_JOB_EXECUTOR_ERROR
- PH_JAVA_AGENT_JOB_STATUS_UPLOAD_ERROR
- PH_JAVA_AGENT_JOB_TYPE_ERROR
- PH_JAVA_AGENT_JOB_XML_LOAD_ERROR

- PH_JAVA_AGENT_JOB_XML_PARSE_ERROR
- PH_JAVA_AGENT_MCAFEE_MYSQL_MONITOR_ERROR
- PH_JAVA_AGENT_MCAFEE_VULN_SCANNER_ERROR
- PH_JAVA_AGENT_MONITOR_GEN_ERROR
- PH_JAVA_AGENT_MONITOR_TIMEOUT_ERROR
- PH_JAVA_AGENT_MSSQL_DDL_CONN_ERROR
- PH_JAVA_AGENT_MSSQL_LOGON_CONN_ERROR
- PH_JAVA_AGENT_MSSQL_LOGON_EXEC_ERROR
- PH_JAVA_AGENT_MSSQL_MONITOR_ERROR
- PH_JAVA_AGENT_MSSQL_PERF_CONN_ERROR
- PH_JAVA_AGENT_MSSQL_PERF_EXECUTE_ERROR
- PH_JAVA_AGENT_MYSQL_PERF_CONN_ERROR
- PH_JAVA_AGENT_MYSQL_PERF_EXEC_ERROR
- PH_JAVA_AGENT_NESSUS_REPORT_PARSE_ERROR
- PH_JAVA_AGENT_ORACLE_DB_ERROR
- PH_JAVA_AGENT_ORADB_AUDIT_CONN_ERROR
- PH_JAVA_AGENT_ORADB_AUDIT_EXEC_ERROR
- PH_JAVA_AGENT_ORADB_LOGON_EXEC_ERROR
- PH_JAVA_AGENT_ORADB_PERF_CONN_ERROR
- PH_JAVA_AGENT_ORADB_PERF_EXEC_ERROR
- PH_JAVA_AGENT_SNORT_CONN_ERROR
- PH_JAVA_AGENT_SNORT_EVENTID_ERROR
- PH_JAVA_AGENT_SNORT_EXEC_ERROR
- PH_JAVA_AGENT_SNORT_SENSORID_ERROR
- PH_JAVA_AGENT_SNORT_TCP_OPTION_ERROR
- PH_JAVA_AGENT_TOMCAT_MONITOR_ERROR
- PH_JAVA_AGENT_UTILS_ERROR
- PH_JAVA_AGENT_VMWARE_HWSTATUS_EXEC_ERROR
- PH_JAVA_AGENT_VMWARE_LOG_CONN_ERROR
- PH_JAVA_AGENT_VMWARE_LOG_EXEC_ERROR
- PH_JAVA_AGENT_VMWARE_MONITOR_ERROR
- PH_JAVA_AGENT_VMWARE_PERF_COUNTER_MISSING
- PH_JAVA_AGENT_VMWARE_PERF_DATA_RETRIEVE_ERROR
- PH_JAVA_AGENT_VMWARE_PERF_ENTITY_MISSING
- PH_JAVA_AGENT_VMWARE_PERF_HOST_MISSING
- PH_JAVA_AGENT_VMWARE_PERF_MON_EXCEPTION
- PH_JAVA_AGENT_VMWARE_PERF_ROLLUP_MISSING
- PH_JAVA_AGENT_VMWARE_PERF_STAT_NAME_MISSING
- PH_JAVA_AGENT_VMWARE_PERF_VM_MISSING
- PH_JAVA_AGENT_VMWARE_THREAD_EXEC_ERROR
- PH_JAVA_AGENT_VULN_REPORT_PARSER_ERROR
- PH_JAVA_AGENT_VULN_REPORT_VERIFY_ERROR
- PH_JAVA_AGENT_WEBLOGIC_MONITOR_ERROR

- [PH_JAVA_AGENT_WEBSense_EMAIL_MISSING_LOGDB](#)
- [PH_JAVA_AGENT_WEBSense_JDBC_PULL_ERROR](#)
- [PH_JAVA_AGENT_WEBSense_MAIL_CONN_ERROR](#)
- [PH_JAVA_AGENT_WEBSense_MAIL_EXEC_ERROR](#)

EventType: PH_DEV_MON_PERFMON_DEVICE_DELAY_LOW

Description: Some performance metric delay for a single device fell below water mark

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERFMON_JOB_DELAY_HIGH

Description: A performance metric delay for a single device crossed high water mark

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERFMON_JOB_DELAY_LOW

Description: A performance metric delay for a single device fell below water mark

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_BACKUP_INFO

Description: Last backup info on SQL Server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_BLOCKBY_INFO

Description: Blocked process in SQL Server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_CONFIG_INFO

Description: SQL Server configuration

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_ERROR_LOG_INFO

Description: SQL Server error log information

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_GEN_INFO

Description: SQL Server general information

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_LOCK_INFO

Description: SQL Server lock information

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_PERDB

Description: Metrics for per database in SQL Server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_SYS

Description: Metrics for the total SQL Server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MSSQL_TOP_QUERIES

Description: Top queries against SQL Server database

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MYSQLDB

Description: MySQL database performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_MYSQLDB_TABLESPACE

Description: MySQL tablespace metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_ORADB

Description: Oracle database performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_ORADB_CLUSTER

Description: Oracle Cluster performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_ORADB_TABLESPACE

Description: Oracle tablespace metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PERF_ORADB_TOP_QUERIES

Description: Top queries against Oracle database

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PING_STAT

Description: Ping Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.
sysDownTime	System Downtime	uint32	

Id	Display name	Type	Description
sysDegradedTime	System Degraded Time	uint32	
pollIntv	Polling Interval	uint32	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_DEV_MON_PING_STAT_SUPPRESSED

Description: Ping stat suppressed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.

EventType: PH_DEV_MON_PORT_CLOSE

Description: A port is closed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
ipPort	IP Port	uint16	IP port number
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_PORT_OPEN

Description: A new port is open

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
serviceName	Service Name	string	
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
ipPort	IP Port	uint16	IP port number
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_PRINTER_OUTPUT_STATUS

Description: Printer Output Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
prtDevStatus	Printer Device Status	string	
prtPrintStatus	Printer Printing Status	string	
prtErrorState	Printer Error State	string	
prtPrintPageCount	Printed Page Count	uint32	

EventType: PH_DEV_MON_PRINTER_SUPPLY_STATUS

Description: Printer Supply Status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
prtSupplyType	Printer Supply Type	string	
prtSupplyName	Printer Supply Name	string	
prtMaxSupplyLevel	Printer Max Supply Level	int32	
prtCurrSupplyLevel	Printer Current Supply Level	int32	
prtSupplyUnit	Printer Supply Unit	string	
prtCurrSupplyUsedPct	Printer Pct Used Supply	double	

EventType: PH_DEV_MON_PROC_CPU_UTIL

Description: Process CPU Utilization stats

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_PROC_MEM_UTIL**Description:** Process Memory Utilization**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**EventType: PH_DEV_MON_PROC_RESOURCE_UTIL****Description:** Process CPU and Memory Utilization stats**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
swProcName	Software Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
procOwner	Process Owner	string	
memUtil	Memory Util	double	
cpuUtil	CPU Util	double	
appName	Application Name	string	
appGroupName	Application Group Name	string	
pollIntv	Polling Interval	uint32	
swParam	Software Param	string	
realMemPeakKBytes	Real Peak Memory KB	uint32	
virtMemKBytes	Virtual Memory KB	uint32	
peakVirtMemKBytes	Peak Virtual Memory KB	uint32	
diskReadKBytesPerSec	Disk Read Rate KBps	double	
diskWriteKBytesPerSec	Disk Write Rate KBps	double	
sysUpTime	System Uptime	uint32	

EventType: PH_DEV_MON_PROC_START

Description: Process Started

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
swProcName	Software Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
procOwner	Process Owner	string	
appName	Application Name	string	
appGroupName	Application Group Name	string	
pollIntv	Polling Interval	uint32	
swParam	Software Param	string	

EventType: PH_DEV_MON_PROC_STOP

Description: Process Stopped

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
swProcName	Software Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
procOwner	Process Owner	string	
appName	Application Name	string	
appGroupName	Application Group Name	string	
pollIntv	Polling Interval	uint32	
swParam	Software Param	string	

EventType: PH_DEV_MON_QUALYS_WEB_APP_FW**Description:** Qualys Web Application Firewall Log**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
eventTime	Event Occur Time	Date	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
type	Type	string	
ipsConfidence	Attack Confidence	string	
policyName	Policy Name	string	
msg	Message	string	

EventType: PH_DEV_MON_RBD_BW**Description:** Riverbed Steelhead appliance bandwidth metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
inLanBytes	Inbound Optimized Bytes LAN Side	uint32	
inWanBytes	Inbound Optimized Bytes WAN Side	uint32	
outLanBytes	Outbound Optimized Bytes LAN Side	uint32	
outWanBytes	Outbound Optimized Bytes WAN Side	uint32	

EventType: PH_DEV_MON_RBD_CONN

Description: Riverbed Steelhead appliance connection metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
optConn	Optimized Connections	uint32	
passthruOptConn	Passthrough Connections	uint32	
halfOpenOptConn	Half-open Optimized Connections	uint32	
halfClosedOptConn	Half-closed Optimized Connections	uint32	
estOptConn	Established Optimized Connections	uint32	
activeOptConn	Active Optimized Connections	uint32	
totalOptConn	Total Opt Connections	uint32	

EventType: PH_DEV_MON_RBD_PEER_STAT

Description: Riverbed Steelhead appliance Peer metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
rbdState	Riverbed Steelhead State	string	

Id	Display name	Type	Description
connFailure	Connection Failures	uint32	
reqTimeout	Request Timeout	uint32	
maxLatency	Max Latency	double	

EventType: PH_DEV_MON_RBD_PER_PORT_BW

Description: Riverbed Steelhead per port bandwidth metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
inLanBytes	Inbound Optimized Bytes LAN Side	uint32	
inWanBytes	Inbound Optimized Bytes WAN Side	uint32	
outLanBytes	Outbound Optimized Bytes LAN Side	uint32	
outWanBytes	Outbound Optimized Bytes WAN Side	uint32	

EventType: PH_DEV_MON_RBD_TOP_APP

Description: Riverbed Steelhead appliance top application metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_DEV_MON_RBD_TOP_DEST

Description: Riverbed Steelhead appliance top dest metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_DEV_MON_RBD_TOP_SRC

Description: Riverbed Steelhead appliance top src metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_DEV_MON_RBD_TOP_TALKER

Description: Riverbed Steelhead appliance top talker metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_DEV_MON_RDS_METRIC

Description: AWS RDS metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
instanceName	DB Instance Name	string	
type	Type	string	
dbCpuTimeRatio	DB CPU Time Ratio	double	
dbUserConn	DB User Connections	uint32	
diskQLen	Disk Queue Length	uint32	
freeMemKB	Free Memory	uint32	
freeDiskMB	Free Disk MB	uint32	
usedSwapMemKB	Used Swap Memory	uint32	
ioReadsPerSec	Total Read I/Os Rate	double	
ioWritesPerSec	Total Write I/Os Rate	double	
devDiskRdLatency	Disk Read Latency ms	double	
devDiskWrLatency	Disk Write Latency ms	double	

EventType: PH_DEV_MON_RUCKUS_ACCESS_POINT_STAT

Description: Ruckus Access Point Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
description	Description	string	
numRadio	Radio Count	uint32	

Id	Display name	Type	Description
numWlanClient	WLAN Station Count	uint32	WLAN Station Count found in SNMP based WLAN monitoring
knownRogueAP	Known Rogue APs	uint32	
connMode	Connection Mode	string	
firstJoinTime	First Join Time	Date	
lastBootTime	Last Boot Time	Date	
lastUpgradeTime	Last Upgrade Time	Date	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	

EventType: PH_DEV_MON_RUCKUS_CONTROLLER_STAT

Description: Ruckus Controller Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
numAp	AP Count	uint32	
numWlanClient	WLAN Station Count	uint32	WLAN Station Count found in SNMP based WLAN monitoring
newRogueAP	New Rogue APs	uint32	
knownRogueAP	Known Rogue APs	uint32	
wlanSentBytes	WLAN Sent Bytes	uint64	WLAN Sent Bytes found in SNMP based WLAN monitoring
wlanRecvBytes	WLAN Recv Bytes	uint64	WLAN Recv Bytes found in SNMP based WLAN monitoring

Id	Display name	Type	Description
wlanSentBitsPerSec	WLAN Sent Rate bps	double	WLAN Sent Rate (in bits/sec) found in SNMP based WLAN monitoring
wlanRecvBitsPerSec	WLAN Recv Rate bps	double	WLAN Recv Rate (in bits/sec)s found in SNMP based WLAN monitoring
lanSentBytes	LAN Sent Bytes	uint64	
lanRecvBytes	LAN Recv Bytes	uint64	
lanSentBitsPerSec	LAN Sent Rate bps	double	

EventType: PH_DEV_MON_RUCKUS_SSID_PERF

Description: Ruckus SSID Performance Metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
wlanSsid	WLAN SSID	string	WLAN Service Set Identifier (SSID) found in SNMP based WLAN monitoring
description	Description	string	
wlanName	WLAN Name	string	WLAN Name found in SNMP based WLAN monitoring
authenMethod	Authentication Method	string	
encryptAlgo	Encryption Algorithm	string	
isGuest	Guest VLAN	string	
srcVLAN	Source VLAN	uint16	The VLAN to which the Source Network Interface belongs. Source network interface through which a packet enters a network device.
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.

Id	Display name	Type	Description
sentBitsPerSec	Sent Bit Rate	double	
recvBitsPerSec	Received Bit Rate	double	
authSuccess	Auth Successes	uint32	
authFailure	Auth Failures	uint32	
assocSuccess	Assoc Success	uint32	
assocFailure	Assoc Failure	uint32	
assocDeny	Assoc Deny	uint32	
disassocAbnormal	Disassoc Abnormal	uint32	
disassocLeave	Disassoc Leave	uint32	
disassocMisc	Disassoc Misc	uint32	

EventType: PH_DEV_MON_SERVERIRON_REAL_SERVER_STAT

Description: Brocade ServerIron ADX Real Server Stat

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
realServerIP	Real Server IP	IP	
realServerState	Real Server State	string	
failedPortExists	Failed Port Exists	uint16	
openConnectionsCount	Open Connections	uint64	
peakConns	Peak Connections	uint64	
activeSessions	Active Sessions	uint64	

EventType: PH_DEV_MON_SLB_METRIC**Description:** Cisco Server Load Balancing metrics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
lbOpenConn	LB Open Conn	uint32	
lbFailedConn	LB Failed Conn	uint32	
lbL4Conn	LB L4 Conn	uint32	
lbL7Conn	LB L7 Conn	uint32	
lbDroppedL4Conn	LB Dropped L4 Conn	uint32	
lbDroppedL7Conn	LB Dropped L7 Conn	uint32	
lbHttpRedirectConn	LB HTTP Redirect Conn	uint32	
lbDroppedHttpRedirectConn	LB Dropped HTTP Redirect Conn	uint32	
lbAclDeniedConn	LB ACL Denied Conn	uint32	
lbTimedoutConn	LB Timed Out Conn	uint32	

EventType: PH_DEV_MON_SNMP_PING_STAT**Description:** SNMP Ping Statistics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.
sysDownTime	System Downtime	uint32	
sysDegradedTime	System Degraded Time	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_SRC_AD_REPL_STAT

Description: Windows Active Directory Source REPLSTAT command output

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_STATUS

Description: Status of devices monitored by FortiSIEM

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_STORAGE_PORT_DOWN_TO_UP

Description: Storage port came back up

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
spName	SAN Storage Processor Name	string	
spPortName	SAN Storage Port Name	string	
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.

EventType: PH_DEV_MON_STORAGE_PORT_UP_TO_DOWN

Description: Storage port went down

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
spName	SAN Storage Processor Name	string	
spPortName	SAN Storage Port Name	string	
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.

EventType: PH_DEV_MON_SYS_CPU_UTIL

Description: System CPU Utilization for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
cpuName	CPU Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cpuUtil	CPU Util	double	
pollIntv	Polling Interval	uint32	
sysCpuUtil	System CPU Util	double	
userCpuUtil	User CPU Util	double	
waitCpuUtil	Wait CPU Util	double	
kernCpuUtil	Kernel CPU Util	double	
contextSwitchPerSec	Context Switch Rate /sec	double	
cpuInterruptPerSec	CPU Interrupt Rate /sec	double	
cpuCore	CPU Cores	uint16	
loadAvg1min	Load Average 1 min	double	Linux Server load average (calculated over 1min ntervals). Linux load average is a metric that shows the number of tasks currently executed by the CPU and tasks waiting in the queue.
loadAvg5min	Load Average 5 min	double	Linux Server load average (calculated over 5min ntervals). Linux load average is a metric that shows the number of tasks currently executed by the CPU and tasks waiting in the queue.
loadAvg15min	Load Average 15 min	double	Linux Server load average (calculated over 15min ntervals). Linux load average is a metric that shows the number of tasks currently executed by the CPU and tasks waiting in the queue.
relayDevIpAddr	Relaying IP	IP	Relaying IP is most commonly used to specify the log relay appliance, usually a collector.
relayDevName	Relaying Device	string	This is the hostname of the relaying device, a log relay, which is most typically a FortiSIEM collector.

EventType: PH_DEV_MON_SYS_DISK_FREE

Description: Free disk space stats for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_SYS_DISK_TREND_DAY

Description: Daily Disk growth trend

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
diskGrowthMBDaily	Current Daily Disk Growth	double	
avgDiskGrowthMBDaily	Avg Daily Disk Growth	double	
timeToDiskFull	Days To Disk Full	int32	

EventType: PH_DEV_MON_SYS_DISK_TREND_MONTH

Description: Monthly disk growth trend

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	
diskGrowthMBMonthly	Current Monthly Disk Growth	double	
avgDiskGrowthMBMonthly	Avg Monthly Disk Growth	double	
timeToDiskFull	Days To Disk Full	int32	

EventType: PH_DEV_MON_SYS_DISK_TREND_WEEK

Description: Weekly disk growth trend

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	

Id	Display name	Type	Description
diskGrowthMBWeekly	Current Weekly Disk Growth	double	
avgDiskGrowthMBWeekly	Avg Weekly Disk Growth	double	
timeToDiskFull	Days To Disk Full	int32	

EventType: PH_DEV_MON_SYS_DISK_UTIL

Description: Disk Utilization stats for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
diskName	Disk Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskUtil	Disk Capacity Util	double	
totalDiskMB	Total Disk MB	uint32	
usedDiskMB	Used Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	
pollIntv	Polling Interval	uint32	
inodeUsedPct	Inode Util	double	
inodeUsed	Used Inodes	uint32	
inodeFree	Free Inodes	uint32	
inodeMax	Max Inodes	uint32	
fileUsedPct	File Util	double	
fileUsed	Used Files	uint32	
fileFree	Free Files	uint32	
fileMax	Max Files	uint32	
maxDiskUtil	Max Disk Util	double	

Id	Display name	Type	Description
maxInodeUsedPct	Max Inode Util	double	
maxFileUsedPct	Max File Util	double	
appTransportProto	Application Protocol	string	
resvDiskMB	Reserved Disk MB	uint32	
availDiskMB	Available Disk MB	uint32	

EventType: PH_DEV_MON_SYS_EXT_CMD

Description: Extensible commands status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
appName	Application Name	string	
command	Command	string	
exitValue	Command exit value	int32	
usrMsg	User defined msg	string	
extCmdErrStatus	Extensible Command Error Status	string	
errFixCmd	Error Fix Command	string	

EventType: PH_DEV_MON_SYS_MEM_FREE

Description: Free system memory stats for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
memName	Memory Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
freeMemKB	Free Memory	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_SYS_MEM_UTIL

Description: System memory Utilization stats for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
memName	Memory Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
memUtil	Memory Util	double	
pollIntv	Polling Interval	uint32	
freeMemKB	Free Memory	uint32	
bufMemKB	Buffer Memory	uint32	
cacheMemKB	Cache Memory	uint32	
swapMemUtil	Swap Memory Util	double	
freeSwapMemKB	Free Swap Memory	uint32	
swapInRate	Swap Read Rate Pages/sec	double	
swapOutRate	Swap Write Rate Pages/sec	double	
swapRate	Total Swap Rate Pages/sec	double	

Id	Display name	Type	Description
totalMemKB	Total Memory	uint32	
usedMemKB	Used Memory	uint32	
relayDevIpAddr	Relaying IP	IP	Relaying IP is most commonly used to specify the log relay appliance, usually a collector.
relayDevName	Relaying Device	string	This is the hostname of the relaying device, a log relay, which is most typically a FortiSIEM collector.

EventType: PH_DEV_MON_SYS_PAGEFILE_USAGE

Description: Pagefile usage for Windows systems

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
pageFileUsage	PageFile Usage	double	
pageFilePeakUsage	PageFile Peak Usage	double	

EventType: PH_DEV_MON_SYS_PER_CPU_UTIL

Description: System per CPU Utilization for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
cpuName	CPU Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cpuUtil	CPU Util	double	
pollIntv	Polling Interval	uint32	
sysCpuUtil	System CPU Util	double	
userCpuUtil	User CPU Util	double	

EventType: PH_DEV_MON_SYS_PROC_COUNT

Description: System process count for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
procCount	System Process Count	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_SYS_RESTART

Description: A device restarted

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
restartTime	Restart Time	Date	

EventType: PH_DEV_MON_SYS_STAT

Description: HP-UNIX logged in users and average system jobs statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
numUser	System Logged In User	uint32	
numJob	Average System Job	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_SYS_STATUS

Description: Overall System ststus

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
overallStatusCode	Overall Health	uint16	
systemStatus	System Health	string	
svcStatus	Service Health	string	
envTempDegC	Temperature Celsius	uint32	

EventType: PH_DEV_MON_SYS_SWAP_MEM_ERROR_MSG

Description: Swap memory error

Severity: 8 (Medium)

Event Category: 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
memName	Memory Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
swapMemUtil	Swap Memory Util	double	
freeSwapMemKB	Free Swap Memory	uint32	
memMinimumSwap	Minimum Swap Memory	uint32	
swapMemErrorString	Swap Memory Error	string	

EventType: PH_DEV_MON_SYS_UPTIME**Description:** System uptime for a device**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
sysUpTime	System Uptime	uint32	
sysUpTimePct	System Uptime Pct	double	
sysDownTime	System Downtime	uint32	
pollIntv	Polling Interval	uint32	
relayDevIpAddr	Relaying IP	IP	Relaying IP is most commonly used to specify the log relay appliance, usually a collector.

Id	Display name	Type	Description
relayDevName	Relaying Device	string	This is the hostname of the relaying device, a log relay, which is most typically a FortiSIEM collector.

EventType: PH_DEV_MON_SYS_VIRT_MEM_UTIL

Description: System virtual memory Utilization stats for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
memName	Memory Name	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
virtMemUsedKB	Virtual Memory	uint32	
virtMemUtil	Virtual Memory Util	double	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_TARGET_FILE_CONTENT_CHANGE

Description: Target file hash changed from gold standard

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
fileName	File Name	string	

Id	Display name	Type	Description
hashCode	Hash Code	string	
oldSVNVersion	Old SVN Version	uint32	
newSVNVersion	New SVN Version	uint32	
deletedItem	Deleted Item	string	
addedItem	Added Item	string	

EventType: PH_DEV_MON_TOMCAT_CPU

Description: Tomcat cpu usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TOMCAT_DB

Description: Tomcat database pool metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TOMCAT_MEMORY

Description: Tomcat memory usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TOMCAT_REQUEST_PROCESSOR

Description: Tomcat request processor metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TOMCAT_SERVLET

Description: Tomcat servlet metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TOMCAT_SESSION

Description: Tomcat session metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TOMCAT_THREAD_POOL

Description: Tomcat thread pool usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_TRACEROUTE_STAT

Description: Trace Route statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventTime	Event Occur Time	Date	
jobId	Job Id	string	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
srcName	Source Host Name	string	Source device's hostname as identified in the log, can also be enriched using reverse lookup of the source IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
hopNum	Hop Count	uint32	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.

EventType: PH_DEV_MON_UCS_HW_CHASSIS_STAT

Description: Cisco UCS Chassis status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
inputPowerWatt	Input Power Watt	double	
inputPowerAvgWatt	Avg Input Power Watt	double	

Id	Display name	Type	Description
inputPowerMaxWatt	Max Input Power Watt	double	
inputPowerMinWatt	Min Input Power Watt	double	
outputPowerWatt	Output Power Watt	double	
outputPowerAvgWatt	Avg Output Power Watt	double	
outputPowerMaxWatt	Max Output Power Watt	double	
outputPowerMinWatt	Min Output Power Watt	double	

EventType: PH_DEV_MON_UCS_HW_FAN_STAT

Description: Cisco UCS fan status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
fanSpeed	Fan Speed	double	
fanSpeedAvg	Avg Fan Speed	double	
fanSpeedMax	Max Fan Speed	double	
fanSpeedMin	Min Fan Speed	double	

EventType: PH_DEV_MON_UCS_HW_MEMORY_STAT

Description: Cisco UCS memory status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
envTempdDegC	Temperature Celsius Detailed	double	
envTempAvgDegC	Avg Temperature Celsius	double	
envTempMaxDegC	Max Temperature Celsius	double	
envTempMinDegC	Min Temperature Celsius	double	

EventType: PH_DEV_MON_UCS_HW_PROCESSOR_STAT

Description: Cisco UCS processor status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
inputCurrentAmp	Input Amp	double	
inputCurrentAvgAmp	Avg Input Amp	double	
inputCurrentMaxAmp	Max Input Amp	double	
inputCurrentMinAmp	Min Input Amp	double	
envTempdDegC	Temperature Celsius Detailed	double	
envTempAvgDegC	Avg Temperature Celsius	double	
envTempMaxDegC	Max Temperature Celsius	double	
envTempMinDegC	Min Temperature Celsius	double	

EventType: PH_DEV_MON_UCS_HW_PSU_STAT

Description: Cisco UCS power supply status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
envTempdDegC	Temperature Celsius Detailed	double	
envTempAvgDegC	Avg Temperature Celsius	double	
envTempMaxDegC	Max Temperature Celsius	double	
envTempMinDegC	Min Temperature Celsius	double	
input210Volt	Input 210 Volt	double	
input210AvgVolt	Avg Input 210 Volt	double	
input210MaxVolt	Max Input 210 Volt	double	
input210MinVolt	Min Input 210 Power Volt	double	
output12Volt	Output 12 Volt	double	
output12AvgVolt	Avg Output Volt	double	
output12MaxVolt	Max Output Volt	double	
output12MinVolt	Min Output Volt	double	
output3V3Volt	Output 3V3 Volt	double	
output3V3AvgVolt	Avg Output 3V3 Volt	double	
output3V3MaxVolt	Max Output 3V3 Volt	double	
output3V3MinVolt	Min Output 3V3 Volt	double	

Id	Display name	Type	Description
outputCurrentAmp	Output Amp	double	
outputCurrentAvgAmp	Avg Output Amp	double	
outputCurrentMaxAmp	Max Output Amp	double	
outputCurrentMinAmp	Min Output Amp	double	
outputPowerWatt	Output Power Watt	double	
outputPowerAvgWatt	Avg Output Power Watt	double	
outputPowerMaxWatt	Max Output Power Watt	double	
outputPowerMinWatt	Min Output Power Watt	double	

EventType: PH_DEV_MON_UPS_METRIC

Description: UPS metric

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
upsRemainBatteryChargePct	UPS Remaining Charge Pct	uint32	
upsBatteryStatus	UPS Battery Status	uint32	
upsReplaceBatteryIndicator	UPS Replace Battery Indicator	uint32	

Id	Display name	Type	Description
upsTimeOnBattery	UPS Time on Battery sec	uint32	
upsBasicOutputStatus	UPS Output Status	uint32	
upsAdvOutputLoad	UPS Output Load	uint32	
upsAdvOutputVoltage	UPS Output Voltage V	uint32	
upsAdvOutputFreq	UPS Output Frequency Hz	uint32	
upsEstSecRemain	UPS Time Remaining sec	uint32	
upsBatteryVoltage	UPS Battery Voltage	double	
upsBatteryCurrent	UPS Battery Current Amp	double	
upsBatteryTempC	UPS Battery Temperature Celsius	uint32	
upsBatteryTempF	UPS Battery Temperature Fahrenheit	uint32	
hwComponentName	Hardware Component Name	string	This field represents the hardware component that has an issue when the hardware status is Warning or Critical. For example when hwDiskStatus is 2 (Critical), this field states which disk has an issue.
upsAdvInputFreq	UPS Input FrequencyHz	uint32	
upsAdvInputVoltage	UPS Input Voltage	uint32	
upsOutputCurrent	UPS Output Current	double	
upsOutputPower	UPS Output Power	double	

EventType: PH_DEV_MON_VMCLUSTER_CPU_UTIL

Description: Physical CPU usage for a VMware Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VMCLUSTER_DATASTORE_IO

Description: Datastore IO stats for a VMware Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VMCLUSTER_MEM_UTIL

Description: Physical memory usage for a VMware Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VMCLUSTER_STATUS

Description: VMware cluster status

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VMRESPOOL_CPU_UTIL

Description: Physical CPU usage for a VMware Resource Pool

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VMRESPOOL_MEM_UTIL

Description: Physical memory usage for a VMware Resource Pool

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_CPU_UTIL

Description: Physical CPU usage for a Virtual Machine

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_DATASTORE_IO

Description: Datastore IO stats for a Virtual Machine

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_DISK_IO

Description: Disk IO stats for a Virtual Machine

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_DISK_UTIL

Description: VM datastore utilization

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_MEM_UTIL

Description: Physical memory usage for a Virtual Machine

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_NET_INTF_UTIL

Description: Network IO stats for a Virtual Machine

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_PER_CPU_UTIL

Description: Physical CPU utilization for a Virtual Machine's virtual CPU

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_SNAPSHOT

Description: Virtual Machine Snapshot

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_STATE

Description: Virtual Machine State

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_TOOLS_STATUS

Description: VMware tools status

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VM_UPTIME

Description: Virtual Machine's up time

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_VPN_CONN

Description: VPN Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
vpnConnCount	VPN Conn Count	uint32	

EventType: PH_DEV_MON_VPN_STATUS

Description: VPN Performance metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
vpnStatus	VPN Status	string	
vpnConnCount	VPN Conn Count	uint32	
sslVpnStatus	SSL VPN Status	string	
sslVpnConnCount	SSL VPN Conn Count	uint32	
vpnTunnelName	VPN Tunnel Name	string	
vpnConnType	VPN Conn Type	string	
remoteVpnIpAddr	Remote VPN Tunnel IP	IP	
sentBitsPerSec	Sent Bit Rate	double	

Id	Display name	Type	Description
recvBitsPerSec	Received Bit Rate	double	
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_WATCHGUARD_POLICY_STAT

Description: Watchguard Firebox Policy Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
policyName	Policy Name	string	
recvDecryptFail	Recv Decrypt Fail	uint64	
authFailure	Auth Failures	uint32	
failureCount	Failure Count	uint32	
activeSessions	Active Sessions	uint64	
totalNum	Total Number of Items	uint32	
totBytesPerSec	Total Byte Rate	double	
totPktsPerSec	Total Packet Rate	double	
pollIntv	Polling Interval	uint32	

EventType: PH_DEV_MON_WEBLOGIC_APP

Description: Weblogic app server configuration and metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_DB_POOL

Description: Weblogic database pool metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_EJB

Description: Weblogic EJB metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_GEN

Description: Weblogic generic settings

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_MEMORY

Description: Weblogic memory usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_SERVLET

Description: Weblogic servlet metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_SESSION

Description: Weblogic session metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBLOGIC_THREAD_POOL

Description: Weblogic thread pool usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_APP

Description: Websphere app server configuration and metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_AUTHENTICATION

Description: Websphere app server authentication metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_CPU

Description: Websphere CPU usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_DB_POOL

Description: Websphere database pool metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_EJB

Description: Websphere EJB metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_MEMORY

Description: Websphere memory usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_SERVLET

Description: Websphere servlet metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_THREAD_POOL

Description: Websphere thread pool usage metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WEBSPHERE_TRANSACTION

Description: Websphere app server transaction metrics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DEV_MON_WMI_PING_STAT

Description: WMI Ping Statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
avgDurationMSec	Avg Round Trip Time	uint32	This attribute represents Average Round Trip Time in msec. Typically used in Ping monitoring.
minDurationMSec	Min Round Trip Time	uint32	This attribute represents Minimum Round Trip Time in msec. Typically used in Ping monitoring.
maxDurationMSec	Max Round Trip Time	uint32	This attribute represents Maximum Round Trip Time in msec. Typically used in Ping monitoring.
pktLossPct	Packet Loss Pct	double	Ratio of lost packets to the total number of sent packets. Mostly set by ping monitoring.
sysDownTime	System Downtime	uint32	
sysDegradedTime	System Degraded Time	uint32	
pollIntv	Polling Interval	uint32	

EventType: PH_DISCOVERY_COMPLETE

Description: Discovery completed

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DISCOVERY_RESULT_SENT

Description: Discovery results sent to app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_ACCESS_IP_PARSE_ERROR

Description: Discovery module failed to parse device Access IP from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_ADS_ACCOUNT_TO_EXPIRE

Description: Active Directory account to expcure in 2 weeks

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	
daysToAccountExpiry	Days To Account Expiry	uint32	

EventType: PH_DISCOV_ADS_ACCT_DISABLED

Description: Accounts Disabled

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	

EventType: PH_DISCOV_ADS_DORMANT_ACCT

Description: Dormant User Accounts - not log on in last 30 days

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	
lastLogon	Last Logon Time	Date	
daysSinceLastLogon	Days Since Last Logon	uint32	

EventType: PH_DISCOV_ADS_PASSWORD_NEVER_EXPIRES

Description: Active Directory user password never expires

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	
passwordAge	Password Age	uint32	
passwordLastSet	Password Last Set	Date	

EventType: PH_DISCOV_ADS_PASSWORD_NOT_REQD

Description: Active Directory user password not required

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	

EventType: PH_DISCOV_ADS_PASSWORD_STALE

Description: Active Directory user password stale - more than 90 days

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	
passwordAge	Password Age	uint32	
passwordLastSet	Password Last Set	Date	

EventType: PH_DISCOV_ADS_PASSWORD_TO_EXPIRE

Description: Active Directory user password to expire in 2 weeks

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
user	User	string	

Id	Display name	Type	Description
userFullName	User Full Name	string	
userDN	User Distinguishing Name	string	
daysToPasswordExpiry	Days To Password Expiry	uint32	
passwordLastSet	Password Last Set	Date	

EventType: PH_DISCOV_ARUBA_WLAN_HOST_LOCATION

Description: Aruba WLAN AP connected Host Identity and Location

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostMACAddr	Host MAC	string	Host Layer 2 MAC Address in the log
user	User	string	
domain	Domain	string	
nepDevIpAddr	Network Access Device IP	IP	
nepDevName	Network Access Device	string	
nepDevPort	Network Access Device Port	string	
wlanSsid	WLAN SSID	string	WLAN Service Set Identifier (SSID) found in SNMP based WLAN monitoring
wlanChannelId	WLAN Channel Id	uint32	WLAN Channel Id found in SNMP based WLAN monitoring
wlanApAssocUpTime	WLAN AP Association Uptime	uint32	WLAN AP Association Uptime found in SNMP based WLAN monitoring
wlanMaxHostTxmitRate	WLAN Max Host Txmit Rate Mbps	uint32	WLAN Max Host Txmit Rate Mbps found in SNMP based WLAN monitoring
wlanContrIpAddr	WLAN Controller IP	IP	WLAN Controller IP found in SNMP based WLAN monitoring

Id	Display name	Type	Description
wlanContrHostName	WLAN Controller Host Name	string	WLAN Controller Host Name found in SNMP based WLAN monitoring
wlanRssi	WLAN RSSI dB	int32	WLAN RSSI dB found in SNMP based WLAN monitoring
wlanProtocol	WLAN Protocol	string	WLAN Protocol found in SNMP based WLAN monitoring

EventType: PH_DISCOV_AWS_DEVICE_DELETED

Description: FortiSIEM AWS Discovery discovered a terminated device - this device will be deleted from CMDB

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ec2InstanceId	EC2 Instance Id	string	
accountId	Account Id	string	
awsRegion	AWS Region	string	
status	Status	string	

EventType: PH_DISCOV_AWS_DEVICE_UNKNOWN

Description: Discovery module failed to recognize AWS device type

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_AWS_DISCOV_FAILED

Description: Discovery module failed to discover AWS environment

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_AZURE_DISCOV_FAILED

Description: Discovery module failed to discover AZURE environment

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_BASIC_FAILED

Description: Basic discovery completely failed for a device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_BASIC_SKIPPED

Description: Device discovery skipped because of device type discovery exclusion policy

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_BASIC_SNMP_DETAIL

Description: Device discovery via SNMP details

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovSuccessCode	PH Discovery Success Code	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BASIC_SNMP_ERROR

Description: Device discovery encountered errors

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_BASIC_SNMP_FAILED

Description: Basic device discovery via SNMP completely failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_BASIC_SNMP_STARTED

Description: Starting device discovery for a device via SNMP

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BASIC_SNMP_SUCCESS

Description: Device discovery via SNMP succeeded for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BASIC_SSH_DETAIL

Description: Device discovery via SSH details

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovSuccessCode	PH Discovery Success Code	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BASIC_SSH_ERROR

Description: Basic device discovery via SSH encountered errors

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_BASIC_SSH_FAILED

Description: Basic device discovery via SSH completely failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_BASIC_SSH_STARTED

Description: Device discovery via SSH started for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BASIC_SSH_SUCCESS

Description: Device discovery via SSH succeeded for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BASIC_STARTED

Description: Starting device discovery for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_BGP_OSPF_FAILED

Description: Failed to send discovery task request for BGP/OSPF change

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_BROCADE_SERVER_IRON_HW_INFO_WARNING

Description: Failed to discover Brocade server iron hardware status

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_CANCEL_UNKNOWN_REQ

Description: Discovery module received discovery cancel request with unknown request ID

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_CERT_FILE_DOWNLOAD_FAILURE

Description: Discovery module failed to download certificate file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_DISCOV_CHECKPOINT_TEST_CONN_FAILED

Description: Discovery module failed to test connectivity for a Checkpoint device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_CISCO_ASA_GET_CONTEXT_FAILED

Description: Discovery module failed to discover Cisco ASA device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
virtContext	Virtualization Context	string	

EventType: PH_DISCOV_CISCO_ASA_IPSEC_VPN_FAILED

Description: Discovery module failed to discover IPSEC VPN for Cisco ASA via SNMP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_ASA_RAS_VPN_FAILED

Description: Discovery module failed to discover RAS VPN for Cisco ASA via SNMP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_ASA_RUN_CONFIG_FAILED

Description: Discovery module failed to discover running config for Cisco ASA via Login

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
virtContext	Virtualization Context	string	

EventType: PH_DISCOV_CISCO_ASA_SET_CONTEXT_FAILED

Description: Discovery module failed to set context for Cisco ASA

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
virtContext	Virtualization Context	string	

EventType: PH_DISCOV_CISCO_ASA_STARTUP_CONFIG_FAILED

Description: Discovery module failed to discover startup config for Cisco ASA via Login

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
virtContext	Virtualization Context	string	

EventType: PH_DISCOV_CISCO_CALL_MANAGER_WARNING

Description: Discovery module failed to obtain Cisco Call Manager statistics

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_CISCO_CATOS_INTF_FAILED

Description: Discovery module failed to find interface by id and name for Cisco CatOS device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.

EventType: PH_DISCOV_CISCO_CDP_ERROR

Description: Discovery module failed to find local interface in CDP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_IOS_L2_WARNING

Description: Discovery module failed to discover Layer 2 for Cisco IOS device - no directly connected host entries

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_IOS_TRUNK_PORT_ERROR

Description: Discovery module encountered SNMP index lookup error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_JUNOS_L2_WARNING

Description: Discovery module failed to discover Layer 2 for JUNOS device - no directly connected host entries

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_NXOS_HW_STATUS_WARNING

Description: Discovery module failed to obtain Cisco NxOS hardware status

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_CISCO_NXOS_INTF_SHORT_NAME_NOT_FOUND

Description: Discovery module failed to find interface short name for Cisco NxOS

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_NXOS_L2_WARNING

Description: Discovery module failed to discover Layer 2 for Cisco NxOS device - no directly connected host entries

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_CISCO_WLAN_HOST_LOCATION

Description: Cisco WLAN AP connected Host Identity and Location

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
hostMACAddr	Host MAC	string	Host Layer 2 MAC Address in the log
user	User	string	
domain	Domain	string	
nepDevIpAddr	Network Access Device IP	IP	
nepDevName	Network Access Device	string	
nepDevPort	Network Access Device Port	string	
wlanSsid	WLAN SSID	string	WLAN Service Set Identifier (SSID) found in SNMP based WLAN monitoring
wlanContrIpAddr	WLAN Controller IP	IP	WLAN Controller IP found in SNMP based WLAN monitoring
wlanContrHostName	WLAN Controller Host Name	string	WLAN Controller Host Name found in SNMP based WLAN monitoring
wlanRssi	WLAN RSSI dB	int32	WLAN RSSI dB found in SNMP based WLAN monitoring
wlanSnr	WLAN SNR dB	uint32	WLAN SNR dB found in SNMP based WLAN monitoring
wlanProtocol	WLAN Protocol	string	WLAN Protocol found in SNMP based WLAN monitoring

EventType: PH_DISCOV_CLOCK_ROLLS_BACK

Description: FortiSIEM Discovery module discovers excessive clock skew during BGP/OSPF discovery

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_CONTACT_APP_SERVER

Description: Discovery module contacting app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_DISCOV_CREDEN_INSERT_ERROR

Description: Discovery module failed to insert device credential into its memory - discovery may fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_CUSTOM_MAP_LOAD_FAILED

Description: Discovery module failed to load customer map from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_DATA_DOMAIN_HW_STATUS_WARNING

Description: Discovery module failed to obtain hardware status from Data Domain device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_DELL_BLADE_CHASSIS_WARNING

Description: Discovery module failed to discover Dell Blade Chassis

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_DELL_COMPELLENT_STORAGE_WARNING

Description: Discovery module failed to discover volume info for Dell Compellent Storage device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_DISCOV_REQ_GET_FAILED

Description: Discovery module failed to get discovery request from App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_DISCOV_RESULT_SENDER_THREADS_SPAWN_FAILED

Description: Discovery module failed to spawn discovery result sender threads

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_DISCOV_THREADS_SPAWN_FAILED

Description: Discovery module failed to spawn discover threads

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_EC2_INSTANCE_PARSE_FAILED

Description: Discovery module failed to parse EC2 instance xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV EMC_CLARION_ERROR

Description: Discovery module failed to discover EMC Clarion

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV EMC_VNX_DISCOV_FAILED

Description: Discovery module failed to discover EMC VNX via navisec client

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
filePath	File Path	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_EMC_VNX_PING_FAILED

Description: Discovery module failed to ping EMC VNX

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
filePath	File Path	string	

EventType: PH_DISCOV_EQLOGIC_CONN_FAILED

Description: Discovery module failed to obtain EqualLogic connection info

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	

Id	Display name	Type	Description
oid	Object Identifier	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_EQLOGIC_HW_INFO_FAILED

Description: Discovery module failed to obtain EqualLogic metric

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
oid	Object Identifier	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_ESX_HOST_PING_ONLY_DISCOV_ERROR

Description: Ping only discovery for ESX host/vCenter failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_FAILED_INVALID_REQUEST

Description: Discovery failed - invalid discovery request from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_FAILED_INVALID_REQUEST_XML

Description: FortiSIEM discovery module received invalid XML from App Server - discovery will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_FAILED_XML_ERROR

Description: Discovery XML request parse error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_FAIL_CMDB_DEV

Description: Existing CMDB device (re)discovery failed

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_FILE_BASED_DISCOV_DIR_NOT_CONFIGURED

Description: File based discovery failed - discover_file_dir missing in phoenix_config.txt

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_FILE_BASED_DISCOV_FAILED

Description: File based discovery failed - cannot open discovery file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
filePath	File Path	string	

EventType: PH_DISCOV_FORTINET_CPU_INFO_WARNING

Description: Discovery module failed to discover cpu info for Fortinet appliance

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_FORTINET_LINK_STAT_WARNING

Description: Discovery module failed to discover link stat for Fortinet appliance

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_FORTINET_SYS_UPDATE_VERSION_WARNING

Description: Discovery module failed to discover system auto update versions for Fortinet appliance

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_GENERIC_ERROR

Description: Device discovery encountered generic errors

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_GEN_WLAN_HOST_LOCATION

Description: Generic WLAN AP connected Host Identity and Location

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostMACAddr	Host MAC	string	Host Layer 2 MAC Address in the log
user	User	string	
domain	Domain	string	
nepDevIpAddr	Network Access Device IP	IP	
nepDevName	Network Access Device	string	
nepDevPort	Network Access Device Port	string	
wlanSsid	WLAN SSID	string	WLAN Service Set Identifier (SSID) found in SNMP based WLAN monitoring
wlanContrIpAddr	WLAN Controller IP	IP	WLAN Controller IP found in SNMP based WLAN monitoring
wlanContrHostName	WLAN Controller Host Name	string	WLAN Controller Host Name found in SNMP based WLAN monitoring

EventType: PH_DISCOV_GET_SNMP_ENGINE_ID_FAILED

Description: Failed to get snmp engine ID

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_HOST_CONVERT_PROCESS_UPTIME_ERROR

Description: Discovery module failed to convert process uptime

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_HOST_ERROR

Description: Discovery module failed to discover device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_HOST_INSTALL_SW_WARNING

Description: Discovery module failed to discover installed software

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_HOST_LOCATE_PROCESS_ERROR

Description: Discovery module failed to locate running process by SNMP id

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_HOST_LOCATION

Description: Wired Host IP location message

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_HOST_NET_INTF

Description: Host network interface identity message

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostMACAddr	Host MAC	string	Host Layer 2 MAC Address in the log
computer	Computer	string	

EventType: PH_DISCOV_HOST_STARTED

Description: Host discovery started for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_HOST_SUCCESS

Description: Host discovery succeeded for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_HOST_SUCCESS_DETAIL

Description: Host discovery success details

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovSuccessCode	PH Discovery Success Code	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_HOST_WARNING

Description: Discovery module failed to discover device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	

EventType: PH_DISCOV_HP3COM_HW_WARNING

Description: Discovery module failed to discover hardware info for HP3Com

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_HP_BLADE_HW_STATUS_WARNING

Description: Discovery module failed to obtain hardware status from HP Blade device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_INIT_MODULE_FAILED

Description: Discovery module failed to initialize

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_INTERFACE_VIA_SNMP_FAILED

Description: Discovery module failed to discover network interfaces vis SNMP

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_ISILON_HW_STATUS_WARNING

Description: Discovery module failed to obtain hardware status from Isilon device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_JMX_TEST_CONN_FAILED

Description: Discovery module failed to test conn for JMX server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_JUNIPER_SSG_HW_INFO_WARNING

Description: Juniper SSG hardware warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_L2_FAILED

Description: Layer 2 device discovery completely failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_L2_STARTED

Description: Layer 2 device discovery started for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_DISCOV_L2_SUCCESS

Description: Layer 2 device discovery succeeded for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_LDAP_ERROR

Description: LDAP discovery failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_LDAP_OU_ERROR

Description: Discovery module failed to lookup LDAP OU in its memory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_LINUX_DSKTABLE_NOT_CONFIG

Description: Linux disk discovery incomplete - Dsktable MIB not configured on Linux server

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
diskName	Disk Name	string	

EventType: PH_DISCOV_LOGIN_ERROR

Description: Discovery / Perf monitoring module failed to execute command via SSH/TELNET

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	
script	Script	string	
command	Command	string	

EventType: PH_DISCOV_NEXT_HOP_VIA_SNMP_FAILED

Description: Discovery module failed to discover next hop address vis SNMP

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_NIMBLE_VOLUME_WARNING

Description: Failed to discover volume for Nimble storage

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_NOZOMI_DISCOV_FAILED

Description: Discovery module failed to discover Nozomi environment

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_PARAM_PARSE_FAILED

Description: Discovery module failed to parse parameters in discovery XML from App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_PARSER_MSG_EXCEEDS_THRESHOLD

Description: Number of parser-to-discover messages to be processed exceeds threshold, discard the oldest one

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_PARSER_MSG_THREAD_SPAWN_FAILED

Description: Discovery module failed to spawn processParserMessage thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_PERF_TEMPLATE_LOAD_FAILED

Description: Discovery module failed to load performance template from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_PING_ONLY_LIST_NOT_MATCH

Description: Discovery module found that ping-only-discover device list does not match include-ip device list. Ping-only-discovery is not effective

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_READ_COMPRESS_THRESHOLD_FAILED

Description: Discovery module failed to read discover_compress_threshold from phoenix configuration, will set it to 2048 bytes

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_RECVD_VALID_REQUEST

Description: Received valid discovery request from app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_DISCOV_RESULT_SEND_FAILED

Description: Discovery module failed to send discovery result to App server after many retries; discovery will fail

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_RESULT_SEND_WARNING

Description: Discovery module failed to upload discovery result to App Server, will retry

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_RESULT_XML_WRITE_FAILURE

Description: Discovery module failed to create discovery result XML file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_DISCOV_RUNNING_SERVICE

Description: Found running service on host

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
appName	Application Name	string	

EventType: PH_DISCOV_RUN_JAVA_PROBE_ERROR

Description: Discovery module failed to execute runJavaProbe.sh

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
exitValue	Command exit value	int32	

EventType: PH_DISCOV_RUN_SW_FILTER_LOAD_FAILED

Description: Discovery module failed to load Running Software Filter from App Server - running software filter may not be discovered correctly

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_RUN_SW_FILTER_PARSE_FAILED

Description: Discovery module failed to parse running software filter xml from App Server - running software filter may not be discovered correctly

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_RUN_VM_TEST_CONN_ERROR

Description: Discovery module failed to execute VMWare Test Connectivity (runVmTestConn.sh)

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
exitValue	Command exit value	int32	

EventType: PH_DISCOV_SKIPPED

Description: Skipping device discovery by discovery request policy

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_SKIP_DEV

Description: Discovery skipped a device for discovery

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

EventType: PH_DISCOV_SNMP_ERROR

Description: Discovery module failed to get data via SNMP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_SSH_ERROR

Description: Discovery module failed to execute command via SSH

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	
script	Script	string	
command	Command	string	

EventType: PH_DISCOV_START

Description: Discovery module starting

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TELNET_ERROR

Description: Discovery module failed to execute command via TELNET

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
phDiscovFailCode	PH Discovery Failure Code	string	
script	Script	string	
command	Command	string	

EventType: PH_DISCOV_TEST_CONN_GET_REQ_FAILED

Description: Discovery module failed to get test connectivity request from App server

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TEST_CONN_MSRPC_ERROR

Description: Discovery module failed to test connection to a Windows Server via MSRPC

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
filePath	File Path	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_TEST_CONN_NO_UCSAPI_CRED

Description: Discovery module failed to test connection to a Cisco UCS Server via UCS API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TEST_CONN_RESULT_SENDER_THREADS_SPAWN_FAILED

Description: Discovery module failed to spawn test connectivity result sender threads

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TEST_CONN_RESULT_SEND_ERROR

Description: Discovery module encountered error in sending Test Connectivity result to app server

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phDiscovFailCode	PH Discovery Failure Code	string	

EventType: PH_DISCOV_TEST_CONN_RESULT_SEND_WARNING

Description: Discovery module failed to upload test connectivity result to App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TEST_CONN_THREADS_SPAWN_FAILED

Description: Discovery module failed to spawn test connectivity threads

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_TEST_CONN_VMSDK_ERROR

Description: Discovery module encountered VMSDK test connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_TRIPP_UPS_HW_STATUS_WARNING

Description: Discovery module failed to obtain hardware status from Tripp UPS device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_TRUNK_PORTS_ERROR

Description: Discovery module failed to get network device trunk port information from App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_UNHANDLED_ACCESS_PROTO

Description: Discovery module encountered unhandled device access method

Severity: 4 (Low)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_UPLOAD_DATA_FAILED

Description: Discovery module failed to upload discovery results to App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_DISCOV_VMWARE_DUP_DEV_ID

Description: Discovery module encountered VMSDK discovery error because of duplicated device id

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
filePath	File Path	string	

EventType: PH_DISCOV_VMWARE_ERROR

Description: Discovery module failed to discover device via VMSDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DISCOV_VOIP_PHONE_ID

Description: VoIP phone identity message

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
computer	Computer	string	
hostMACAddr	Host MAC	string	Host Layer 2 MAC Address in the log
user	User	string	
domain	Domain	string	
voIPPhoneStatus	VoIP Phone Status	string	

EventType: PH_DISCOV_WMI_PULL_ERROR

Description: Windows WMI pulling error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DISC_DATA_PROCESS_ERROR

Description: Discovery result process error

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DIVIDE_BY_ZERO

Description: Devide by zero

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_DROP_EVENT_FROM_SHARED_BUFFER

Description: Event dropped from shared buffer

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
collectorId	Collector ID	uint32	This field captures the ID of a FortiSIEM Collector
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_DROP_INCIDENT

Description: Incident dropped

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.
incidentId	Incident ID	uint64	Unique ID of a FortiSIEM Incident
details	Details	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_DROP_INCIDENT_COUNT

Description: Dropped incident count

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
incidentCount	Triggered Event Count	uint32	This field represents the number of Triggering events in an Incident.
policyName	Policy Name	string	

EventType: PH_ES_ARCHIVE_STORAGE_CHECK_ERROR

Description: Failed to get disk usage of Elasticsearch Cluster archive

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_ES_ARCHIVE_STORAGE_LOW

Description: The available storage of archive for Elasticsearch Cluster is low

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_ARCHIVE_STORAGE_PURGING_FAILED

Description: Failed purge snapshot from archive on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_ES_ARCHIVE_STORAGE_PURGING_FINISHED

Description: Finished purge snapshot from archive on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_ARCHIVE_STORAGE_PURGING_STARTED

Description: Start purge snapshots from archive on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_ARCHIVE_STORAGE_PURGING_SUCCESS

Description: Succeed purge snapshots from archive on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_ARCHIVE_STORAGE_USAGE

Description: Disk usage of Elasticsearch Cluster archive

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_CCR_DELAY

Description: Elasticsearch CCR delay detail

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_COLD_STORAGE_ARCHIVING_FAILED

Description: Failed to archive indices from cold nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_COLD_STORAGE_ARCHIVING_FINISHED

Description: Finished archive indices from cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_COLD_STORAGE_ARCHIVING_STARTED

Description: Start archive indices from cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_COLD_STORAGE_ARCHIVING_SUCCESS

Description: Successfully archived indices from cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_COLD_STORAGE_CHECK_ERROR

Description: Failed to get disk usage of Elasticsearch Cluster cold nodes

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_ES_COLD_STORAGE_LOW

Description: The available storage of cold nodes on Elasticsearch Cluster is low

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_COLD_STORAGE_PURGING_FAILED

Description: Failed purge indices from cold nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_COLD_STORAGE_PURGING_FINISHED

Description: Finished purge indices from cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_COLD_STORAGE_PURGING_STARTED

Description: Start purge indices from cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_COLD_STORAGE_PURGING_SUCCESS

Description: Succeed purge indices from cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_COLD_STORAGE_USAGE

Description: Disk usage of Elasticsearch Cold nodes

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_HOTCOLD_STORAGE_MOVING_FAILED

Description: Failed move indices from Hot to cold nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_HOTCOLD_STORAGE_MOVING_FINISHED

Description: Finished moved indices from Hot to cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOTCOLD_STORAGE_MOVING_STARTED

Description: Start move indices from Hot to cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOTCOLD_STORAGE_MOVING_SUCCESS

Description: Succeed moved indices from Hot to cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_ARCHIVING_FAILED

Description: Failed archive indices from hot nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_HOT_STORAGE_ARCHIVING_FINISHED

Description: Finished archive indices from hot nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_ARCHIVING_STARTED

Description: Start archive indices from hot nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_ARCHIVING_SUCCESS

Description: Succeed archive indices from hot nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_CHECK_ERROR

Description: Failed to get disk usage of Elasticsearch Cluster Hot Nodes

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_ES_HOT_STORAGE_LOW

Description: The available storage of Hot Nodes on Elasticsearch Cluster is low

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_HOT_STORAGE_MOVING_FAILED

Description: Failed move indices from Hot to warm nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_HOT_STORAGE_MOVING_FINISHED

Description: Finished moved indices from Hot to warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_MOVING_STARTED

Description: Start move indices from Hot to warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_MOVING_SUCCESS

Description: Succeed moved indices from Hot to warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_PURGING_FAILED

Description: Failed purge indices from hot nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_HOT_STORAGE_PURGING_FINISHED

Description: Finished purge indices from hot nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_PURGING_STARTED

Description: Start purge indices from hot nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_PURGING_SUCCESS

Description: Succeed purge indices from hot nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_HOT_STORAGE_USAGE

Description: Disk usage of Elasticsearch Hot Nodes

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_INDEX_SEGMENT_MERGE_FAILED

Description: Elasticsearch index segment merge failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_ES_REST_FAILED

Description: ES REST returns error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_SM_ADD_INDEX_FAILED

Description: Failed to add ShardManager Index

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_SM_HOURCHECK_FAILED

Description: Failed ShardManager hourcheck

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_SM_INIT_FAILED

Description: Failed to init ShardManager

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_SM_INIT_INDEX_FAILED

Description: Failed to init ShardManager Index

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_SNAPSHOT_FAILED

Description: Failed to do snapshot for ES

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_TO_NFS_ARCHIVE_FAILED_ADD_INDEX

Description: ES TO NFS Archive failed to add an index

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_ES_WARM_STORAGE_ARCHIVING_FAILED

Description: Failed to archive indices from warm nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_WARM_STORAGE_ARCHIVING_FINISHED

Description: Finished archive indices from warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_ARCHIVING_STARTED

Description: Start archive indices from warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_ARCHIVING_SUCCESS

Description: Successfully archived indices from warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_CHECK_ERROR

Description: Failed to get disk usage of Elasticsearch Cluster warm nodes

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_ES_WARM_STORAGE_LOW

Description: The available storage of warm nodes on Elasticsearch Cluster is low

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_ES_WARM_STORAGE_MOVING_FAILED

Description: Failed move indices from Warm to cold nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_WARM_STORAGE_MOVING_FINISHED

Description: Finished moved indices from Warm to cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_MOVING_STARTED

Description: Start move indices from Warm to cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_MOVING_SUCCESS

Description: Succeed moved indices from Warm to cold nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_PURGING_FAILED

Description: Failed purge indices from warm nodes on Elasticsearch Cluster

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_ES_WARM_STORAGE_PURGING_FINISHED

Description: Finished purge indices from warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_PURGING_STARTED

Description: Start purge indices from warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_PURGING_SUCCESS

Description: Succeed purge indices from warm nodes on Elasticsearch Cluster

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_ES_WARM_STORAGE_USAGE

Description: Disk usage of Elasticsearch Warm nodes

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_EVENT_ATTR_XML_ISSUE

Description: Event attribute xml issue

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FORWARDER_CHECKSUM_MISMATCH

Description: FortiSIEM Event Forwarder module encountered checksum error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FORWARDER_CONNECT_ERROR

Description: FortiSIEM Event Forwarder failed to connect to forwarding destination host

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_EVENT_FORWARDER_DIR_OPEN_FAILURE

Description: FortiSIEM Event Forwarder failed to open directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_EVENT_FORWARDER_FILE_OPEN_FAILURE

Description: FortiSIEM Event Forwarder failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FORWARDER_FILE_RENAME_FAILURE

Description: FortiSIEM Event Forwarder failed to rename file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	

EventType: PH_EVENT_FORWARDER_INIT_FAILURE

Description: FortiSIEM Event Forwarder module initialization failure

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_EVENT_FORWARDER_INVALID_GZIP_FILE

Description: FortiSIEM Event Forwarder module encountered invalid gzip file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FORWARDER_INVALID_PHOENIX_CONFIG

Description: FortiSIEM Event Forwarder module encountered invalid phoenix_config file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	
configName	Config Name	string	
configValue	Config Value	string	

EventType: PH_EVENT_FORWARDER_INVALID_PROTOCOL

Description: FortiSIEM Event Forwarder module encountered invalid forwarding protocol

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FORWARDER_KAFKA_ERROR

Description: FortiSIEM Event Forwarder module encountered Kafka protocol error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
actionName	Notification Action Name	string	

EventType: PH_EVENT_FORWARDER_KAFKA_INIT_FAILURE

Description: FortiSIEM Event Forwarder module initialization failure

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_EVENT_FORWARDER_KAFKA_PRODUCE_ERROR

Description: FortiSIEM Event Forwarder module encountered error while forwarding via Kafka protocol

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_EVENT_FORWARDER_MKDIR_FAILURE

Description: FortiSIEM Event Forwarder failed to create directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_EVENT_FORWARDER_RUN_PROCESS_ERROR

Description: FortiSIEM Event Forwarder failed to run process during execution

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FORWARDER_SOCKET_ERROR

Description: FortiSIEM Event Forwarder failed to create socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_EVENT_FORWARDER_SOCKET_WRITE_ERROR

Description: FortiSIEM Event Forwarder failed to write to socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_EVENT_FORWARDER_SSL_CERT_ERROR

Description: FortiSIEM Event Forwarder SSL certification error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_EVENT_FORWARDER_SSL_ERROR

Description: FortiSIEM Event Forwarder Generic SSL error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_EVENT_FWD_CERT_LOAD_FAILED

Description: Event Forwarder module failed to load certification file or key file for TLS based forwarding - forwarding via this method will not occur

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_EVENT_FWD_CERT_UNPAIRED

Description: Event Forwarder module detected unpaired certification file or key file - forwarding via this method will not occur

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_EVENT_FWD_DIR_MAKE_FAILED

Description: Event Forwarder module failed to create a directory during initialization

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_EVENT_FWD_DIR_OPEN_FAILED

Description: Event Forwarder module failed to open a directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_EVENT_FWD_FILE_RENAME_FAILED

Description: Event Forwarder module failed to rename a file

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	

EventType: PH_EVENT_FWD_FULL_FORWARDING_FAILED

Description: Event Forwarder failed to forward all events in one file to the destination, will retry

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_EVENT_FWD_GET_FILE_NUM_FAILURE

Description: Event Forwarder module failed to get event file count in /opt/phoenix/cache/parser/fwd

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_GZ_CLOSE_ERROR

Description: Event Forwarder module cannot close gz file stored in /opt/phoenix/cache/parser/fwd - event will not be forwarded

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FWD_GZ_FILE_OPEN_ERROR

Description: Event Forwarder failed to open event file (gz), or not enough memory to open it

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FWD_GZ_MD5_ERROR

Description: Event Forwarder module cannot get md5 of event file (gz)

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FWD_GZ_RENAME_ERROR

Description: Event Forwarder module cannot rename event file (gz)

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_GZ_SIZE_MISMATCH

Description: Event Forwarder found malformed event file (gz) - length mismatch

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FWD_KAFKA_WARNING

Description: Event Forwarder module failed on event serialization to send via Kafka

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_MD5_CHECKSUM_MISMATCH

Description: Event Forwarder found event file (gz) MD5 checksum

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_NETFLOW_REGEX_IGNORED

Description: Event Forwarder ignores regex filter in forwarding rule for Netflow since Netflow is binary

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_PARTIAL_FORWARDING_FAILED

Description: Event Forwarder failed to forward a subset of events in one file to the destination. Those events will be lost

Severity: 8 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_PARTIAL_FORWARDING_WARNING

Description: FortiSIEM Event Forwarder was able to do partial forwarding

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_EVENT_FWD_PCRE_ERROR

Description: Event Forwarder module failed to Pcre compile - this means the regular expression in the forwarding rule is invalid

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_PROCESS_INIT_FAILED

Description: Event Forwarder failed to initialize this process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_PROCESS_START_FAILED

Description: Event Forwarder failed to run

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_PROTO_FORWARDED_WRONG

Description: Event Forwarder found incorrect proto in the forwarding rule

Severity: 8 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_RENAME_GZ_ERROR

Description: FortiSIEM Event Forwarder failed to rename gz file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_FWD_RULE_PARSE_ERROR

Description: Event forwarder module failed to parse event forwarding rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_SOCKET_CONNECT_FAILED

Description: Event Forwarder failed to connect the destination for TCP based forwarding

Severity: 8 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_EVENT_FWD_SOCKET_GET_FAILED

Description: Event Forwarder failed to get socket for connecting the destination

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_EVENT_FWD_SOCKET_WRITE_FAILED

Description: Event Forwarder failed to write to socket for sending events

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_EVENT_FWD_SSL_CREATE_FAILED

Description: Event Forwarder unable to create new SSL context structure for TLS based forwarding

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_EVENT_FWD_SSL_SESSION_BUILD_FAILED

Description: Event Forwarder unable to build SSL session for TLS based forwarding

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_FWD_UNEXPECTED_FILE_REMOVED

Description: Event Forwarder removed unexpected event file (mismatched name format)

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_PKG_ATTR_NOT_FOUND

Description: Event Packager cannot find Worker name in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_EMPTY_FILE_REMOVED

Description: Event Packager found an empty event file - filw will be removed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_PKG_FILE_ADD_TO_SVN_FAILED

Description: Event Packager failed to add configuration file to svn upload queue

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_PKG_FILE_REMOVED_ERROR

Description: Event Packager failed to remove event file after upload

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_PKG_FILE_RENAME_FAILED

Description: Event Packager failed to rename configuration file after scanning

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
exitValue	Command exit value	int32	

EventType: PH_EVENT_PKG_FILE_STAT_FAILED

Description: Event Packager failed to stat configuration or event file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_EVENT_PKG_FILE_UPLOAD_FAILED

Description: Event Packager failed to upload event file to Worker or Super; will retry

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
serverIpAddr	Server IP	IP	

EventType: PH_EVENT_PKG_FILE_UPLOAD_SUCCESS_HIGH

Description: Event file upload success is high

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ratio	Ratio	double	

EventType: PH_EVENT_PKG_FILE_UPLOAD_SUCCESS_LOW

Description: Event file upload success is low

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ratio	Ratio	double	

EventType: PH_EVENT_PKG_GZ_CLOSE_FAILED

Description: Event Packager failed to close event file after writing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_EVENT_PKG_GZ_FILE_OPEN_ERROR

Description: Event Packager failed to open gz file or not enough memory to open it

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVENT_PKG_HTTP_FAILED

Description: Event Packager encountered HTTPS error response code

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_EVENT_PKG_HTTP_INIT_FAILED

Description: Event Packager HTTP client initialization failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_EVENT_PKG_INSERT_TASK_FAILED

Description: Failed to insert task into event file upload queue

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_NO_EVENT

Description: Event Packager did not upload any event in last 10 minutes

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_OPEN_DIR_FAILED

Description: Failed to open directory

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_EVENT_PKG_PROCESS_INIT_FAILED

Description: Event Packager failed to initialize

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_PROCESS_START_FAILED

Description: Event Packager failed to run

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_QUEUE_GET_FAILED

Description: Event Packager failed to get event file from the queue

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_EVENT_PKG_SERVER_LIST_UPLOAD_FAILED

Description: Event Packager failed to get upload server list from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_EVENT_PKG_SERVICE_LIST_EMPTY

Description: Empty upload service list

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_TASK_ADD_TO_QUEUE_FAILED

Description: Event Packager failed to add file upload task to queue

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVENT_PKG_XML_PARSE_FAILED

Description: Event Packager failed to parse XML from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVTPKGGER_FILE_UPLOAD_FAILED

Description: File upload failed

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_EVT_HANDLER_DBG

Description: Event handler debug message

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_ERR

Description: Event handler error message

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_EVT_QUEUE_LARGE

Description: Uploaded event files on Worker has a size of more than 100MB

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_EVT_QUEUE_WARNING

Description: Worker Input Event Queue large

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_INFO

Description: Event handler information

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_SVN_QUEUE_LARGE

Description: Uploaded SVN files size large

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVT_HANDLER_SVN_QUEUE_WARNING

Description: Worker Input Event Queue large

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_EVT_PACKAGER_COND_WAIT_ERROR

Description: FortiSIEM Event Packager Conditional Wait Error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_EVT_PACKAGER_FILE_CLOSE_FAILURE

Description: FortiSIEM Event Packager file close error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_EVT_PACKAGER_FILE_OPEN_FAILURE

Description: FortiSIEM Event Packager file open error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_EVT_PACKAGER_FILE_REMOVE_FAILURE

Description: FortiSIEM Event Packager file remove error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_EVT_PACKAGER_FILE_RENAME_FAILURE

Description: FortiSIEM Event Packager file rename error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	

EventType: PH_EVT_PACKAGER_FILE_STAT_FAILURE

Description: FortiSIEM Event Packager file stat error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_EVT_PACKAGER_FILE_UPLOAD_FAILURE

Description: FortiSIEM Event Packager file upload failure

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_EVT_PACKAGER_HTTP_RESPONSE_ERROR

Description: FortiSIEM Event Packager http response error from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_EVT_PACKAGER_INIT_FAILURE

Description: FortiSIEM Event Packager module initialization error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_EVT_PACKAGER_REST_PARSE_ERROR

Description: FortiSIEM Event Packager module failed to parse REST output

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_EVT_PACKAGER_RUN_PROCESS_ERROR

Description: FortiSIEM Event Packager module encountered error to run process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_FAILED_TO_EXEC

Description: Failed to execute specified command

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_FILE_NOT_FOUND

Description: Can not find the specified file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GCS_BUCKET_ACCESS_FAILURE

Description: Failed to access GCS Bucket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GENERIC_CRITICAL

Description: PH system generic critical message

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_GENERIC_DEBUG

Description: PH system generic debug message

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_GENERIC_ERROR

Description: PH system generic error

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GENERIC_INFO

Description: PH system generic info

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_GENERIC_WARNING

Description: PH system generic warning

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GET_CURL_HANDLE_FAILED

Description: FortiSIEM HTTP Client failed to get handle

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GET_SUPER_LEADER_FAILURE

Description: Failed to get super leader IP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GRPC_CERT_CREATE_SUCCESS

Description: Create gRPC certificate files

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_GRPC_CERT_ERROR

Description: 700-Grpc: Grpc cert error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_GRPC_CERT_LOADED_FAILED

Description: Failed to load certs file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_GRP_CERT_UPDATE_FAILED

Description: Failed to update gRPC certificate file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_GRP_CERT_UPDATE_SUCCESS

Description: Updated gRPC certificate file

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_GRP_FORMAT_JSON_FAILED

Description: Failed to format Json response

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_GRP_INIT_SSL_CONTEXT

Description: Failed to initial ACE_SSL_Context

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_GRPCTASK_DATA_EMPTY

Description: GRPC task is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HDFS_ARCHIVE_STORAGE_LOW

Description: The available storage of HDFS Archive database is low

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_HDFS_ARCHIVE_STORAGE_USAGE

Description: Storage usage of HDFS Archive database

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totalDiskMB	Total Disk MB	uint32	
freeDiskMB	Free Disk MB	uint32	

EventType: PH_HDFS_PURGING_FAILED

Description: Failed purging from HDFS Archive database

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_HDFS_PURGING_FINISHED

Description: Finished purging from HDFS Archive database - triggered by low space

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_HDFS_PURGING_STARTED

Description: Started purging from HDFS Archive database - triggered by low space

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_HDFS_PURGING_SUCCESS

Description: Successfully purged from HDFS Archive database - triggered by low space

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_HTTP_CLIENT_COMPRESS_FAILED

Description: FortiSIEM HTTP Client failed to compress payload

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_HTTP_CLIENT_CURL_ERROR

Description: FortiSIEM HTTP Client failed with curl error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event

EventType: PH_HTTP_CLIENT_GET_CACHE_FROM_MONITOR_FAILED

Description: FortiSIEM HTTP Client failed to get cache

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_HTTP_CLIENT_GET_DATA_FROM_CACHE_FAILED

Description: FortiSIEM HTTP Client failed to get data from cache

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_HTTP_CLIENT_GET_INIT_RESPONSE_FAILED

Description: FortiSIEM HTTP Client failed to get initialization response

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_HTTP_CLIENT_GET_INIT_RESPONSE_WARNING

Description: FortiSIEM HTTP Client encountered error getting initialization response

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_HTTP_CLIENT_GET_RESPONSE_WARNING

Description: FortiSIEM HTTP Client encountered error getting response

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event

EventType: PH_HTTP_CLIENT_HOST_IS_NULL

Description: FortiSIEM HTTP Client host is null error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_INIT_FAILURE

Description: FortiSIEM HTTP Client initialization failure

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_HTTP_CLIENT_INIT_WARNING

Description: FortiSIEM HTTP Client initialization warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_INVALID_FILE_SIZE

Description: FortiSIEM HTTP Client encountered invalid file size

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_MKSTEMP_FAILED

Description: FortiSIEM HTTP Client failed to mkstemp

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_HTTP_CLIENT_NO_FILE_PARAM

Description: FortiSIEM HTTP Client missing file parameter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_PICK_SUPER_FAILED

Description: FortiSIEM HTTP Client failed to pick super

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_PREP_REQUEST_ERROR

Description: FortiSIEM HTTP Client Prep Request error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_HTTP_CLIENT_PUT_REDIRECT_FAILURE

Description: FortiSIEM HTTP Client PUT Redirect error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_HTTP_CLIENT_SETOPT_FAILED

Description: FortiSIEM HTTP Client setopt call failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_HTTP_CLIENT_SET_HOST_WARNING

Description: FortiSIEM HTTP Client set host call failed

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_HTTP_CLIENT_UPLOAD_FILE_FAILED

Description: FortiSIEM HTTP Client file upload failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	
infoURL	Informational URL	string	This field captures an URL if present in an event
httpStatusCode	HTTP Status	string	
errorNoInt	Error Number Int	int32	

EventType: PH_HTTP_CLIENT_WRITE_CACHE_NULL

Description: FortiSIEM HTTP Client cache write error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_INIT_FAILURE

Description: Http client initialization failure

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_HTTP_RESPONSE_FAILURE

Description: HTTP response code failure

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_IDENTITYMASTER_HTTP_UPLOAD_ERROR

Description: Identity Master failed to upload identity location information to App server

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_IDENTITYMASTER_INIT_ERROR

Description: Identity Master initialization error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_IDENTITYWORKER_ATTRIB_ERROR

Description: Identity Worker found invalid event attribute in identityDef.xml

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_IDENTITYWORKER_EVT_LOAD_ERROR

Description: Identity Worker failed to load event from shared store

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_IDENTITYWORKER_EVT_SEND_ERROR

Description: Identity Worker failed to send event to Identity Master

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
sentBytes64	Sent Bytes64	uint64	Number of bytes sent by a host. This has 64bit resolution.

EventType: PH_IDENTITYWORKER_INIT_ERROR

Description: Identity Worker initialization error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_IDENTITYWORKER_PARAM_ERROR

Description: Identity Worker configuration parameter undefined in phoenix_config.txt

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_IDENTITYWORKER_PROCESSING_EPS

Description: IP Identity Worker EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_IDENTITYWORKER_SS_OBTAIN_ERROR

Description: Identity Worker failed to create shared store

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_INCIDENT_ACTION_STATUS

Description: Record action result for incident notification

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
scriptOutput	Script Output	string	

EventType: PH_INVALID_IP_ADDR

Description: FortiSIEM backend module detected invalid IP address

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_INVALID_PARAM

Description: Invalid Parameter

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
paraName	Param Name	string	

EventType: PH_INVALID_PARAM_CNT

Description: Invalid number of parameter

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_INVALID_PARAM_VAL_EMPTY

Description: Invalid empty parameter value

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
paraName	Param Name	string	

EventType: PH_JAVA_AGENT_APPSERVER_CONN_ERROR

Description: FSM FSM Java Agent failed to connect to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_APPSERVER_EXECUTE_ERROR

Description: FSM FSM Java Agent app server JMX Pull SQL Error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CONTROLLER_CMD_PARSE_ERROR

Description: FSM Java Agent parse file failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CONTROLLER_CMD_READ_ERROR

Description: FSM Java Agent control channel problem, exiting ...

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CONTROLLER_GENERIC_ERROR

Description: FSM Java Agent parse file failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CONTROLLER_LINE_READ_ERROR

Description: FSM Java Agent hit exception while reading line type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CONTROLLER_XML_READ_ERROR

Description: FSM Java Agent hit exception while reading command XML from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CUSTOM_JDBC_CONN_ERROR

Description: FSM Java Agent failed to execute custom JDBC monitoring job - connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_CUSTOM_JDBC_EXEC_ERROR

Description: FSM Java Agent failed to execute custom JDBC monitoring job - execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_DISCOVERY_TEST_ERROR

Description: FSM Java Agent failed to connect to Snort database for testing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ERROR

Description: PH java agent generic error

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_GLASSFISH_MONITOR_ERROR

Description: FSM Java Agent GlassFish monitoring failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_GLASS_FISH_WARNING

Description: FSM Java Agent GlassFish monitoring warning

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_GOOGLEAPPS_EXEC_ERROR

Description: FSM Java Agent Google Apps Monitor Exception

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_IBMDB2_AUDIT_CONN_ERROR

Description: FSM Java Agent IBM DB2 connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_IBMDB2_AUDIT_EXEC_ERROR

Description: FSM Java Agent IBM DB2 audit error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_IBM_DB2_CAT_READ_ERROR

Description: FSM Java Agent IBM loading error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_IBM_DB2_CONN_ERROR

Description: FSM Java Agent failed to connect to IBM DB2 for collecting audit logs

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_IBM_DB2_INTERNAL_ERROR

Description: FSM Java Agent IBM Sleep Interrupted error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_INFO

Description: PH java agent generic info

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JBOSS_CONN_ERROR

Description: FSM Java Agent app server connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JBOSS_EXEC_ERROR

Description: FSM Java Agent app server connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JBOSS_MONITOR_ERROR

Description: Fail to monitor Jboss

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JDBC_PULL_UNSUPP_ERROR

Description: No connection for job when pulling JDBC

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JDBC_SQL_NOT_SUPPORT_ERROR

Description: FSM Java Agent cannot support such a SQL

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JMX_CONN_ERROR

Description: FSM Java Agent jmx JDBC error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JMX_EXEC_ERROR

Description: FSM Java Agent JMX monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JOB_EXECUTOR_ERROR

Description: Exception in AgentJobExecutor.run error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JOB_STATUS_UPLOAD_ERROR

Description: Failed to upload job status xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JOB_TYPE_ERROR

Description: AgentUtils createAndInitAgent serverType is not defined

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JOB_XML_LOAD_ERROR

Description: Exception caught while parsing JobXml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_JOB_XML_PARSE_ERROR

Description: Exception caught while parsing JobXml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MCAFEE_MYSQL_MONITOR_ERROR

Description: FSM Java Agent my sql performance monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MCAFEE_VULN_SCANNER_ERROR

Description: FSM Java Agent vulnerability pulling error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MONITOR_GEN_ERROR

Description: FSM Java Agent job monitor rest error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MONITOR_TIMEOUT_ERROR

Description: FSM Java Agent job monitor execute too long

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MSSQL_DDL_CONN_ERROR

Description: FSM Java Agent JDBC pull don't support dev error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MSSQL_LOGON_CONN_ERROR

Description: FSM Java Agent MySql Connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MSSQL_LOGON_EXEC_ERROR

Description: FSM Java Agent app server JMX Pull SQL Error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MSSQL_MONITOR_ERROR

Description: FSM Java Agent ms sql performance error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MSSQL_PERF_CONN_ERROR

Description: FSM Java Agent job connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MSSQL_PERF_EXECUTE_ERROR

Description: FSM Java Agent MSSQL job execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MYSQL_PERF_CONN_ERROR

Description: FSM Java Agent MYSQL connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_MYSQL_PERF_EXEC_ERROR

Description: FSM Java Agent mysql audit performance error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_NESSUS_REPORT_PARSE_ERROR

Description: FSM Java Agent nessus report parse error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ORACLE_DB_ERROR

Description: FSM Java Agent Oracle DB performance metrics error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ORADB_AUDIT_CONN_ERROR

Description: FSM Java Agent Oracle DB connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ORADB_AUDIT_EXEC_ERROR

Description: FSM Java Agent Oracle DB execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ORADB_LOGON_EXEC_ERROR

Description: FSM Java Agent Oracle Audit trail pull error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ORADB_PERF_CONN_ERROR

Description: FSM Java Agent Oracle Database performance metrics collection error - connection issue

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_ORADB_PERF_EXEC_ERROR

Description: FSM Java Agent Oracle Database performance metrics collection error - SQL exec error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_SNORT_CONN_ERROR

Description: FSM Java Agent Snort IPS connect error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_SNORT_EVENTID_ERROR

Description: FSM Java Agent Snort IPS alert collection error - exception in setMaxEventId function

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_SNORT_EXEC_ERROR

Description: FSM Java Agent Snort IPS alert collection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_SNORT_SENSORID_ERROR

Description: FSM Java Agent Snort IPS alert collection error - exception in setSensorId2MaxEventId function

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_SNORT_TCP_OPTION_ERROR

Description: FSM Java Agent Snort IPS alert collection error - exception in getTcpOptions functions

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_TOMCAT_MONITOR_ERROR

Description: FSM Java Agent Tomcat Application Server monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_UTILS_ERROR

Description: FSM Java Agent status file error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_HWSTATUS_EXEC_ERROR

Description: FSM Java Agent failed to collect VMWare ESX hardware status

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_LOG_CONN_ERROR

Description: FSM Java Agent failed to connect VMWare ESX / Vcenter for collecting logs

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_LOG_EXEC_ERROR

Description: FSM Java Agent hit an exception while collecting logs from VMWare ESX / Vcenter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_MONITOR_ERROR

Description: FSM Java Agent hit an error while connecting to VMWare ESX / Vcenter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_COUNTER_MISSING

Description: FSM Java Agent VMWare performance pull error - missing performance counter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_DATA_RETRIEVE_ERROR

Description: FSM Java Agent VMWare performance pull error - data retrieve error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_ENTITY_MISSING

Description: FSM Java Agent VMWare performance pull error - missing performance entity

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_HOST_MISSING

Description: FSM Java Agent VMWare performance pull error - missing host

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_MON_EXCEPTION

Description: FSM Java Agent VMWare performance pull error - hit exception

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_ROLLUP_MISSING

Description: FSM Java Agent VMWare performance pull error - missing rollup

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_STAT_NAME_MISSING

Description: FSM Java Agent VMWare performance pull error - missing stat name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_PERF_VM_MISSING

Description: FSM Java Agent VMWare performance pull error - missing VM

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VMWARE_THREAD_EXEC_ERROR

Description: FSM Java Agent VMWare performance pull error - thread execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VULN_REPORT_PARSER_ERROR

Description: FSM Java Agent failed to parse external vulnerability scanner report

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_VULN_REPORT_VERIFY_ERROR

Description: FSM Java Agent failed to verify external vulnerability scanner report

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBLOGIC_MONITOR_ERROR

Description: FSM Java Agent Weblogic monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSENSE_EMAIL_MISSING_LOGDB

Description: FSM Java Agent Websense Email Gateway log collection error - logDBName is null

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSENSE_JDBC_PULL_ERROR

Description: FSM Java Agent Websense WebSecurity Gateway log collection error - Event Pull SQL Error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSENSE_MAIL_CONN_ERROR

Description: FSM Java Agent Websense Email Gateway connection audit error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSENSE_MAIL_EXEC_ERROR

Description: FSM Java Agent Websense Email Gateway execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

All Logs Page 4

Every FortiSIEM internally generated event log regardless of category

- PH_JAVA_AGENT_WEBSSENSE_MAIL_PULL_ERROR
- PH_JAVA_AGENT_WEBSSENSE_WEB_CONN_ERROR
- PH_JAVA_AGENT_WEBSSENSE_WEB_EXEC_ERROR
- PH_JAVA_AGENT_WEBSSENSE_WEB_MISSING_LOGDB
- PH_JAVA_AGENT_WEBSPHERE_CONN_ERROR
- PH_JAVA_AGENT_WEBSPHERE_EXEC_ERROR
- PH_JAVA_AGENT_WEBSPHERE_MONITOR_ERROR
- PH_JAVA_QUERYSERVER_ACTION_UNSUPPORTED_ERROR
- PH_JAVA_QUERYSERVER_ELASTIC_ERROR
- PH_JAVA_QUERYSERVER_ERROR
- PH_JAVA_QUERYSERVER_INFO
- PH_JAVA_QUERYSERVER_QUERYID_ERROR
- PH_JAVA_QUERYSERVER_QUERY_SYNTAX_ERROR
- PH_JAVA_QUERYSERVER_REDIS_ERROR
- PH_JAVA_QUERYSERVER_WARN
- PH_JMS_QUEUE_SIZE_WARNING
- PH_JOB_STAT
- PH_JOB_STATUS_XML_SEND_ERROR
- PH_JOB_STATUS_XML_SENT
- PH_JOB_STAT_SUPPRESSED
- PH_LIBEVENT_BUFFER_OVERFLOW
- PH_LIBEVENT_IP_TYPE_INVALID
- PH_LIBEVENT_UNKNOWN_ATTR_ID
- PH_LIBEVENT_UNKNOWN_ATTR_NAME
- PH_LIB_TOPO_APACHE_PING_FAILED
- PH_LIB_TOPO_APP_GROUP_FILTER_PARSE_ERROR
- PH_LIB_TOPO_APP_GROUP_FILTER_PUSH_ERROR
- PH_LIB_TOPO_AWS_NEW_INSTANCE_NOT_RUN
- PH_LIB_TOPO_AWS_OBTAIN_INSTANCE_FAILURE
- PH_LIB_TOPO_CHECK_APP_LIST_WARNING
- PH_LIB_TOPO_CISCO_IOS_CBQOS_ERROR
- PH_LIB_TOPO_CISCO_MERAKI_GET_CHILD_DEVICE_WARNING
- PH_LIB_TOPO_CISCO_MERAKI_GET_INTFS_WARNING
- PH_LIB_TOPO_CISCO_MERAKI_GET_INTF_WARNING
- PH_LIB_TOPO_CISCO_MERAKI_MAC_2_HOST_LOOKUP_FAILED
- PH_LIB_TOPO_CISCO_MERAKI_MAC_2_INTF_LOOKUP_FAILED
- PH_LIB_TOPO_CISCO_UCS_LOGIN_FAILED

- PH_LIB_TOPO_CISCO_UCS_REQUEST_ERROR
- PH_LIB_TOPO_CPU_TOO_HIGH
- PH_LIB_TOPO_CUST_CONFIG_JOB_DOWNLOAD_SCRIPT_FAILED
- PH_LIB_TOPO_CUST_FIM_JOB_CHECK_PATH_ERROR
- PH_LIB_TOPO_CUST_FIM_JOB_DEVICE_UNAVAILABLE
- PH_LIB_TOPO_CUST_FIM_JOB_FILE_TOO_LARGE
- PH_LIB_TOPO_CUST_FIM_JOB_GET_DATA_FAILED
- PH_LIB_TOPO_CUST_FIM_JOB_GET_FILE_INFO_FAILED
- PH_LIB_TOPO_CUST_FIM_JOB_GET_MD5_FAILED
- PH_LIB_TOPO_CUST_FIM_JOB_GET_REMOTE_FILE_ERROR
- PH_LIB_TOPO_CUST_FIM_JOB_INCORRECT_CRED
- PH_LIB_TOPO_CUST_FIM_JOB_RUN_SCP_FAILED
- PH_LIB_TOPO_CUST_FIM_JOB_TOO_MANY_FILES
- PH_LIB_TOPO_CUST_LOGIN_JOB_CREATE_EVENT_FAILED
- PH_LIB_TOPO_CUST_LOGIN_JOB_GET_DATA_FAILED
- PH_LIB_TOPO_CUST_SNMP_JOB_CREATE_EVENT_FAILED
- PH_LIB_TOPO_CUST_SNMP_JOB_GET_DATA_FAILED
- PH_LIB_TOPO_CUST_WMI_JOB_CREATE_EVENT_FAILED
- PH_LIB_TOPO_CUST_WMI_JOB_GET_DATA_FAILED
- PH_LIB_TOPO_ETHERMIB_STAT_LOOKUP_ERROR
- PH_LIB_TOPO_EVENT_DROP_RULE_ENCODE_VALUE_GROUP_ERROR
- PH_LIB_TOPO_EVENT_DROP_RULE_PARSE_ERROR
- PH_LIB_TOPO_EXCLUDED_DISK_PARSE_ERROR
- PH_LIB_TOPO_FCT_DEV_MAPPING_ENTRY_INVALID
- PH_LIB_TOPO_FGT_FABRIC_DISCOV_FAIL
- PH_LIB_TOPO_FGT_GET_CONFIG_BACKUP_FAILED
- PH_LIB_TOPO_FGT_GET_USER_DEV_STORE_FAIL
- PH_LIB_TOPO_FGT_GET_USER_DEV_UNKNOWN
- PH_LIB_TOPO_FGT_INSTALLED_SW_FAIL
- PH_LIB_TOPO_FGT_SEC_POSTURE_RPT_API_FAIL
- PH_LIB_TOPO_FILE_READ_ERROR
- PH_LIB_TOPO_FOUNDRY_HW_STATUS_ERROR
- PH_LIB_TOPO_GEN_UPS_STATUS_GET_ERROR
- PH_LIB_TOPO_GET_NETAPP_NFS_FAILED
- PH_LIB_TOPO_H3C_CPU_UTIL_ERROR
- PH_LIB_TOPO_HP3COM_CPU_UTIL_ERROR
- PH_LIB_TOPO_HP3COM_MEM_UTIL_ERROR
- PH_LIB_TOPO_HPUX_PROC_CPU_MEM_TOO_HIGH
- PH_LIB_TOPO_HYPERV_METRICS_GET_ERROR
- PH_LIB_TOPO_IMPORTANT_INTF_PARSE_ERROR
- PH_LIB_TOPO_INTF_UTIL_ERROR
- PH_LIB_TOPO_JSON_PARSE_FAILED
- PH_LIB_TOPO_JUNIPER_INTF_SPEED_GET_ERROR

- PH_LIB_TOPO_LIEBERT_HVAC_STATUS_GET_ERROR
- PH_LIB_TOPO_LOGIN_PING_FAILED
- PH_LIB_TOPO_MAINTENANCE_DURATION_INCORRECT
- PH_LIB_TOPO_MEM_TOO_HIGH
- PH_LIB_TOPO_NETAPP_AGGREGATE_STAT_ERROR
- PH_LIB_TOPO_NETAPP_ANALYZE_VERSION_ERROR
- PH_LIB_TOPO_NETAPP_DISK_STAT_ERROR
- PH_LIB_TOPO_NETAPP_GET_NFS_METRIC_ERROR
- PH_LIB_TOPO_NETAPP_GET_VERSION_ERROR
- PH_LIB_TOPO_NETAPP_LUN_STAT_ERROR
- PH_LIB_TOPO_NETAPP_PROTO_STAT_ERROR
- PH_LIB_TOPO_NETAPP_VOLUME_STAT_ERROR
- PH_LIB_TOPO_NOT_SUPPORT_REST_API
- PH_LIB_TOPO_OPEN_FILE_FAILED
- PH_LIB_TOPO_PARSE_INTF_MAP_FAILURE
- PH_LIB_TOPO_PERF_JOB_EXEC_FAILED
- PH_LIB_TOPO_PERF_JOB_INIT_FAILED
- PH_LIB_TOPO_PERF_JOB_REMOVE_FAILED
- PH_LIB_TOPO_PERF_TEMPLATE_LOAD_ERROR
- PH_LIB_TOPO_PERF_TEMPLATE_PARSE_FAILURE
- PH_LIB_TOPO_PERF_TEMPLATE_PARSE_WARNING
- PH_LIB_TOPO_PORT_FILTER_PARSE_ERROR
- PH_LIB_TOPO_PORT_FILTER_PUSH_ERROR
- PH_LIB_TOPO_PROC_CPU_MEM_TOO_HIGH
- PH_LIB_TOPO_REST_API_FAILED
- PH_LIB_TOPO_RUN_SW_FILTER_PARSE_ERROR
- PH_LIB_TOPO_RUN_SW_FILTER_PUSH_ERROR
- PH_LIB_TOPO_SNMPWALK_ERROR
- PH_LIB_TOPO_STM_JOB_EXEC_FAILED
- PH_LIB_TOPO_STM_JOB_INIT_FAILED
- PH_LIB_TOPO_TEST_CONN_HTTP_AGENT_FAILED
- PH_LIB_TOPO_TEST_CONN_JDBC_AGENT_FAILED
- PH_LIB_TOPO_TEST_CONN_JMX_AGENT_FAILED
- PH_LIB_TOPO_TRUNK_PORT_MAP_PARSE_ERROR
- PH_LIB_TOPO_VALIDATE_ACCESS_FAILED
- PH_LIB_TOPO_WIN_GET_EXCH_DATABASE_INSTANCE_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_DATABASE_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_MAIL_SUBMISSION_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_PUB_MAILBOX_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_REG_MAILBOX_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_REPLICATION_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_RPC_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_SMTP_WARNING

- PH_LIB_TOPO_WIN_GET_EXCH_STORE_INTF_WARNING
- PH_LIB_TOPO_WIN_GET_EXCH_TRANSPORT_QUEUE_WARNING
- PH_LIB_TOPO_WMI_GET_CPU_COUNT_ERROR
- PH_LIB_TOPO_WMI_GET_CPU_WARNING
- PH_LIB_TOPO_WMI_GET_PAGE_ACTIVITY_ERROR
- PH_LIB_TOPO_WMI_GET_REAL_MEM_ERROR
- PH_LIB_TOPO_WMI_GET_RUN_SW_PERF_ERROR
- PH_LICENSE_ERROR
- PH_LICENSE_INFO_FAILURE
- PH_LICENSE_INFO_INVALIDATED
- PH_LICENSE_NOT_EXIST
- PH_LINUX_AGENT_ACCOUT_MISSING
- PH_LINUX_AGENT_BIND_PORT_FAILED
- PH_LINUX_AGENT_CONFIG_ATTR_DECRYPTED_FAILED
- PH_LINUX_AGENT_CONFIG_ATTR_ENCRYPTED_FAILED
- PH_LINUX_AGENT_CONFIG_ATTR_NOT_FOUND
- PH_LINUX_AGENT_CONFIG_MISS_ATTR
- PH_LINUX_AGENT_CREATE_SOCKET_FAILED
- PH_LINUX_AGENT_EXIT
- PH_LINUX_AGENT_HOST_IP_GOT_FAILED
- PH_LINUX_AGENT_INCREASE_RECV_SOCK_BUF_MAX_FAILED
- PH_LINUX_AGENT_INIT_FIM_FAILED
- PH_LINUX_AGENT_INIT_HTTP_FAILED
- PH_LINUX_AGENT_LOG_GENERIC
- PH_LINUX_AGENT_NEW_FIM_LOADED
- PH_LINUX_AGENT_OPEN_FILE_FAILED
- PH_LINUX_AGENT_OPEN_PORT_FAILED
- PH_LINUX_AGENT_PWD_MISSING
- PH_LINUX_AGENT_RECV_ERROR
- PH_LINUX_AGENT_REGISSTER_FAILED
- PH_LINUX_AGENT_TEMPLATE_STATUS
- PH_LINUX_AGENT_UNINSTALL
- PH_LINUX_AGENT_UPLOAD_FILE_FAILED
- PH_LINUX_AGENT_UPLOAD_FILE_SUCCESS
- PH_LINUX_AGENT_USER_FILE_LOG_GENERIC
- PH_LINUX_AGENT_VERIFIER_ERROR
- PH_LOAD_CONFIG_CHANGE_FAILED
- PH_LOOKUP_TABLE_CANNOT_LOAD_DATA
- PH_MAX_DEVICES_EXCEEDED
- PH_MAX_DEVICES_LIMIT_REACHED
- PH_ML_ANOMALY_DETECTED
- PH_MODULE_ABORT
- PH_MODULE_ABORT_FOUND

- PH_MODULE_ACCEPTED_CONN
- PH_MODULE_ACE_ACCEPTOR_FAILED
- PH_MODULE_ACE_HANDLE_EVENT_ERROR
- PH_MODULE_COMM_ERROR
- PH_MODULE_COMM_HANDLER_REG
- PH_MODULE_COMM_PORTS_OPENED
- PH_MODULE_DB_CONFIG_LOADED
- PH_MODULE_DIODE_CONFIG_ERROR
- PH_MODULE_EXCEPTION_NOT_CAUGHT
- PH_MODULE_EXITING
- PH_MODULE_EXIT_OK
- PH_MODULE_HEARTBEAT_INIT
- PH_MODULE_INITIALIZING
- PH_MODULE_INIT_COMPLETE
- PH_MODULE_INIT_FAILURE
- PH_MODULE_LICENSE_FAILURE
- PH_MODULE_LOADED_NEW_CONFIG
- PH_MODULE_LOAD_DIODE_CRED_ERROR
- PH_MODULE_LOCAL_CONFIG_LOADED
- PH_MODULE_LOCAL_CONFIG_SECTION_ERROR
- PH_MODULE_LOCAL_CONFIG_VALUE_ERROR
- PH_MODULE_LOG_LEVEL_CHANGE
- PH_MODULE_RECVD_EXIT_EXT
- PH_MODULE_RECVD_EXIT_MONITOR
- PH_MODULE_RECVD_NEW_CONFIG
- PH_MODULE_RECVD_START
- PH_MODULE_SETPIDFILE_ERR
- PH_MODULE_UNABLE_INIT_SHARED_STORE
- PH_MODULE_UNABLE_OPEN_COMM_PORT
- PH_MONITOR_ARCHIVE_GET_WORKER_FAILURE
- PH_MONITOR_ARCHIVE_UPDATE_WORKER_FAILURE
- PH_MONITOR_BEACONING_REGISTER_FAILURE
- PH_MONITOR_CHECK_DEPENDENCY_FAILED
- PH_MONITOR_CMD_FAILURE
- PH_MONITOR_CMD_SEND_FAILURE
- PH_MONITOR_COLLECTOR_REGISTER_FAILURE
- PH_MONITOR_COLLECTOR_UPDATE_STATUS_FAILURE
- PH_MONITOR_CONFIG_DOWNLOAD_FAILURE
- PH_MONITOR_DBCLUSTER_SEND_COMMAND_FAILED
- PH_MONITOR_DELETE_DR_FAILED
- PH_MONITOR_DELETE_SECONDARY_ON_WORKER_FAILED
- PH_MONITOR_DELETE_SUPER_FOLLOWER_FAILED
- PH_MONITOR_DISPATCH_CMD_MISMATCH

- PH_MONITOR_DOMAIN_CHANGE_XML_PARSE_FAILURE
- PH_MONITOR_ENT_OR_SP_MODE_MISSING
- PH_MONITOR_EXCESSIVE_DB_LOGIN_FAILURE
- PH_MONITOR_FAILED_CONN_QUERYMASTER
- PH_MONITOR_FILE_IO_ERROR
- PH_MONITOR_FILE_PERMISSION_ERROR
- PH_MONITOR_FILE_PERMISSION_WARNING
- PH_MONITOR_FLIP_PRIMARY_FAILURE
- PH_MONITOR_FSM_AGENT_UPDATE_PWD_ERROR
- PH_MONITOR_GET_REPLICATION_PROGRESS_FAILED
- PH_MONITOR_GET_UPTIME_ERROR
- PH_MONITOR_HANDLE_TASK
- PH_MONITOR_HARDWARE_SN_FORK_FAILURE
- PH_MONITOR_HOST_UUID_READ_FAILURE
- PH_MONITOR_HTTP_PULL_ERROR
- PH_MONITOR_INIT_PROC_MODULE_NOT_FOUND
- PH_MONITOR_INIT_SECONDARY_ON_WORKER_FAILED
- PH_MONITOR_INIT_SUPER_FOLLOWER_FAILED
- PH_MONITOR_INIT_SYSTEM_XML_PARSE_FAILURE
- PH_MONITOR_JDBC_POOL_NOT_EXIST
- PH_MONITOR_LIB_DEPENDENCY_WARNING
- PH_MONITOR_LICENSE_ERROR
- PH_MONITOR_LOAD_CONF_FROM_APP_SERVER_FAILED
- PH_MONITOR_LOCAL_HOSTNAME_GET_FAILURE
- PH_MONITOR_MEM_FILE_OPEN_FAILURE
- PH_MONITOR_MISSING_MONITOR
- PH_MONITOR_MMAP_FAILURE
- PH_MONITOR_MOTNIROR_REGISTER_FAILURE
- PH_MONITOR_NOTIFICATION_CLIENT_CONTACT_FAILURE
- PH_MONITOR_NOTIFICATION_CMD_EMPTY
- PH_MONITOR_NOTIFICATION_CMD_MISMATCH
- PH_MONITOR_NOTIFICATION_RETURN_FAILURE
- PH_MONITOR_PHOENIX_CONFIG_GLOBAL_MISSING
- PH_MONITOR_PHOENIX_CONFIG_INVALID
- PH_MONITOR_PROCESS_OWNER_NOT_ADMIN_ERROR
- PH_MONITOR_QUERY_LICENSE_FAILED
- PH_MONITOR_RECVD_CONFIG_CHANGE
- PH_MONITOR_RECVD_HEARTBEAT
- PH_MONITOR_REDIS_UPDATE_FAILED
- PH_MONITOR_REGISTER_MONITOR_GET_WORKER_FAILURE
- PH_MONITOR_REGISTER_NODE
- PH_MONITOR_REGISTER_SUPER_FOLLOWER
- PH_MONITOR_REGISTER_WORKER

- PH_MONITOR_REMOVE_NODE
- PH_MONITOR_REMOVE_SUPER_FOLLOWER
- PH_MONITOR_REMOVE_WORKER
- PH_MONITOR_REPORTSERVER_LICENSE_INVALID
- PH_MONITOR_REPORTSERVER_NOTIFICATION_CLIENT_CONTACT_FAILURE
- PH_MONITOR_REPORTSERVER_NOTIFICATION_CLIENT_INIT_FAILURE
- PH_MONITOR_REPORTSERVER_NOTIFICATION_SERVER_RETURN_FAILURE
- PH_MONITOR_RESET_DB_SERVER_NAME_FAILED
- PH_MONITOR_RESET_JDBC_CONN_FAILED
- PH_MONITOR_RESET_STORAGE_CONFIG_FAILED
- PH_MONITOR_RESTART_MODULES
- PH_MONITOR_REST_CACHE_REQUEST_EMPTY
- PH_MONITOR_REST_CACHE_REQUEST_FAILURE
- PH_MONITOR_REST_CACHE_REQUEST_FORMAT_ILLEGAL
- PH_MONITOR_REST_CACHE_SERVER_INIT_FAILURE
- PH_MONITOR_REST_CALL_FAILURE
- PH_MONITOR_ROLE_UNDEFINED
- PH_MONITOR_SAVE_DR_CONFIG_FAILED
- PH_MONITOR_SEND_CMD_TO_MODULE
- PH_MONITOR_SEND_VG_UPDATE_CMD_TO_MODULE
- PH_MONITOR_SETUID_FAILURE
- PH_MONITOR_START_MODULE
- PH_MONITOR_START_MODULES
- PH_MONITOR_STATFS_FAILURE
- PH_MONITOR_STATUS_PUSHER_SPAWN_FAILURE
- PH_MONITOR_STOP_MODULES
- PH_MONITOR_STOP_READER
- PH_MONITOR_STORAGE_ES_CUSTOMIZED_TEMPLATE_DEPLOYED
- PH_MONITOR_STORAGE_GET_WORKER_FAILURE
- PH_MONITOR_STORAGE_LOCAL_GET_FAILURE
- PH_MONITOR_STORAGE_NFS_GET_FAILURE
- PH_MONITOR_STORAGE_TYPE_GET_FAILURE
- PH_MONITOR_STORAGE_TYPE_UNKNOWN
- PH_MONITOR_STORAGE_UPDATE_WORKER_FAILURE
- PH_MONITOR_SVC_PASSWORD_DISTRIBUTION_ERROR
- PH_MONITOR_SYSINFO_FAILURE
- PH_MONITOR_SYSTEM_DB_LOGIN_ERROR
- PH_MONITOR_SYSTEM_HEALTH_CPU
- PH_MONITOR_SYSTEM_HEALTH_ISSUE
- PH_MONITOR_SYSTEM_HEALTH_MEM
- PH_MONITOR_SYSTEM_STATUS_SPAWN_FAILURE
- PH_MONITOR_THREAD_SPAWN_FAILED
- PH_MONITOR_TUNNEL_ERROR

- PH_MONITOR_UMOUNT_NFS_FAILURE
- PH_MONITOR_UNABLE_CONTACT_APPSVR
- PH_MONITOR_UPDATE_DATA_FAILED
- PH_MONITOR_UPDATE_DR_FAILED
- PH_MONITOR_UPDATE_WORKER_INFO_FAILED
- PH_MONITOR_UPLOAD_LOG_SPAWN_FAILURE
- PH_MONITOR_WINAGENT_DELETE_PWD_SPAWN_FAILURE
- PH_MONITOR_WINAGENT_UPDATE_PWD_ERROR
- PH_MONITOR_WIN_LINUX_AGENT_PWD_UPDATE_SUCCESS
- PH_MONITOR_WORKER_NODECONFIG_UPDATE_FAILED
- PH_MONITOR_WORKER_REDIS_ADDSLAVE_UPDATE_FAILED
- PH_MONITOR_WORKER_REDIS_CONF_UPDATE_FAILED
- PH_NETFLOW_BAD_FLOW
- PH_NETFLOW_BAD_FLOW_END
- PH_NETFLOW_BAD_HEADER_PROTOCOL
- PH_NETFLOW_BAD_PACKET
- PH_NETFLOW_BAD_RECORD
- PH_NETFLOW_BAD_TYPE
- PH_NETFLOW_BAD_VER
- PH_NETFLOW_EXCEPTION
- PH_NOTIFICATION_ACCEPT_FAILURE
- PH_NOTIFICATION_CALLBACK_ERROR
- PH_NOTIFICATION_CONN_FAILED
- PH_NOTIFICATION_INIT_FAILED
- PH_NOTIFICATION_NO_RESPONSE
- PH_NOTIFICATION_RETURN_FAILURE
- PH_NOTIFICATION_SEND_FAILURE
- PH_NOTIFICATION_SEND_FILE_FAILURE
- PH_NO_PARSER_FOR_EVENT
- PH_OBJECT_NOT_FOUND
- PH_PARSER_BIND_PORT_FAILURE
- PH_PARSER_DATA_SIZE_OVERFLOW
- PH_PARSER_DIR_OPEN_FAILURE
- PH_PARSER_EVENT_PARSER_ERROR
- PH_PARSER_EVENT_SERIALIZE_ERROR
- PH_PARSER_FILE_DELETE_FAILURE
- PH_PARSER_FILE_DELETE_FAILURE_RENAME
- PH_PARSER_FILE_INVALID_FORMAT
- PH_PARSER_FILE_INVALID_HEADER
- PH_PARSER_FILE_NOT_EXIST
- PH_PARSER_FILE_OPEN_FAILURE
- PH_PARSER_FILE_PARSE_FAILURE
- PH_PARSER_FILE_READ_FAILURE

- PH_PARSER_FILE_RENAME_FAILURE
- PH_PARSER_FILE_SIZE_MISMATCH
- PH_PARSER_FILE_STAT_FAILURE
- PH_PARSER_FILE_WRITE_FAILURE
- PH_PARSER_GEO_WRONG_ATTR_NUMBER
- PH_PARSER_GEO_WRONG_CACHE_NUMBER
- PH_PARSER_GET_PROCESS_ERROR
- PH_PARSER_GLOBAL_LICENSE_EXCEED
- PH_PARSER_HTTP_RESPONSE_ERROR
- PH_PARSER_HTTP_UPLOAD_FAILURE
- PH_PARSER_INIT_DEV_CRED_FAILED
- PH_PARSER_INIT_FAILURE
- PH_PARSER_INVALID_CSV
- PH_PARSER_INVALID_EXT_LOG_PROTO
- PH_PARSER_INVALID_ORG_NAME
- PH_PARSER_INVALID_PHOENIX_CONFIG
- PH_PARSER_IP_TYPE_INVALID
- PH_PARSER_JSON_PARSE_FAILURE
- PH_PARSER_MALLOC_FAILURE
- PH_PARSER_PACK_EVENT_ERROR
- PH_PARSER_RAWEVENT_TOO_LARGER
- PH_PARSER_REST_PARSE_ERROR
- PH_PARSER_RUN_PROCESS_ERROR
- PH_PARSER_SEND_EVENT_FAILURE
- PH_PARSER_SEND_TO_DISCOV_FAILURE
- PH_PARSER_SEND_TO_MONITOR_FAILURE
- PH_PARSER_SET_USER_ID_FAILURE
- PH_PARSER_SHARED_STORE_ERROR
- PH_PARSER_SNMPTRAP_INIT_FAILURE
- PH_PARSER_SOCKET_ERROR
- PH_PARSER_SOCKET_RECV_ERROR
- PH_PARSER_SOCKET_SELECT_ERROR
- PH_PARSER_SPAWN_THREAD_FAILURE
- PH_PARSER_SSL_ACCEPT_ERROR
- PH_PARSER_SSL_CERT_LOAD_ERROR
- PH_PARSER_TCP_SOCKET_ACCEPT_ERROR
- PH_PARSER_TEST_RULES_PARSE_ALL_EVENTS_BEGIN
- PH_PARSER_TEST_RULES_PARSE_ALL_EVENTS_END
- PH_PARSER_TEST_RULES_PARSE_ONE_EVENT_BEGIN
- PH_PARSER_TEST_RULES_PARSE_ONE_EVENT_END
- PH_PARSER_TOO_MANY_UNKNOWN_EVENTS
- PH_PARSER_UPDATE_FAILURE
- PH_PARSER_USE_ERROR_BEFORE_INIT

- PH_PARSER_WRONG_EVENT_SIZE
- PH_PARSER_WRONG_PARAMETER
- PH_PARSER_WTAP_ERR_BAD_FILE
- PH_PARSER_WTAP_ERR_CANT_OPEN
- PH_PARSER_WTAP_ERR_COMPRESSION_NOT_SUPPORTED
- PH_PARSER_WTAP_ERR_DECOMPRESS
- PH_PARSER_WTAP_ERR_ENCAP_PER_PACKET_UNSUPPORTED
- PH_PARSER_WTAP_ERR_FILE_UNKNOWN_FORMAT
- PH_PARSER_WTAP_ERR_NOT_REGULAR_FILE
- PH_PARSER_WTAP_ERR_RANDOM_OPEN_PIPE
- PH_PARSER_WTAP_ERR_SHORT_READ
- PH_PARSER_WTAP_ERR_SHORT_WRITE
- PH_PARSER_WTAP_ERR_UNSUPPORTED
- PH_PARSER_XML_PARSE_ERROR
- PH_PARSER_XML_PARSE_FAILURE
- PH_PARSE_CONFIG_CHANGE_FAILED
- PH_PDF_BUILDER_ERROR
- PH_PERFMON_COMMIT_FILE_FAILED
- PH_PERFMON_CONFIG_SEND_FAILED
- PH_PERFMON_CONFIG_VERSION_ERROR
- PH_PERFMON_CONFIG_VERSION_WARNING
- PH_PERFMON_CUST_JOB_ADD_FAILED
- PH_PERFMON_INIT_ERROR
- PH_PERFMON_INST_SW_MAP_EMPTY
- PH_PERFMON_INST_SW_NO_NAME
- PH_PERFMON_JOB_ADD_FAILED
- PH_PERFMON_MASS_PING_WARNING
- PH_PERFMON_MONITEE_BAD
- PH_PERFMON_MONITEE_NOT_FOUND
- PH_PERFMON_NO_DEV_TYPE
- PH_PERFMON_PERF_OBJ_PARSE_FAILURE
- PH_PERFMON_PING_RESULT_OPEN_FAILED
- PH_PERFMON_PROC_RUN_FAILED
- PH_PERFMON_REAL_TIME_JOB_RUN_FAILED
- PH_PERFMON_ROUTE_LOAD_ERROR
- PH_PERFMON_STATUS_REPORTER_INIT_FAILED
- PH_PERFMON_STATUS_REPORT_FAILED
- PH_PERFMON_SVN_CHECKOUT_FAILED
- PH_PERFMON_SVN_CONFIG_MISSING
- PH_PERFMON_SVN_DIR_CREATE_FAILED
- PH_PERFMON_SVN_DIR_UPDATE_FAILED
- PH_PERFMON_SVN_FILE_COPY_FAILED
- PH_PERFMON_SVN_FILE_EMPTY

- PH_PERFMON_SVN_FILE_MARK_FAILED
- PH_PERFMON_SVN_FILE_OPEN_FAILED
- PH_PERFMON_SVN_FILE_PARSE_FAILED
- PH_PERFMON_SVN_FILE_REMOVE_FAILED
- PH_PERFMON_SVN_FILE_RENAME_FAILED
- PH_PERFMON_SVN_FIM_FILE_MISSING
- PH_PERFMON_SVN_FIRSTFILELINES_EMPTY
- PH_PERFMON_SVN_FIRSTFILELINES_NOT_IN_FILE
- PH_PERFMON_SVN_GET_DEVICE_ID_FAILED
- PH_PERFMON_SVN_GET_DISCOV_TIME_FAILED
- PH_PERFMON_SVN_INFO_GET_FAILED
- PH_PERFMON_SVN_INST_SW_BAD
- PH_PERFMON_SVN_INVALID_FILE_FORMAT
- PH_PERFMON_SVN_INVALID_HEADER_IN_FILE
- PH_PERFMON_SVN_INVALID_SECONDFILENAME
- PH_PERFMON_SVN_LINE_MISMATCH
- PH_PERFMON_SVN_SECONDFILENAME_EMPTY
- PH_PERFMON_SVN_SOFTWARE_MISSING
- PH_PERFMON_TOPO_CONFIG_ERROR
- PH_PERFMON_TOPO_FILE_OPEN_FAILED
- PH_PERFMON_TOPO_LOAD_ERROR
- PH_PERFMON_TRACERT_FILE_OPEN_FAILED
- PH_PERFMON_UNKNOWN_CUST_PERF_JOB_ID
- PH_PERFMON_UNKNOWN_PERF_JOB_ID
- PH_PERFMON_UNKNOWN_PROBE_JOB_ID
- PH_PERFMON_UPDATE_CONFIG_ERROR
- PH_PERFMON_UPDATE_FILTERS_ERROR
- PH_PERFMON_UPDATE_ROUTE_DEPENDENCY_FAILED
- PH_PERFMON_USER_PWD_GET_FAILED
- PH_PERFORM_MONITOR_ERROR
- PH_PER_MON_CONFIG_ERROR
- PH_PER_MON_FETCH
- PH_PER_MON_FUNCTION
- PH_PER_MON_SNMP_DONE
- PH_PER_MON_WALK
- PH_PER_MON_WALK_ERROR
- PH_QUERYSRV_DUPLICATED_QUERYID
- PH_QUERYSRV_INVALID_QUERYXML
- PH_QUERY_AGGR_RESULTS_POST_PROCESS_FAILED
- PH_QUERY_ATTR_UNDEFINED
- PH_QUERY_BAD_RESULT_STATUS
- PH_QUERY_CACHE_GET_FAILED
- PH_QUERY_CACHE_RESULT_GET_FAILED

- PH_QUERY_CACHE_TRIGGER_EVENT_GET_FAILED
- PH_QUERY_CHAR_UNEXPECTED
- PH_QUERY_CH_PARSE_FAILED
- PH_QUERY_CH_POST_FAILED
- PH_QUERY_CLICKHOUSE_DATA_FAILED
- PH_QUERY_CLICKHOUSE_EXEC_FAILED
- PH_QUERY_CLICKHOUSE_STARTS
- PH_QUERY_CLICKHOUSE_STOP_FAILED
- PH_QUERY_CLICKHOUSE_WAITING_QUEUE_FULL
- PH_QUERY_COMMAND_BAD
- PH_QUERY_COMPLETION_NOTIFICATION_SEND_FAILED
- PH_QUERY_CONFIG_UNDEFINED
- PH_QUERY_CONVERT_FAILED
- PH_QUERY_DATA_ENUM_FAILED
- PH_QUERY_DATA_MANAGER_NODES_GET_FAILED
- PH_QUERY_DATA_SEND_FAILED
- PH_QUERY_DATA_SIZE_MISMATCH
- PH_QUERY_DATA_SIZE_UNEXPECTED
- PH_QUERY_DATA_TYPE_UNEXPECTED
- PH_QUERY_DB_SERVER_HOST_UNDEFINED
- PH_QUERY_DIR_CREATE_FAILED
- PH_QUERY_DIR_RENAME_FAILED
- PH_QUERY_DISTRIBUTION
- PH_QUERY_DURATION
- PH_QUERY_ES_PARSE_FAILED
- PH_QUERY_ES_POST_FAILED
- PH_QUERY_ES_SCROLL_FAILED
- PH_QUERY_EVENT_COLLECTOR_UNAVAILABLE
- PH_QUERY_EVENT_ID_GET_FAILED
- PH_QUERY_EVENT_PARSE_FAILED
- PH_QUERY_EVENT_PAYLOAD_READ_FAILED
- PH_QUERY_EXCEPTION_CAUGHT
- PH_QUERY_EXPORT_TASK_CREAT_FAILED
- PH_QUERY_EXPORT_TASK_INSERT_FAILED
- PH_QUERY_EXPR_INCOMPLETE
- PH_QUERY_FILE_CONTENT_BAD
- PH_QUERY_FILE_CONTENT_MISSING
- PH_QUERY_FILE_COPY_FAILED
- PH_QUERY_FILE_CORRUPT
- PH_QUERY_FILE_CREATE_FAILED
- PH_QUERY_FILE_EMPTY
- PH_QUERY_FILE_HEADER_GET_FAILED
- PH_QUERY_FILE_LINK_FAILED

- PH_QUERY_FILE_MAGIC_BAD
- PH_QUERY_FILE_MMAP_FAILED
- PH_QUERY_FILE_NAME_BAD
- PH_QUERY_FILE_OPEN_FAILED
- PH_QUERY_FILE_READ_FAILED
- PH_QUERY_FILE_REMOVE_FAILED
- PH_QUERY_FILE_SEEK_FAILED
- PH_QUERY_FILE_STAT_FAILED
- PH_QUERY_FORMAT_UNSUPPORTED
- PH_QUERY_FUNC_ERROR
- PH_QUERY_ID_DUPLICATE
- PH_QUERY_ID_INACTIVE
- PH_QUERY_ID_NOT_FOUND
- PH_QUERY_ID_REMOVE_FAILED
- PH_QUERY_ID_UNSUPPORTED
- PH_QUERY_INLINEREQUEST_BAD
- PH_QUERY_IPC_EVENT_SEND_FAILED
- PH_QUERY_IP_GET_FAILED
- PH_QUERY_IP_INVALID
- PH_QUERY_IP_TYPE_INVALID
- PH_QUERY_LOGINTEGRITYEXPORT_TASK_CREAT_FAILED
- PH_QUERY_LOGINTEGRITYEXPORT_TASK_INSERT_FAILED
- PH_QUERY_LOG_INTEGRITY_EXPORT_DIR_UNCONFIGURED
- PH_QUERY_LOG_INTEGRITY_EXPORT_FAILED
- PH_QUERY_LONG_RUNNING_STOPPED
- PH_QUERY_MEM_ALLOC_FAILED
- PH_QUERY_MESSAGE_SEND_FAILED
- PH_QUERY_MODULE_INIT_FAILED
- PH_QUERY_MODULE_UNCONFIGURED
- PH_QUERY_ONLINE_WORKER_CHANGED
- PH_QUERY_PARSED_EVENT_LOAD_FAILED
- PH_QUERY_PARTIAL_WORKER_FAILURE
- PH_QUERY_PCAP_FINALIZE_FAILED
- PH_QUERY_PCAP_LOAD_FAILED
- PH_QUERY_PCAP_RENAME_FAILED
- PH_QUERY_PCAP_TRANSFER_FAILED
- PH_QUERY_PGDB_EXEC_SQL_FAILED
- PH_QUERY_PGDB_RECONNECT_FAILED
- PH_QUERY_PGDB_SQL_GET_VAL_FAILED
- PH_QUERY_POST_FILTER_PARSE_FAILED
- PH_QUERY_PQ_ERROR
- PH_QUERY_PROCESS_GET_FAILED
- PH_QUERY_PROFILE_ATTR_UNSPECIFIED

- [PH_QUERY_PROFILE_EVENT_TYPE_ERROR](#)
- [PH_QUERY_PROFILE_FUNCTION_ERROR](#)
- [PH_QUERY_PROFILE_NOT_MARKED_AS_BASELINE](#)
- [PH_QUERY_PROGRESS_REJECTED](#)

EventType: PH_JAVA_AGENT_WEBSense_MAIL_PULL_ERROR

Description: FSM Java Agent Websense Email Gateway mail pulling error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSense_WEB_CONN_ERROR

Description: FSM Java Agent WebSecurity Gateway connection audit error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSense_WEB_EXEC_ERROR

Description: FSM Java Agent WebSecurity execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSense_WEB_MISSING_LOGDB

Description: FSM Java Agent WebSecurity log collection error - logDBName or urlDBName or urlCategoryDBName or dispositionDBName is null

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSPHERE_CONN_ERROR

Description: FSM Java Agent IBM Web sphere monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSPHERE_EXEC_ERROR

Description: FSM Java Agent IBM Web sphere log pulling error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_AGENT_WEBSPHERE_MONITOR_ERROR

Description: FSM Java Agent IBM Web sphere monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_ACTION_UNSUPPORTED_ERROR

Description: Java Query Server unsupported action

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_ELASTIC_ERROR

Description: Java Query Server Elasticsearch error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_ERROR

Description: Java Query Server error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_INFO

Description: Java Query Server Query informational log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_QUERYID_ERROR

Description: Java Query Server unknown or expired Query ID error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_QUERY_SYNTAX_ERROR

Description: Java Query Server Query syntax error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_REDIS_ERROR

Description: Java Query Server Redis error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JAVA_QUERYSERVER_WARN

Description: Java Query Server Query warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_JMS_QUEUE_SIZE_WARNING

Description: JMS Queue large

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_JOB_STAT

Description: Performance Monitor job status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobId	Job Id	string	
jobType	Job Type	uint16	
jobDetail	Job Detail	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
jobName	Job Name	string	
jobDesc	Job Description	string	
jobStatus	Job Status	uint16	
pollIntv	Polling Interval	uint32	
eventTime	Event Occur Time	Date	

EventType: PH_JOB_STATUS_XML_SEND_ERROR

Description: Error in sending Performance Monitor job status to app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_JOB_STATUS_XML_SENT

Description: Performance Monitor job status sent to app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_JOB_STAT_SUPPRESSED

Description: Performance monitor job status sending suppressed because of no change

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobId	Job Id	string	
jobType	Job Type	uint16	
jobDetail	Job Detail	string	
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
jobName	Job Name	string	
jobDesc	Job Description	string	
jobStatus	Job Status	uint16	
pollIntv	Polling Interval	uint32	
eventTime	Event Occur Time	Date	

EventType: PH_LIBEVENT_BUFFER_OVERFLOW

Description: FortiSIEM module encountered error while reading events from shared buffer

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIBEVENT_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIBEVENT_UNKNOWN_ATTR_ID

Description: Query/Report/Rule module encountered unknown event attribute id

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIBEVENT_UNKNOWN_ATTR_NAME

Description: Query/Report/Rule module encountered unknown event attribute name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_APACHE_PING_FAILED

Description: Discovery module failed to ping apache server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_APP_GROUP_FILTER_PARSE_ERROR

Description: Discovery module failed to parse Application Group filter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_APP_GROUP_FILTER_PUSH_ERROR

Description: Discovery module found empty group name in App Group Filter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_AWS_NEW_INSTANCE_NOT_RUN

Description: Discovery module found new AWS instance but it is not running

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_AWS_OBTAIN_INSTANCE_FAILURE

Description: FortiSIEM Discovery failed to obtain AWS instance

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_CHECK_APP_LIST_WARNING

Description: Discovery module failed to checking monitorability for windows servers

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CISCO_IOS_CBQOS_ERROR

Description: Discovery module encountered CBQoS monitoring error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CISCO_MERAKI_GET_CHILD_DEVICE_WARNING

Description: Discovery module failed to get Cisco Meraki child devices

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CISCO_MERAKI_GET_INTFS_WARNING

Description: Discovery module failed to get Cisco Meraki interfaces

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CISCO_MERAKI_GET_INTF_WARNING

Description: Discovery module failed to get Cisco Meraki interface

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.

EventType: PH_LIB_TOPO_CISCO_MERAKI_MAC_2_HOST_LOOKUP_FAILED

Description: Discovery module failed to get prev found Meraki device by MAC in mac-to-host table

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_CISCO_MERAKI_MAC_2_INTF_LOOKUP_FAILED

Description: Discovery module failed to get prev found Meraki device by MAC in mac-to-interface table

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_CISCO_UCS_LOGIN_FAILED

Description: Discovery module failed to login to Cisco UCS

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CISCO_UCS_REQUEST_ERROR

Description: Discovery module failed to send request to Cisco UCS

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_CPU_TOO_HIGH

Description: Discovery / Perf Monitoring module found CPU util for device to be too high

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
cpuUtil	CPU Util	double	

EventType: PH_LIB_TOPO_CUST_CONFIG_JOB_DOWNLOAD_SCRIPT_FAILED

Description: Discovery / Perf Monitoring module failed to download expect script from app server for custom config job

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
filePath	File Path	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_CHECK_PATH_ERROR

Description: Discovery / Perf Monitoring module failed to check configured path name for custom FIM job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_DEVICE_UNAVAILABLE

Description: Discovery / Perf Monitoring module found that device is not available for custom FIM job

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
command	Command	string	
exitValue	Command exit value	int32	

EventType: PH_LIB_TOPO_CUST_FIM_JOB_FILE_TOO_LARGE

Description: Discovery / Perf Monitoring FIM module found that file is too large to be pulled

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
filePath	File Path	string	
fileSize64	File Size64 Bytes	uint64	

EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_DATA_FAILED

Description: Discovery / Perf Monitoring failed to get data for custom FIM job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_FILE_INFO_FAILED

Description: Discovery / Perf Monitoring failed to get general file info for FIM job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_MD5_FAILED

Description: Discovery / Perf Monitoring failed to get file MD5 for FIM job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_GET_REMOTE_FILE_ERROR

Description: Discovery / Perf Monitoring failed to get remote file for FIM

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
jobName	Job Name	string	
filePath	File Path	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_INCORRECT_CRED

Description: Discovery / Perf Monitoring found incorrect username or password for custom FIM job

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
command	Command	string	
exitValue	Command exit value	int32	

EventType: PH_LIB_TOPO_CUST_FIM_JOB_RUN_SCP_FAILED

Description: Discovery / Perf Monitoring module failed to runScp.exp for FIM job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_FIM_JOB_TOO_MANY_FILES

Description: Discovery / Perf Monitoring module found that files count exceeds the max files count limitation under one directory for custom FIM job

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
dirName	Directory Name	string	

EventType: PH_LIB_TOPO_CUST_LOGIN_JOB_CREATE_EVENT_FAILED

Description: Discovery / Perf Monitoring module failed to create event for custom LOGIN job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_LOGIN_JOB_GET_DATA_FAILED

Description: Discovery / Perf Monitoring module failed to get data for custom LOGIN job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_SNMP_JOB_CREATE_EVENT_FAILED

Description: Discovery / Perf Monitoring module failed to create event for custom SNMP job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_SNMP_JOB_GET_DATA_FAILED

Description: Discovery / Perf Monitoring module failed to get data for custom SNMP job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_WMI_JOB_CREATE_EVENT_FAILED

Description: Discovery / Perf Monitoring module failed to create event for custom WMI job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_CUST_WMI_JOB_GET_DATA_FAILED

Description: Discovery / Perf Monitoring module failed to get data for custom WMI job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_ETHERMIB_STAT_LOOKUP_ERROR

Description: Discovery / Perf Monitoring module failed to get ethermib stat for interface

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

Id	Display name	Type	Description
srcSnmplntfIndex	Source Interface SNMP Index	uint16	SNMP index of the network interface through which a packet enters a network device. This information is typically present in Firewall logs.

EventType: PH_LIB_TOPO_EVENT_DROP_RULE_ENCODE_VALUE_GROUP_ERROR

Description: Discovery / Perf Monitoring module failed to encode value group

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_EVENT_DROP_RULE_PARSE_ERROR

Description: Parser module failed to parse event dropping rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_EXCLUDED_DISK_PARSE_ERROR

Description: Discovery / Perf Monitoring module failed to parse excluded disks

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_FCT_DEV_MAPPING_ENTRY_INVALID

Description: FortiClient device type mapping in /opt/phoenix/data-definition/FortiClientOSVersionMap.csv is invalid.

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_FGT_FABRIC_DISCOV_FAIL

Description: FortiGate Fabric Discovery Failure, if security fabric not enabled, this may be normal

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_FGT_GET_CONFIG_BACKUP_FAILED

Description: Failed to get config backup for FortiGate. Ensure that the FortiGate's rest api user role allows WRITE for System -> Administrator Users access permissions.

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_FGT_GET_USER_DEV_STORE_FAIL

Description: FortiGate User Device Store record retrieval failed. This is optional data

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_FGT_GET_USER_DEV_UNKNOWN

Description: FortiGate User Device Store identified an unknown device type. Add mapping to /opt/phoenix/data-definition/FortiClientOSVersionMap.csv

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_FGT_INSTALLED_SW_FAIL

Description: FortiGate failed to collect software module status via /api/v2/monitor/license/status.

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_FGT_SEC_POSTURE_RPT_API_FAIL

Description: FortiGate security posture report could not be retrieved via API on root fabric firewall.

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_FILE_READ_ERROR

Description: Discovery / Perf Monitoring module failed to read file

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_LIB_TOPO_FOUNDRY_HW_STATUS_ERROR

Description: Discovery / Perf Monitoring module failed to get hardware status for Foundry Iron device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oid	Object Identifier	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_GEN_UPS_STATUS_GET_ERROR

Description: Discovery / Perf Monitoring module failed to get hardware status via SNMP for GEN UPS device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_GET_NETAPP_NFS_FAILED

Description: Discovery / Perf Monitoring module failed to get NFS metrics via SNMP or ONTAP SDK for NetApp Filer

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_H3C_CPU_UTIL_ERROR

Description: Discovery / Perf Monitoring module failed to get CPU Util of H3C via SNMP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oid	Object Identifier	string	

EventType: PH_LIB_TOPO_HP3COM_CPU_UTIL_ERROR

Description: Discovery / Perf Monitoring module failed to get CPU Util of Hp3Com via SNMP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oid	Object Identifier	string	

EventType: PH_LIB_TOPO_HP3COM_MEM_UTIL_ERROR

Description: Discovery / Perf Monitoring module failed to get CPU Util of Hp3Com device via SNMP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
oid	Object Identifier	string	

EventType: PH_LIB_TOPO_HPUX_PROC_CPU_MEM_TOO_HIGH

Description: Discovery / Perf Monitoring module found HPUX Process CPU Util or Mem Util too high

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
procName	Process Name	string	
cpuUtil	CPU Util	double	
memUtil	Memory Util	double	

EventType: PH_LIB_TOPO_HYPERV_METRICS_GET_ERROR

Description: Discovery / Perf Monitoring module failed to get HyperV metrics

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_IMPORTANT_INTF_PARSE_ERROR

Description: Discovery / Perf Monitoring module failed to parse important interfaces

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_INTF_UTIL_ERROR

Description: Discovery / Perf Monitoring module found interface util monitoring data inconsistency

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.

EventType: PH_LIB_TOPO_JSON_PARSE_FAILED

Description: Failed to parse JSON

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_JUNIPER_INTF_SPEED_GET_ERROR

Description: Discovery / Perf Monitoring module failed to get interface speed from Juniper firewall

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
intfName	Host Interface Name	string	Name of a network interface in a host.

EventType: PH_LIB_TOPO_LIEBERT_HVAC_STATUS_GET_ERROR

Description: Discovery / Perf Monitoring module failed to get hardware status via SNMP for LIEBERT HAVC device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_LOGIN_PING_FAILED

Description: Discovery / Perf Monitoring module failed to execute a login command for discovery pruposes

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
ipPort	IP Port	uint16	IP port number
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_MAINTENANCE_DURATION_INCORRECT

Description: Perf Monitoring module failed to properly parse device maintenance duration from App Server

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	

EventType: PH_LIB_TOPO_MEM_TOO_HIGH

Description: Discovery / Perf Monitoring module memory util for device to be too high

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
memUtil	Memory Util	double	

EventType: PH_LIB_TOPO_NETAPP_AGGREGATE_STAT_ERROR

Description: Discovery / Perf Monitoring module failed to get NetApp Aggregate Stat via ONTAP SDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NETAPP_ANALYZE_VERSION_ERROR

Description: Discovery / Perf Monitoring module failed to analyze NetApp version via ONTAP SDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NETAPP_DISK_STAT_ERROR

Description: Discovery / Perf Monitoring module failed to get NetApp Disk Stat via ONTAP SDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NETAPP_GET_NFS_METRIC_ERROR

Description: Discovery / Perf Monitoring module failed to obtain NetApp NFS V3 metrics via ONTAPI

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NETAPP_GET_VERSION_ERROR

Description: Discovery / Perf Monitoring module failed to get NetApp version -- volume latencies may not be correct

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_NETAPP_LUN_STAT_ERROR

Description: Discovery / Perf Monitoring module failed to get NetApp LUN Stat via ONTAP SDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NETAPP_PROTO_STAT_ERROR

Description: Discovery / Perf Monitoring module failed to get NetApp Protocol Stat via ONTAP SDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NETAPP_VOLUME_STAT_ERROR

Description: Discovery / Perf Monitoring module failed to get NetApp Volume Stat via ONTAP SDK

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_NOT_SUPPORT_REST_API

Description: Rest API doesn't support in this fortigate version

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_OPEN_FILE_FAILED

Description: Unable to open file

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
details	Details	string	

EventType: PH_LIB_TOPO_PARSE_INTF_MAP_FAILURE

Description: Discovery / Perf Monitoring module failed to parse device interface map

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_PERF_JOB_EXEC_FAILED

Description: Perf Monitoring module failed to execute a specific performance monitoring job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
jobId	Job Id	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_PERF_JOB_INIT_FAILED

Description: Perf Monitoring module failed to initialize the performance monitoring job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_PERF_JOB_REMOVE_FAILED

Description: Perf Monitoring module failed to remove performance monitoring job by JOB ID

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
jobId	Job Id	string	

EventType: PH_LIB_TOPO_PERF_TEMPLATE_LOAD_ERROR

Description: Perf Monitoring module failed to load performance monitor template xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_PERF_TEMPLATE_PARSE_FAILURE

Description: Perf Monitoring module failed to parse performance monitor template xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_PERF_TEMPLATE_PARSE_WARNING

Description: Perf Monitoring module skipped one device type while loading Performance Monitor template xml

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_PORT_FILTER_PARSE_ERROR

Description: Perf Monitoring module failed to parse port filter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_PORT_FILTER_PUSH_ERROR

Description: Perf Monitoring module found empty protocol name in Port Filter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_PROC_CPU_MEM_TOO_HIGH

Description: Perf Monitoring module found process CPU Util or Mem Util to be too high

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
procName	Process Name	string	
cpuUtil	CPU Util	double	
memUtil	Memory Util	double	

EventType: PH_LIB_TOPO_REST_API_FAILED

Description: Failed to call a REST API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_RUN_SW_FILTER_PARSE_ERROR

Description: Discovery / Perf Monitoring module found failed to parse running software filter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_RUN_SW_FILTER_PUSH_ERROR

Description: Discovery / Perf Monitoring module found empty name and path in running software Filter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LIB_TOPO_SNMPWALK_ERROR

Description: Discovery / Perf Monitoring module found found empty or incomplete snmpwalk response

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
oid	Object Identifier	string	

EventType: PH_LIB_TOPO_STM_JOB_EXEC_FAILED

Description: Discovery / Perf Monitoring module failed to execute STM job for device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	

EventType: PH_LIB_TOPO_STM_JOB_INIT_FAILED

Description: Perf Monitoring module failed to initialize the STM job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
jobName	Job Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_TEST_CONN_HTTP_AGENT_FAILED

Description: Discovery module failed to test connectivity for http java agent

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LIB_TOPO_TEST_CONN_JDBC_AGENT_FAILED

Description: Discovery module failed to test connectivity for jdbc java agent

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LIB_TOPO_TEST_CONN_JMX_AGENT_FAILED

Description: Discovery module failed to test connectivity for jmx java agent

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LIB_TOPO_TRUNK_PORT_MAP_PARSE_ERROR

Description: Discovery module failed to parse trunk port map

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_VALIDATE_ACCESS_FAILED

Description: Perf Monitor module found device credential issues during initialization

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_DATABASE_INSTANCE_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange Database instance metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_DATABASE_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange Database metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_MAIL_SUBMISSION_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange mail submission metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_PUB_MAILBOX_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange public mailbox metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_REG_MAILBOX_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange regular mailbox metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_REPLICATION_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange replication metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_RPC_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange RPC metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_SMTP_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange SMTP metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_STORE_INTF_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange store interface metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WIN_GET_EXCH_TRANSPORT_QUEUE_WARNING

Description: Discovery/Perf Monitor module failed to get Exchange transport queue metrics via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WMI_GET_CPU_COUNT_ERROR

Description: Discovery/Perf Monitor module failed to get Windows CPU count via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WMI_GET_CPU_WARNING

Description: Discovery/Perf Monitor module failed to get CPU info for Windows device

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WMI_GET_PAGE_ACTIVITY_ERROR

Description: Discovery/Perf Monitor module failed to get Windows paging activity via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WMI_GET_REAL_MEM_ERROR

Description: Discovery/Perf Monitor module failed to get Windows real memory via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LIB_TOPO_WMI_GET_RUN_SW_PERF_ERROR

Description: Discovery/Perf Monitor module failed to get Windows running software performance via WMI

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LICENSE_ERROR

Description: FortiSIEM discovered license parsing error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LICENSE_INFO_FAILURE

Description: Failed to get license info

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LICENSE_INFO_INVALIDATED

Description: Invalid license

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LICENSE_NOT_EXIST

Description: There is no license file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_ACCOUT_MISSING

Description: Registration user name is missing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_BIND_PORT_FAILED

Description: Socket failed to bind port

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_LINUX_AGENT_CONFIG_ATTR_DECRYPTED_FAILED

Description: Failed to decrypt attr in config file.

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_LINUX_AGENT_CONFIG_ATTR_ENCRYPTED_FAILED

Description: Failed to encrypt attr in config file.

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_LINUX_AGENT_CONFIG_ATTR_NOT_FOUND

Description: Cannot find attribute in config file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_LINUX_AGENT_CONFIG_MISS_ATTR

Description: Cannot find attribute in config file

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_LINUX_AGENT_CREATE_SOCKET_FAILED

Description: Failed to create socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LINUX_AGENT_EXIT

Description: Linux agent received exit signal

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_HOST_IP_GOT_FAILED

Description: Failed to get host ip

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_INCREASE_RECV SOCK_BUF_MAX_FAILED

Description: Failed to increase Linux Agent recv socket buffe size

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_INIT_FIM_FAILED

Description: Linux Agent FIM Init Failed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_LINUX_AGENT_INIT_HTTP_FAILED

Description: Failed to initial http client

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_LINUX_AGENT_LOG_GENERIC

Description: Linux agent generic log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_NEW_FIM_LOADED

Description: Linux Agent New FIM Config Loaded

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_OPEN_FILE_FAILED

Description: Linux agent open file failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_LINUX_AGENT_OPEN_PORT_FAILED

Description: Failed to open port

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ipPort	IP Port	uint16	IP port number

EventType: PH_LINUX_AGENT_PWD_MISSING

Description: Registration password is missing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_RECV_ERROR

Description: Linux agent received error from socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number
recvBytes64	Received Bytes64	uint64	Number of bytes received by a host. This has 64bit resolution.

EventType: PH_LINUX_AGENT_REGISSTER_FAILED

Description: Failed to register linux agent

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_TEMPLATE_STATUS

Description: Linux Agent State

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
status	Status	string	

EventType: PH_LINUX_AGENT_UNINSTALL

Description: Linux agent received uninstall signal

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_UPLOAD_FILE_FAILED

Description: File Upload to destHost failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_LINUX_AGENT_UPLOAD_FILE_SUCCESS

Description: File is uploaded to collector successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_LINUX_AGENT_USER_FILE_LOG_GENERIC

Description: Linux agent generic user file log

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_LINUX_AGENT_VERIFIER_ERROR

Description: Linux agent verifier error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
size	Size	uint32	

EventType: PH_LOAD_CONFIG_CHANGE_FAILED

Description: FortiSIEM Rule/Report Master/Worker modules failed to load performance monitoring config change

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
infoURL	Informational URL	string	This field captures an URL if present in an event
item	Item	string	

EventType: PH_LOOKUP_TABLE_CANNOT_LOAD_DATA

Description: Failed to load data from Nodejs/Redis

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MAX_DEVICES_EXCEEDED

Description: Max number of devices exceeded license

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_MAX_DEVICES_LIMIT_REACHED

Description: Max number of devices exceeded license

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_ML_ANOMALY_DETECTED

Description: Machine Learning Anomaly Detected

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MODULE_ABORT

Description: Module exited abnormally

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
coreDumpFile	Coredump File Name	string	

EventType: PH_MODULE_ABORT_FOUND

Description: Module found aborted

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	
eventTime	Event Occur Time	Date	

EventType: PH_MODULE_ACCEPTED_CONN

Description: Module accepted connection

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_MODULE_ACE_ACCEPTOR_FAILED

Description: ACE failed to accept

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MODULE_ACE_HANDLE_EVENT_ERROR

Description: ACE failed to handle event

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MODULE_COMM_ERROR

Description: Module encountered inter-module communication error

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MODULE_COMM_HANDLER_REG

Description: Module registering notification handlers

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
notifId	Notification ID	uint32	
handlerName	Notification Handler Name	string	

EventType: PH_MODULE_COMM_PORTS_OPENED

Description: Module opened Notification Service ports

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event

EventType: PH_MODULE_DB_CONFIG_LOADED

Description: Module loaded database config successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_DIODE_CONFIG_ERROR

Description: Module failed to load diode collector config

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MODULE_EXCEPTION_NOT_CAUGHT

Description: Exception not caught

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MODULE_EXITING

Description: Module exiting

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_EXIT_OK

Description: Module exited gracefully

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_HEARTBEAT_INIT

Description: Module initializing heartbeat object

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_INITIALIZING

Description: Module initialization

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_INIT_COMPLETE

Description: Module successfully started

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_INIT_FAILURE

Description: Module initialization failure

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	

EventType: PH_MODULE_LICENSE_FAILURE

Description: Module failed to get license

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MODULE_LOADED_NEW_CONFIG

Description: Module successfully loaded new config

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_LOAD_DIODE_CRED_ERROR

Description: Failed to load diode collector agent credential

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MODULE_LOCAL_CONFIG_LOADED

Description: Module loaded local config successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configName	Config Name	string	

EventType: PH_MODULE_LOCAL_CONFIG_SECTION_ERROR

Description: Module failed to load local config section

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configSectName	Config Section Name	string	

EventType: PH_MODULE_LOCAL_CONFIG_VALUE_ERROR

Description: Module failed to load local config value

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configName	Config Name	string	
configValue	Config Value	string	

EventType: PH_MODULE_LOG_LEVEL_CHANGE

Description: Module received log level change

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
oldLogLevel	Old Log Level	uint32	
newLogLevel	New Log Level	uint32	

EventType: PH_MODULE_RECVD_EXIT_EXT

Description: Module received external signal to exit

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_MODULE_RECVD_EXIT_MONITOR

Description: Module received exit request from Monitor

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_RECVD_NEW_CONFIG

Description: Module received config change notification

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_RECVD_START

Description: Module received start request

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MODULE_SETPIDFILE_ERR

Description: Module unable to set PID file

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_MODULE_UNABLE_INIT_SHARED_STORE

Description: Module unable to init shared store

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MODULE_UNABLE_OPEN_COMM_PORT

Description: Module unable to open inter-module comm port during initialization

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ipProto	IP Protocol	uint16	IP Protocol, e.g. TCP, UDP, ICMP etc as defined in IP RFPs
srcIpPort	Source TCP/UDP Port	uint16	This is the source TCP or UDP port as identified in the event

EventType: PH_MONITOR_ARCHIVE_GET_WORKER_FAILURE

Description: phMonitor Failed to get worker list for archive change

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_ARCHIVE_UPDATE_WORKER_FAILURE

Description: phMonitor Failed to update worker archive

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_BEACONING_REGISTER_FAILURE

Description: Beaconing Registration Failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_CHECK_DEPENDENCY_FAILED

Description: Failed to check dependency

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_CMD_FAILURE

Description: phMonitor failed to run command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
errorNoInt	Error Number Int	int32	

EventType: PH_MONITOR_CMD_SEND_FAILURE

Description: FortiSIEM Monitor module failed to send command to other FortiSIEM modules

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
targetProcName	Target Process Name	string	

EventType: PH_MONITOR_COLLECTOR_REGISTER_FAILURE

Description: phMonitor failed to register collector

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_COLLECTOR_UPDATE_STATUS_FAILURE

Description: FortiSIEM Monitor module failed to update Collector status

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

EventType: PH_MONITOR_CONFIG_DOWNLOAD_FAILURE

Description: phMonitor failed to download config from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_DBCLUSTER_SEND_COMMAND_FAILED

Description: Send Reset Command to Super failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_DELETE_DR_FAILED

Description: Failed to delete DR

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_DELETE_SECONDARY_ON_WORKER_FAILED

Description: Failed to remove DR configuration on secondary worker

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_DELETE_SUPER_FOLLOWER_FAILED

Description: Failed to remove configuration of follower super

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_DISPATCH_CMD_MISMATCH

Description: phMonitor failed to dispatch wrong command to other processes

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_MONITOR_DOMAIN_CHANGE_XML_PARSE_FAILURE

Description: phMonitor failed to parse AppDefn object from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_ENT_OR_SP_MODE_MISSING

Description: phMonitor failed to identify Service Provider or Enterprise installation

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_EXCESSIVE_DB_LOGIN_FAILURE

Description: phMonitor failed to login to PostGreSQL

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_MONITOR_FAILED_CONN_QUERYMASTER

Description: Unable to send status query to QueryMaster

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_FILE_IO_ERROR

Description: phMonitor encountered empty or unreadable file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_MONITOR_FILE_PERMISSION_ERROR

Description: File Permission error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_FILE_PERMISSION_WARNING

Description: File permission warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
details	Details	string	

EventType: PH_MONITOR_FLIP_PRIMARY_FAILURE

Description: phMonitor failed to flip primary server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_FSM_AGENT_UPDATE_PWD_ERROR

Description: phMonitor failed to update FortiSIEM Agent upload password

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_GET_REPLICATION_PROGRESS_FAILED

Description: Failed to get replication progress

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_GET_UPTIME_ERROR

Description: FortiSIEM Monitor module failed to get system uptime

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_HANDLE_TASK

Description: Monitor handles task

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_HARDWARE_SN_FORK_FAILURE

Description: phMonitor failed to fork to determine hardware Serial Number

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_HOST_UUID_READ_FAILURE

Description: phMonitor on Collector failed to read CSI

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_HTTP_PULL_ERROR

Description: phMonitor failed to pull information via HTTP from App Server

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_INIT_PROC_MODULE_NOT_FOUND

Description: phMonitor failed to initialize - Module not found

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	

EventType: PH_MONITOR_INIT_SECONDARY_ON_WORKER_FAILED

Description: Failed to update configuration on secondary worker

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_INIT_SUPER_FOLLOWER_FAILED

Description: Failed to update configuration of follower super

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_INIT_SYSTEM_XML_PARSE_FAILURE

Description: phMonitor failed to initialize - Wrong System Services XML in Config file

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_MONITOR_JDBC_POOL_NOT_EXIST

Description: JDBC Connection Pool exist

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_LIB_DEPENDENCY_WARNING

Description: Library dependency warning

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
details	Details	string	

EventType: PH_MONITOR_LICENSE_ERROR

Description: phMonitor encountered license file error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_LOAD_CONF_FROM_APP_SERVER_FAILED

Description: Failed to load configure from app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_LOCAL_HOSTNAME_GET_FAILURE

Description: phMonitor cannot get local machine host name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_MEM_FILE_OPEN_FAILURE

Description: phMonitor failed on mem file open

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
userId	User Id	string	

EventType: PH_MONITOR_MISSING_MONITOR

Description: No running phMonitor process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_MMAP_FAILURE

Description: phMonitor encountered MMAP failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_MOTNIROR_REGISTER_FAILURE

Description: phMonitor failed to register other monitors

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_NOTIFICATION_CLIENT_CONTACT_FAILURE

Description: phMonitor Notification Client failed to contact another process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_MONITOR_NOTIFICATION_CMD_EMPTY

Description: phMonitor Notification client encountered invalid argument

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_NOTIFICATION_CMD_MISMATCH

Description: phMonitor Notification client encountered unknown command type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
notifEvtId	Notification Event Id	uint32	

EventType: PH_MONITOR_NOTIFICATION_RETURN_FAILURE

Description: phMonitor Notification client encountered returns failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
xmlBody	XML Body	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_MONITOR_PHOENIX_CONFIG_GLOBAL_MISSING

Description: phMonitor found GLOBAL phoenix_config section missing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_PHOENIX_CONFIG_INVALID

Description: phMonitor found Invalid phoenix config file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_PROCESS_OWNER_NOT_ADMIN_ERROR

Description: FortiSIEM Monitor module detected that a file owner is not admin

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
userId	User Id	string	
groupId	Group ID	string	

EventType: PH_MONITOR_QUERY_LICENSE_FAILED

Description: Follower Super query license failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id				Display name				Type				Description			
errorString				Error String				string				This is the error message, synonymous to attribute errReason			

EventType: PH_MONITOR_RECVD_CONFIG_CHANGE

Description: Monitor received config change notification

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_RECVD_HEARTBEAT

Description: Monitor received heartbeat from module

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id				Display name				Type				Description			
reptProcName				Reported Process Name				string							
hostIpAddr				Host IP				IP				This is the IP of the device of interest in the event.			
usrMsg				User defined msg				string							

EventType: PH_MONITOR_REDIS_UPDATE_FAILED

Description: Failed to update redis cluster

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_REGISTER_MONITOR_GET_WORKER_FAILURE

Description: phMonitor failed to get workers

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REGISTER_NODE

Description: Register node

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REGISTER_SUPER_FOLLOWER

Description: Register follower super

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REGISTER_WORKER

Description: Register worker

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REMOVE_NODE

Description: Remove node

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REMOVE_SUPER_FOLLOWER

Description: Remove follower super

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REMOVE_WORKER

Description: Remove worker

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REPORTSERVER_LICENSE_INVALID

Description: phMonitor found invalid Report Server license

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_MONITOR_REPORTSERVER_NOTIFICATION_CLIENT_CONTACT_FAILURE

Description: phMonitor Notification client failed to contact report server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_MONITOR_REPORTSERVER_NOTIFICATION_CLIENT_INIT_FAILURE

Description: phMonitor Notification client failed to contact report server

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_MONITOR_REPORTSERVER_NOTIFICATION_SERVER_RETURN_FAILURE

Description: phMonitor Notification client encountered report server return failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	

EventType: PH_MONITOR_RESET_DB_SERVER_NAME_FAILED

Description: Failed to set phoenixPool.ServerName

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_RESET_JDBC_CONN_FAILED

Description: Failed to flush database connection pool

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_RESET_STORAGE_CONFIG_FAILED

Description: Failed to reset storage configuration

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
type	Type	string	

EventType: PH_MONITOR_RESTART_MODULES

Description: Monitor restarting all modules

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REST_CACHE_REQUEST_EMPTY

Description: phMonitor found empty REST Cache Request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REST_CACHE_REQUEST_FAILURE

Description: phMonitor failed to get response to Cache REST API request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
requestBody	Request Body	string	

EventType: PH_MONITOR_REST_CACHE_REQUEST_FORMAT_ILLEGAL

Description: phMonitor encountered Invalid REST Request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
requestBody	Request Body	string	

EventType: PH_MONITOR_REST_CACHE_SERVER_INIT_FAILURE

Description: phMonitor failed to initialize HTTP cache server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_REST_CALL_FAILURE

Description: phMonitor REST API call failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
uriStem	URI Stem	string	

EventType: PH_MONITOR_ROLE_UNDEFINED

Description: phMonitor found undefined Monitor Role in phoenix_config.txt

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_SAVE_DR_CONFIG_FAILED

Description: Failed to write DR config in local file. The secondary DB Leader can't update DR config

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_SEND_CMD_TO_MODULE

Description: Monitor sending command to module

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_MONITOR_SEND_VG_UPDATE_CMD_TO_MODULE

Description: Monitor sending value group update command to module

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_MONITOR_SETUID_FAILURE

Description: phMonito failed to raise privilege via setuid()

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_START_MODULE

Description: Monitor starting a module

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	

EventType: PH_MONITOR_START_MODULES

Description: Monitor starting all modules

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STATFS_FAILURE

Description: phMonitor statfs() return failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_MONITOR_STATUS_PUSHER_SPAWN_FAILURE

Description: phMonitor encountered error in spawning statusPusher thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STOP_MODULES

Description: Monitor stopping all modules

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STOP_READER

Description: Deactivating shared store reader

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	

EventType: PH_MONITOR_STORAGE_ES_CUSTOMIZED_TEMPLATE_DEPLOYED

Description: Monitor deployed customized ES templated

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STORAGE_GET_WORKER_FAILURE

Description: phMonitor Failed to get worker list for storage change

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STORAGE_LOCAL_GET_FAILURE

Description: FortiSIEM Monitor module failed to get local disk configuration for event database storage

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STORAGE_NFS_GET_FAILURE

Description: phMonitor failed to get nfs

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_MONITOR_STORAGE_TYPE_GET_FAILURE

Description: phMonitor failed to get storage type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_STORAGE_TYPE_UNKNOWN

Description: phMonitor encountered unknown storage type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
type	Type	string	

EventType: PH_MONITOR_STORAGE_UPDATE_WORKER_FAILURE

Description: phMonitor Failed to update worker storage

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_SVC_PASSWORD_DISTRIBUTION_ERROR

Description: phMonitor failed to contact one or more processes with changed svc passwd - so restarting all processes

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_SYSINFO_FAILURE

Description: phMonitor could not get system uptime via sysinfo - assuming uptime of 1 day

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_MONITOR_SYSTEM_DB_LOGIN_ERROR

Description: DB login failure

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_SYSTEM_HEALTH_CPU

Description: PH system health issue: high CPU usage

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	

EventType: PH_MONITOR_SYSTEM_HEALTH_ISSUE

Description: PH system health issue: high CPU and/or memory usage

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
reptProcName	Reported Process Name	string	

EventType: PH_MONITOR_SYSTEM_HEALTH_MEM

Description: PH system health issue: memory usage

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	

EventType: PH_MONITOR_SYSTEM_STATUS_SPAWN_FAILURE

Description: phMonitor encountered error in spawning systemStatus thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_THREAD_SPAWN_FAILED

Description: Failed to spawn thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_TUNNEL_ERROR

Description: phMonitor encountered Tunnel XML error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_UMOUNT_NFS_FAILURE

Description: phMonitor failed to umount nfs

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_MONITOR_UNABLE_CONTACT_APPSVR

Description: phMonitor unable to contact App Server - see response code

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
httpStatusCode	HTTP Status	string	

EventType: PH_MONITOR_UPDATE_DATA_FAILED

Description: Failed to update GeoDB Files

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_UPDATE_DR_FAILED

Description: Failed to update DR

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_UPDATE_WORKER_INFO_FAILED

Description: Failed to update worker info with app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_UPLOAD_LOG_SPAWN_FAILURE

Description: phMonitor encountered error in spawning logUploader thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_WINAGENT_DELETE_PWD_SPAWN_FAILURE

Description: phMonitor encountered error in spawning removeHttpdPassword thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_WINAGENT_UPDATE_PWD_ERROR

Description: phMonitor encountered failed to update windows agent upload password

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_MONITOR_WIN_LINUX_AGENT_PWD_UPDATE_SUCCESS

Description: Windows/Linux Agent password is update successfully

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phAgentId	Agent ID	string	Unique ID of Linux or Windows Agents in FortiSIEM. This is assigned by App Server when an agent registers.

EventType: PH_MONITOR_WORKER_NODECONFIG_UPDATE_FAILED

Description: Failed to update nodejs config file with auth info on worker

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_WORKER_REDIS_ADDSLAVE_UPDATE_FAILED

Description: Failed to update redis config file with addslave info on worker

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_MONITOR_WORKER_REDIS_CONF_UPDATE_FAILED

Description: Failed to update redis config file with auth info on worker

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_FLOW

Description: Parser module module received a netflow packet with wrong length

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_FLOW_END

Description: Parser module received a netflow packet with unsupported end of netflow datagram

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_HEADER_PROTOCOL

Description: Parser module received a netflow packet with unsupported netflow header protocol

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_PACKET

Description: Parser module received a incorrectly formatted netflow packet

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_RECORD

Description: Parser module received a incorrectly formatted netflow flow

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_TYPE

Description: Parser module received a netflow packet with unsupported netflow sample type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NETFLOW_BAD_VER

Description: Parser module received a netflow packet with unsupported netflow version

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_NETFLOW_EXCEPTION

Description: Parser module encountered netflow parsing error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NOTIFICATION_ACCEPT_FAILURE

Description: failed to accept connection

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NOTIFICATION_CALLBACK_ERROR

Description: FortiSIEM Notification module callback error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NOTIFICATION_CONN_FAILED

Description: FortiSIEM Notification module failed connection

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverName	Server Name	string	
ipPort	IP Port	uint16	IP port number
module	Module Name	string	

EventType: PH_NOTIFICATION_INIT_FAILED

Description: FortiSIEM Notification module initialization failed

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_NOTIFICATION_NO_RESPONSE

Description: has no response on Notification

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NOTIFICATION_RETURN_FAILURE

Description: Notification returns failure

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NOTIFICATION_SEND_FAILURE

Description: FortiSIEM Notification module send failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_NOTIFICATION_SEND_FILE_FAILURE

Description: FortiSIEM Notification module file send failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_NO_PARSER_FOR_EVENT

Description: No parser available for event

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventName	Event Name	string	This is the eventType display name, or human readable name. In many cases the eventType is sufficiently labeled.

EventType: PH_OBJECT_NOT_FOUND

Description: Can not find specified object

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_PARSER_BIND_PORT_FAILURE

Description: Parser module failed to bind to a TCP/UDP ports

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_DATA_SIZE_OVERFLOW

Description: Data size exceeding capacity

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_DIR_OPEN_FAILURE

Description: Parser module failed to open directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_PARSER_EVENT_PARSER_ERROR

Description: Parser module failed to parse event parsing xml from local disk or App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
tagName	Tag Name	string	
parserName	Event Parser Name	string	The name of parser that parsed the event
funName	Function Name	string	

EventType: PH_PARSER_EVENT_SERIALIZE_ERROR

Description: Parser module failed to serialize event before writing to shared buffer

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_FILE_DELETE_FAILURE

Description: Parser module failed to delete file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_FILE_DELETE_FAILURE_RENAME

Description: Parser module failed to delete file but succeeded to rename. These files may fill up disk

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_FILE_INVALID_FORMAT

Description: Parser module failed to parse event or metadata files with invalid file format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_FILE_INVALID_HEADER

Description: Parser module failed to parse event files with invalid file header

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_FILE_NOT_EXIST

Description: File doesn't exist

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_FILE_OPEN_FAILURE

Description: Parser module failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_FILE_PARSE_FAILURE

Description: Failed to parse file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_FILE_READ_FAILURE

Description: Parser module failed to read file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_FILE_RENAME_FAILURE

Description: Parser module failed to rename file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_FILE_SIZE_MISMATCH

Description: Parser module ignored event file from collector because of file size mismatch

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_FILE_STAT_FAILURE

Description: Parser module failed to obtain file status and will skip the file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_FILE_WRITE_FAILURE

Description: Parser module failed to write file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_GEO_WRONG_ATTR_NUMBER

Description: Parser module internal error - mismatched GEO attribute count

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_GEO_WRONG_CACHE_NUMBER

Description: Parser module internal error - incorrect GEO cache attribute count

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_GET_PROCESS_ERROR

Description: Parser module failed to get own process information

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_GLOBAL_LICENSE_EXCEED

Description: Global EPS license exceeded and events will be dropped

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
licenseEventsPerSec	License EPS	uint64	

EventType: PH_PARSER_HTTP_RESPONSE_ERROR

Description: Parser module failed to get response from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_PARSER_HTTP_UPLOAD_FAILURE

Description: Parser module failed to upload information to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_INIT_DEV_CRED_FAILED

Description: Failed to initialize device credential

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_INIT_FAILURE

Description: Parser module failed to initialize

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_INVALID_CSV

Description: Parser module failed to load CSV file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_INVALID_EXT_LOG_PROTO

Description: Parser module encountered unsupported external log receive protocol

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_INVALID_ORG_NAME

Description: Parser module received invalid organization in event

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.

EventType: PH_PARSER_INVALID_PHOENIX_CONFIG

Description: Parser module found incorrectly formatted phoenix config file entry

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	
configName	Config Name	string	
configValue	Config Value	string	

EventType: PH_PARSER_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_JSON_PARSE_FAILURE

Description: Parser module failed to parse Json

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
jsonBody	JSON Body	string	

EventType: PH_PARSER_MALLOC_FAILURE

Description: Parser module failed to dynamically allocate memory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_PACK_EVENT_ERROR

Description: Parser module failed to pack event before sending to other modules for internal communication

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_PARSER_RAWEVENT_TOO_LARGER

Description: Raw event's size is more than 10M. Save it to tmp file and not send to parser

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_REST_PARSE_ERROR

Description: Parser module failed to parse REST api from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_RUN_PROCESS_ERROR

Description: Parser module failed to start

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_SEND_EVENT_FAILURE

Description: Parser module failed to send event

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_SEND_TO_DISCOV_FAILURE

Description: Parser module failed to send internal event to discovery module

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_SEND_TO_MONITOR_FAILURE

Description: Parser module failed to send internal event to Supervisor phMonitor process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_SET_USER_ID_FAILURE

Description: Parser module unable to set effective user ID

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_SHARED_STORE_ERROR

Description: FortiSIEM Parser module encountered shared store error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_SNMPTRAP_INIT_FAILURE

Description: Parser module failed to initialize snmptrap

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_SOCKET_ERROR

Description: Parser module failed to open socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_SOCKET_RECV_ERROR

Description: Parser module failed to receive message via socket

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_SOCKET_SELECT_ERROR

Description: Parser module failed to select in socket API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_PARSER_SPAWN_THREAD_FAILURE

Description: Parser module failed to spawn thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_PARSER_SSL_ACCEPT_ERROR

Description: Parser module failed to accept SSL connection

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_SSL_CERT_LOAD_ERROR

Description: Parser module failed to load SSL certificate

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_TCP_SOCKET_ACCEPT_ERROR

Description: Failed to accept connect

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_TEST_RULES_PARSE_ALL_EVENTS_BEGIN

Description: Parser beginning to parse all events

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_PARSER_TEST_RULES_PARSE_ALL_EVENTS_END

Description: Parser finished parsing all events

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_PARSER_TEST_RULES_PARSE_ONE_EVENT_BEGIN

Description: Event parsing begins

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_PARSER_TEST_RULES_PARSE_ONE_EVENT_END

Description: Event parsing ends

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventId	Event ID	uint64	This is a globally unique ID assigned to every raw event ingested into the SIEM. This is used by the system for tying events to incidents, and is typically not needed by end users.

EventType: PH_PARSER_TOO_MANY_UNKNOWN_EVENTS

Description: Too many unknown events

Notes: This event is generated by the phParser process running on a FortiSIEM node when too many unknown events are received from a single source IP (Reporting IP). Unknown events implies that there is no matching parser to parse those events. The thresholds are defined in /opt/phoenix/config/phoenix_config.txt.

[BEGIN PHPARSER]

unknown_event_skip_eps=20

unknown_event_skip_size=10240 # 10kB

[END PHPARSER]

The explanation of these attributes is as follows. The attribute `unknown_event_skip_eps` is used to calculate the maximum number of allowed unparsed events from a source. The attribute `unknown_event_skip_size` is used to calculate the maximum size of allowed unparsed raw events from a source.

The window for detecting excessive unknown events in 3 minutes (or 180 seconds). In this window:

- the maximum number of allowed unparsed events from a single source is `unknown_event_skip_eps` times 180, and
- the maximum cumulative raw event size (in bytes) of all unparsed events from a single source is `unknown_event_skip_size`.

For example: For `unknown_event_skip_eps=20` and `unknown_event_skip_size=10240`, if either 3600 unknown events is received from one source or the total size of unknown events from one source reaches 10kB in a 3 minute window, then the event `PH_PARSER_TOO_MANY_UNKNOWN_EVENTS` is generated and parsing stops for that reporting IP for the remainder of the 3 minute window. Once the 3 minute window expires, the restriction is lifted and events from that IP are parsed again. If the condition happens again in the new window, then the same action is taken as the previous window.

This action is taken to reduce the load on the parser module in the case of excessive unknown events. Increasing the values of `unknown_event_skip_eps` and `unknown_event_skip_size` may have a performance impact on the CPU and memory consumption by the parser module on that FortiSIEM node.

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
relayDevIpAddr	Relaying IP	IP	Relaying IP is most commonly used to specify the log relay appliance, usually a collector.

EventType: PH_PARSER_UPDATE_FAILURE

Description: Parser module failed to update internal information from REST API

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_USE_ERROR_BEFORE_INIT

Description: Parser module attempted to use an object before initialization

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_WRONG_EVENT_SIZE

Description: FortiSIEM module failed to load serialized event

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PARSER_WRONG_PARAMETER

Description: Parser module encountered wrong parameter during event parsing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
paraName	Param Name	string	
parserName	Event Parser Name	string	The name of parser that parsed the event

EventType: PH_PARSER_WTAP_ERR_BAD_FILE

Description: The file is damaged or corrupt

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_WTAP_ERR_CANT_OPEN

Description: Parser module failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_COMPRESSION_NOT_SUPPORTED

Description: Parser module failed to write this file type as a compressed file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_DECOMPRESS

Description: The compressed file appears to be damaged or corrupt

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_WTAP_ERR_ENCAP_PER_PACKET_UNSUPPORTED

Description: Parser module doesn't support the network type in the file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_FILE_UNKNOWN_FORMAT

Description: Parser module doesn't support this file format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_NOT_REGULAR_FILE

Description: Parser module failed to parse a special file or socket or other non-regular file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_RANDOM_OPEN_PIPE

Description: Parser module can't parse a pipe or FIFO files

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_SHORT_READ

Description: The file has been cut short in the middle of a packet

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_SHORT_WRITE

Description: Parser module failed to write a full header in the file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PARSER_WTAP_ERR_UNSUPPORTED

Description: Parser module doesn't support record data in the file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PARSER_XML_PARSE_ERROR

Description: Parser module failed to parse generic xml document

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
tagName	Tag Name	string	
parserName	Event Parser Name	string	The name of parser that parsed the event

EventType: PH_PARSER_XML_PARSE_FAILURE

Description: Parser module failed to parse XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propName	Property Name	string	
propValue	Property Value	string	

EventType: PH_PARSE_CONFIG_CHANGE_FAILED

Description: FortiSIEM bRule/Report Master/Worker modules failed to parse performance monitoring config change

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PDF_BUILDER_ERROR

Description: PDF builder error

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_COMMIT_FILE_FAILED

Description: Perf Monitoring module failed to commit file into svn - may due to race condition - will retry

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_CONFIG_SEND_FAILED

Description: Perf Monitoring module found unexpected http return code when sending config version to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_PERFMON_CONFIG_VERSION_ERROR

Description: Perf Monitoring module encountered wrong config version

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_CONFIG_VERSION_WARNING

Description: FortiSIEM Performance monitoring module detected Monitoring Config version out of sync with App server

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PERFMON_CUST_JOB_ADD_FAILED

Description: Perf Monitoring module failed to add custom monitoring job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_INIT_ERROR

Description: Perf Monitoring module failed to initialize

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PERFMON_INST_SW_MAP_EMPTY

Description: Perf Monitoring module found that downloaded Installed software map from App Server is empty

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_INST_SW_NO_NAME

Description: Perf Monitoring module found that downloaded Installed software from App Server has no name

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_JOB_ADD_FAILED

Description: Perf Monitoring module failed to add monitoring job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_MASS_PING_WARNING

Description: Perf Monitoring MassPing module found invalid IP

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_MONITEE_BAD

Description: Perf Monitoring module encountered bad monitee map entry

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_MONITEE_NOT_FOUND

Description: Perf Monitoring module failed to find a monitee

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_NO_DEV_TYPE

Description: Perf Monitoring module encountered internal error - devTypeToJobItemMap find failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_PERF_OBJ_PARSE_FAILURE

Description: Perf Monitoring module did not find performance object definition in XML received from App Server

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_PING_RESULT_OPEN_FAILED

Description: Perf Monitoring module failed to open Ping result file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_PROC_RUN_FAILED

Description: Perf Monitoring module failed to run process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_REAL_TIME_JOB_RUN_FAILED

Description: Perf Monitoring module failed to run real time job

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PERFMON_ROUTE_LOAD_ERROR

Description: Perf Monitoring module failed to load network dependency from app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PERFMON_STATUS_REPORTER_INIT_FAILED

Description: Perf Monitoring module failed to initialize job status reporter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_STATUS_REPORT_FAILED

Description: Perf Monitoring module failed to report task status to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_SVN_CHECKOUT_FAILED

Description: Perf / Config Monitoring module failed to check out SVN directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_PERFMON_SVN_CONFIG_MISSING

Description: Perf / Config Monitoring module failed to find running or startup config

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_SVN_DIR_CREATE_FAILED

Description: Perf / Config Monitoring module failed to create svn root dir

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_PERFMON_SVN_DIR_UPDATE_FAILED

Description: Perf / Config Monitoring module failed to update dir

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_PERFMON_SVN_FILE_COPY_FAILED

Description: Perf / Config Monitoring module failed to copy file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	

EventType: PH_PERFMON_SVN_FILE_EMPTY

Description: Perf / Config Monitoring module config file is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_FILE_MARK_FAILED

Description: Perf / Config Monitoring module failed to mark file for add to svn

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_FILE_OPEN_FAILED

Description: Perf / Config Monitoring module cannot open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_PERFMON_SVN_FILE_PARSE_FAILED

Description: Perf / Config Monitoring module failed to parse file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_FILE_REMOVE_FAILED

Description: Perf / Config Monitoring module failed to remove file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_PERFMON_SVN_FILE_RENAME_FAILED

Description: Perf / Config Monitoring module cannot rename file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	

EventType: PH_PERFMON_SVN_FIM_FILE_MISSING

Description: Perf / Config Monitoring module failed to find FIM file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_SVN_FIRSTFILELINES_EMPTY

Description: Perf / Config Monitoring module found that FIRSTFILENAME is empty in file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_FIRSTFILELINES_NOT_IN_FILE

Description: Perf / Config Monitoring module found that FIRSTFILELINES is not in file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_GET_DEVICE_ID_FAILED

Description: Perf / Config Monitoring module failed to get device ID via hostname and IP from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_PERFMON_SVN_GET_DISCOV_TIME_FAILED

Description: Perf / Config Monitoring module failed to get discover time

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PERFMON_SVN_INFO_GET_FAILED

Description: Perf / Config Monitoring module failed to get svn info on file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_INST_SW_BAD

Description: Perf / Config Monitoring module found that Installed Software xml is incorrectly formatted

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_SVN_INVALID_FILE_FORMAT

Description: Perf / Config Monitoring module found file format error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_INVALID_HEADER_IN_FILE

Description: Perf / Config Monitoring module found that file has incomplete header

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_INVALID_SECONDFILENAME

Description: Perf / Config Monitoring module found that SECONDFILENAME is invalid

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_LINE_MISMATCH

Description: Perf / Config Monitoring module found that line number not matched with the expected value

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_SVN_SECONDFILENAME_EMPTY

Description: Perf / Configuration Monitoring module found that SECONDFILENAME is empty in file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_SVN_SOFTWARE_MISSING

Description: Perf / Configuration Monitoring module found missing installed software

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_TOPO_CONFIG_ERROR

Description: Perf Monitoring module failed to parse topo xml from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PERFMON_TOPO_FILE_OPEN_FAILED

Description: Perf Monitoring module failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_PERFMON_TOPO_LOAD_ERROR

Description: Perf Monitoring module failed to load topology from app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_TRACERT_FILE_OPEN_FAILED

Description: Perf Monitoring module cannot open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_PERFMON_UNKNOWN_CUST_PERF_JOB_ID

Description: Perf Monitoring module encountered unknown custom performance monitoring job id from App Server

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_UNKNOWN_PERF_JOB_ID

Description: Perf Monitoring module encountered unknown performance monitoring job id from App Server

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_UNKNOWN_PROBE_JOB_ID

Description: Perf Monitoring module encountered unknown probe job id from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_PERFMON_UPDATE_CONFIG_ERROR

Description: Perf Monitoring module failed to update monitoring config from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PERFMON_UPDATE_FILTERS_ERROR

Description: Perf Monitoring module failed to update interface filter Perf Monitoring module

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PERFMON_UPDATE_ROUTE_DEPENDENCY_FAILED

Description: Perf Monitoring module failed to upload network dependency to app server - Unexpected http response code

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_PERFMON_USER_PWD_GET_FAILED

Description: Perf Monitoring module failed to get user and password

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_PERFORM_MONITOR_ERROR

Description: FortiSIEM Performance Monitor generic error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_PER_MON_CONFIG_ERROR

Description: Config discover error occurred

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_PER_MON_FETCH

Description: Performance Monitoring module doing SNMP fetch for an OID

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
comm	Community String	string	
oid	Object Identifier	string	

EventType: PH_PER_MON_FUNCTION

Description: Entering Performance Monitoring Debug Function

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_PER_MON_SNMP_DONE

Description: Performance Monitoring module successfully did SNMP fetch

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
comm	Community String	string	
oid	Object Identifier	string	

EventType: PH_PER_MON_WALK

Description: Performance Monitoring module starting SNMP walk for an OID

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
comm	Community String	string	
oid	Object Identifier	string	

EventType: PH_PER_MON_WALK_ERROR

Description: FortiSIEM Performance Monitor SNMP Walk error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
comm	Community String	string	
oid	Object Identifier	string	

EventType: PH_QUERYSRV_DUPLICATED_QUERYID

Description: Duplicated query id

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERYSRV_INVALID_QUERYXML

Description: Invalid query xml

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_AGGR_RESULTS_POST_PROCESS_FAILED

Description: Query Master failed to post-process aggregate query results - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_ATTR_UNDEFINED

Description: Query Master/Worker found undefined attribute in Query XML - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_BAD_RESULT_STATUS

Description: Bad Query Result Status

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_CACHE_GET_FAILED

Description: FortiSIEM Query Master failed to get cache results

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_CACHE_RESULT_GET_FAILED

Description: Query Master failed to get query results from its own cache - query will be resubmitted

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_CACHE_TRIGGER_EVENT_GET_FAILED

Description: Query Master failed to get trigger event query from Data Manager - Query Master will attempt to get trigger events from event database

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_CHAR_UNEXPECTED

Description: Query Master/Worker found unexpected character in expression in a Query XML - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_QUERY_CH_PARSE_FAILED

Description: Query Master failed to parse CLICKHOUSE query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_CH_POST_FAILED

Description: Query Master failed to post query to CLICKHOUSE

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
httpStatusCode	HTTP Status	string	

EventType: PH_QUERY_CLICKHOUSE_DATA_FAILED

Description: FortiSIEM ClickHouse DATA failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_CLICKHOUSE_EXEC_FAILED

Description: Failed to exec query from ClickHouse

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_CLICKHOUSE_STARTS

Description: ClickHouse query starts

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_CLICKHOUSE_STOP_FAILED

Description: Failed to stop ClickHouse query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_CLICKHOUSE_WAITING_QUEUE_FULL

Description: ClickHouse query waiting queue is full

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_COMMAND_BAD

Description: Internal error - unsupported query control command - expected Stop, pause and resume

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_COMPLETION_NOTIFICATION_SEND_FAILED

Description: Query Master failed to send query completion notification to App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_CONFIG_UNDEFINED

Description: Query Master/Worker found undefined phoenix_config item

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configName	Config Name	string	

EventType: PH_QUERY_CONVERT_FAILED

Description: Query Master/Worker failed to convert a particular query to certain format - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_DATA_ENUM_FAILED

Description: Query Master failed to enumerate inline report results for a particular report - inline report will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_DATA_MANAGER_NODES_GET_FAILED

Description: Query Master failed to get Data Manager IP addresses - queries will be done by Query Master until the next attempt to get this list of IP addresses

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_DATA_SEND_FAILED

Description: Query Master failed to send query-related data to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_DATA_SIZE_MISMATCH

Description: Query Master found size mismatch between two data entries while loading a particular inline query - this inline report will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_DATA_SIZE_UNEXPECTED

Description: Query Master found unexpected data size while returning results to App server - inline report will not have results

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_DATA_TYPE_UNEXPECTED

Description: Query Master found unexpected data types while returning results to App server - inline report will not have results

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_DB_SERVER_HOST_UNDEFINED

Description: Database server host not defined for query master

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configName	Config Name	string	

EventType: PH_QUERY_DIR_CREATE_FAILED

Description: Query Master/Worker/Data Manager failed to create directory

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_DIR_RENAME_FAILED

Description: Query Master/Worker/Data Manager failed to rename directory

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_DISTRIBUTION

Description: Query distribution (Worker IP: Workload)

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
oldDistrib	Old Distribution	string	Old Distribution is the profiled login distribution that is computed based on statistics from previous days. It is the probability mass function for the logins at various hours of the day and represented in a comma separated set of values, one for each hour. For each hour of the day (0 representing 12AM-1AM, 1 representing 1AM-2AM etc), the value represents the probability of login during that hour.
newDistrib	New Distribution	string	New Distribution is the login distribution for the current day. It is the probability mass function for the logins at various hours of the day and represented in a comma separated set of values, one for each hour. For each hour of the day (0 representing 12AM-1AM, 1 representing 1AM-2AM etc), the value represents the probability of login during that hour.

EventType: PH_QUERY_DURATION

Description: Query statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportName	Report Name	string	FortiSIEM report name.

EventType: PH_QUERY_ES_PARSE_FAILED

Description: Query Master failed to parse Elastic Search Summary query result - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_ES_POST_FAILED

Description: Query Master failed to provide Elastic Search Summary query results to App Server - query results will not be available

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
httpStatusCode	HTTP Status	string	

EventType: PH_QUERY_ES_SCROLL_FAILED

Description: ES Query scroll failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_EVENT_COLLECTOR_UNAVAILABLE

Description: Query Master/Worker failed to get event collector for a particular query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_EVENT_ID_GET_FAILED

Description: Query Master failed to get triggered event ID for a particular triggered event query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventId	Event ID	uint64	This is a globally unique ID assigned to every raw event ingested into the SIEM. This is used by the system for tying events to incidents, and is typically not needed by end users.
queryId	Query Id	string	

EventType: PH_QUERY_EVENT_PARSE_FAILED

Description: Query Master failed to parse events from Data Manager - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.
queryId	Query Id	string	

EventType: PH_QUERY_EVENT_PAYLOAD_READ_FAILED

Description: Query Master failed to read events - some real time events may be missed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_EXCEPTION_CAUGHT

Description: Query Worker encountered corrupt event index or data - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_EXPORT_TASK_CREAT_FAILED

Description: FortiSIEM Query Engine failed to export query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_QUERY_EXPORT_TASK_INSERT_FAILED

Description: FortiSIEM Query Engine failed to start query result export task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_QUERY_EXPR_INCOMPLETE

Description: Query Master failed to handle Query XML during internal processing- Incomplete expression

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_QUERY_FILE_CONTENT_BAD

Description: Query Master / Worker found invalid content in Query XML file - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_FILE_CONTENT_MISSING

Description: Query Master / Worker found certain content missing in Query XML file - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_FILE_COPY_FAILED

Description: Query Master failed to copy query XML file from completed/active to eventdb directory - XXX

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_CORRUPT

Description: Query Master found corrupt query status file for a particular query - query will not be completed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_FILE_CREATE_FAILED

Description: Query Master / Worker failed to create query result file - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_EMPTY

Description: Query Master/Worker found empty query status backup file - system loses redundancy for this query

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_FILE_HEADER_GET_FAILED

Description: Query Master failed to read query related file header from query result file - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_FILE_LINK_FAILED

Description: Query Master / Worker failed to hard link query result file - query cache will not be used

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_MAGIC_BAD

Description: Query Master found bad query-related file magic inside query status or result file - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_FILE_MMAP_FAILED

Description: Query Master failed to memory-map summary event cache file - summary event query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_NAME_BAD

Description: Query Master found invalidly formatted summary event cache file - summary event query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_FILE_OPEN_FAILED

Description: Query Master / Worker/ Data Manager failed to open query related file - related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_READ_FAILED

Description: Query Master / Worker/ Data Manager failed to read query related file - related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_REMOVE_FAILED

Description: Query Master failed to remove cached query result file - disk may eventually get full

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FILE_SEEK_FAILED

Description: Query Master failed to seek trend file to offset for a specific inline report - that inline report will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.

EventType: PH_QUERY_FILE_STAT_FAILED

Description: Query Master / Worker/ Data Manager failed to stat query related file - related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_FORMAT_UNSUPPORTED

Description: Query Master received unsupported report export file format from App Server - export will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_FUNC_ERROR

Description: Query Master / Worker encountered internal function error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_ID_DUPLICATE

Description: Query Master / Worker encountered duplicate query ID assigned by App server - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_ID_INACTIVE

Description: Query Master / Worker failed to retrieve supposedly active query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_ID_NOT_FOUND

Description: Query Master / Worker failed to find Query ID not found in task queue - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_ID_REMOVE_FAILED

Description: Query Master failed to remove trigger event query ID from task queue - partial results will be returned

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_ID_UNSUPPORTED

Description: Query Master found unsupported query type hint from App Server - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_INLINEREQUEST_BAD

Description: Query Master received bad inline query request via TCP socket - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_IPC_EVENT_SEND_FAILED

Description: Query Master failed to send IPC event (containing heartbeat data) to Data Manager - trigger event queries may be slow

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_QUERY_IP_GET_FAILED

Description: Query Master failed to get Supervisor IP - Query Master will not be able to communicate with Super data Manager

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_QUERY_IP_INVALID

Description: Query Worker got invalid Query Master IP - queries will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_QUERY_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_LOGINTEGRITYEXPORT_TASK_CREAT_FAILED

Description: Data Manager failed to create task for exporting log integrity check request from App Server - request will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_LOGINTEGRITYEXPORT_TASK_INSERT_FAILED

Description: Data Manager failed to insert task for exporting log integrity check request from App Server into internal task queue - request will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_LOG_INTEGRITY_EXPORT_DIR_UNCONFIGURED

Description: Query Master failed to obtain log integrity export directory - particular request will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_LOG_INTEGRITY_EXPORT_FAILED

Description: Query Master failed to export bad event blocks from file - log integrity query from App server will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_LONG_RUNNING_STOPPED

Description: Long running query stopped

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
reportName	Report Name	string	FortiSIEM report name.

EventType: PH_QUERY_MEM_ALLOC_FAILED

Description: Query Master / Worker failed to allocate memory during event / rule processing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_QUERY_MESSAGE_SEND_FAILED

Description: FortiSIEM Query Engine failed to send message

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
type	Type	string	
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_QUERY_MODULE_INIT_FAILED

Description: Query Master / Worker module failed to initialize

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_MODULE_UNCONFIGURED

Description: Query Master / Worker module failed to obtain some parameters during phoenix_config.txt during initialization - module likely will not start

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	

EventType: PH_QUERY_ONLINE_WORKER_CHANGED

Description: FortiSIEM Online Query Worker number changed

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_QUERY_PARSED_EVENT_LOAD_FAILED

Description: Query Worker failed to load parsed event from shared buffer during real time query which may not show events from this Query Worker node

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_PARTIAL_WORKER_FAILURE

Description: Partial query results due to worker failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
reportName	Report Name	string	FortiSIEM report name.

EventType: PH_QUERY_PCAP_FINALIZE_FAILED

Description: Query Master failed to finalize pcap export - export will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_PCAP_LOAD_FAILED

Description: Query Master failed to load query results in pcap format - results will not be complete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.

EventType: PH_QUERY_PCAP_RENAME_FAILED

Description: Query Master failed to rename pcap file - export will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_QUERY_PCAP_TRANSFER_FAILED

Description: Query Master failed to transfer event to pcap packet - results will not be complete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.

EventType: PH_QUERY_PGDB_EXEC_SQL_FAILED

Description: Query Master failed to execute SQL statement against Supervisor Postgres DB for Incident Query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbQuery	Database Query	string	

EventType: PH_QUERY_PGDB_RECONNECT_FAILED

Description: Query Master failed to reconnect to Supervisor Postgres DB - Query Master will remain disconnected and all incident queries will fail

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_QUERY_PGDB_SQL_GET_VAL_FAILED

Description: Query Master failed to get column value from SQL result - incident query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_POST_FILTER_PARSE_FAILED

Description: Query Master failed to parse post-filter inline query results - no post-filtering is going to occur

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id		Display name	Type	Description
task		Task	string	

EventType: PH_QUERY_PQ_ERROR

Description: FortiSIEM Postgres DB connection or execution error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id		Display name	Type	Description
funName		Function Name	string	
errorString		Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_PROCESS_GET_FAILED

Description: Query Master failed to get its own parent process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_PROFILE_ATTR_UNSPECIFIED

Description: Query Master failed to find specified attribute in Profile Query XML from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_PROFILE_EVENT_TYPE_ERROR

Description: Query Master encountered unexpected event type in a Profile Query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_PROFILE_FUNCTION_ERROR

Description: Query Master hit Function error while executing Profile Query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_PROFILE_NOT_MARKED_AS_BASELINE

Description: Query Master will not execute a profile query since it is not marked as baseline

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_PROGRESS_REJECTED

Description: Query Worker fails to upload query progress to Query Master - some progress reporting will be skipped

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
httpStatusCode	HTTP Status	string	

All Logs Page 5

Every FortiSIEM internally generated event log regardless of category

- PH_QUERY_REPORTEXPORT_TASK_CREAT_FAILED
- PH_QUERY_REPORTEXPORT_TASK_INSERT_FAILED
- PH_QUERY_REPORT_RESULTS_LOAD_FAILED
- PH_QUERY_REPORT_RESULTS_POST_FILTER_FAILED
- PH_QUERY_REPORT_RESULT_FILE_NOT_EXIST
- PH_QUERY_REQUEST_BAD
- PH_QUERY_RESULT_FILES_MERGE_FAILED
- PH_QUERY_RESULT_GET_FAILED
- PH_QUERY_RESULT_NOT_READY
- PH_QUERY_RESULT_PARSE_FAILED
- PH_QUERY_RESULT_REJECTED
- PH_QUERY_RESULT_SAVE_FAILED
- PH_QUERY_RESULT_UPLOAD_FAILED
- PH_QUERY_RT_ERROR
- PH_QUERY_SORT_SPEC_GET_FAILED
- PH_QUERY_START_FAILED
- PH_QUERY_STATE_BAD
- PH_QUERY_STATUS_LOAD_FAILED
- PH_QUERY_STATUS_SAVE_FAILED
- PH_QUERY_SUMM_ATTR_BAD
- PH_QUERY_SUMM_ATTR_MISSING
- PH_QUERY_SUMM_ATTR_UPDATE_FAILED
- PH_QUERY_SUMM_COLUMN_UNSUPPORTED
- PH_QUERY_SUMM_EVENT_SKIPPED
- PH_QUERY_SUMM_PARSE_FAILED
- PH_QUERY_SUMM_PERF_ETINFO_UNSUPPORTED
- PH_QUERY_TASK_INVALID
- PH_QUERY_TASK_REROUTED
- PH_QUERY_TASK_REROUTE_FAILED
- PH_QUERY_VALUE_TYPE_UNSUPPORTED
- PH_QUERY_WORKERS_GET_FAILED
- PH_QUERY_WORKERS_SPLIT_AMONG_FAILED
- PH_QUERY_WORKER_CHANGED_TO_OFFLINE
- PH_QUERY_WORKER_CHANGED_TO_ONLINE
- PH_QUERY_XML_PARSE_FAILED
- PH_READER_BLOCK_WRITE
- PH_REPORT_ACTION_STATUS

- PH_REPORT_ACT_FAILED
- PH_REPORT_AGGR_FIELDS_EMPTY
- PH_REPORT_AGGR_FIELD_NOT_ADDED
- PH_REPORT_AGGR_FUNC_EMPTY
- PH_REPORT_AGGR_TYPE_ERROR
- PH_REPORT_AGGR_TYPE_UNDEFINED
- PH_REPORT_ATTR_ID_UNSUPPORTED
- PH_REPORT_ATTR_MISSING
- PH_REPORT_ATTR_UNDEFINED
- PH_REPORT_BUFFER_OVERFLOW
- PH_REPORT_CHECKSUM_MISMATCH
- PH_REPORT_CONFIG_UPDATE_NULL
- PH_REPORT_CONVERT_FAILED
- PH_REPORT_DATA_INIT_FAILED
- PH_REPORT_DATA_SIZE_MISMATCH
- PH_REPORT_DATA_SIZE_OVERFLOW
- PH_REPORT_DATA_SIZE_UNEXPECTED
- PH_REPORT_DATA_SIZE_UNKNOWN
- PH_REPORT_DATA_TYPE_UNEXPECTED
- PH_REPORT_DIR_CREATE_FAILED
- PH_REPORT_DIR_OPEN_FAILED
- PH_REPORT_DIR_REMOVE_FAILED
- PH_REPORT_ES_BUCKETS_EMPTY
- PH_REPORT_ES_POST_FAILED
- PH_REPORT_ES_PROFILE_EMPTY
- PH_REPORT_ES_PROFILE_TIMEOUT
- PH_REPORT_ES_PURGE_INDEX_FAILED
- PH_REPORT_ES_TIME_RANGE_INVALID
- PH_REPORT_EXPR_PARSE_FAILED
- PH_REPORT_FILE_CONTENT_MISSING
- PH_REPORT_FILE_COPY_FAILED
- PH_REPORT_FILE_HEADER_BAD
- PH_REPORT_FILE_INIT_FAILED
- PH_REPORT_FILE_LINK_FAILED
- PH_REPORT_FILE_MAGIC_BAD
- PH_REPORT_FILE_MMAP_FAILED
- PH_REPORT_FILE_NAME_BAD
- PH_REPORT_FILE_OPEN_FAILED
- PH_REPORT_FILE_PARSE_FAILED
- PH_REPORT_FILE_READ_FAILED
- PH_REPORT_FILE_REMOVE_FAILED
- PH_REPORT_FILE_RENAME_FAILED
- PH_REPORT_FILE_RSYNC_FAILED

- PH_REPORT_FILE_STAT_FAILED
- PH_REPORT_FILE_TYPE_UNKNOWN
- PH_REPORT_FILE_UNSPECIFIED
- PH_REPORT_FILE_WRITE_FAILED
- PH_REPORT_FUNC_OBJ_DEF_ERROR
- PH_REPORT_FUNC_OBJ_DEF_GET_FAILED
- PH_REPORT_FUNC_OBJ_DEF_UNKNOWN
- PH_REPORT_ID_LOC_DEVICE_EXCLUDED_INVALID
- PH_REPORT_ID_LOC_EVENT_SEND_FAILED
- PH_REPORT_ID_LOC_RESULT_UPLOAD_FAILED
- PH_REPORT_ID_LOC_SYNCH_DATA_UPLOAD_FAILED
- PH_REPORT_ID_LOC_USER_ALREADY_EXCLUDED
- PH_REPORT_ID_LOC_USER_EXCLUDE_FAILED
- PH_REPORT_INDEX_OVERFLOW
- PH_REPORT_IP_GET_FAILED
- PH_REPORT_IP_TYPE_INVALID
- PH_REPORT_KEY_LOAD_FAILED
- PH_REPORT_MODULE_INIT_FAILED
- PH_REPORT_MODULE_UNCONFIGURED
- PH_REPORT_OLD_REPORT_DATA
- PH_REPORT_OP_UNEXPECTED
- PH_REPORT_ORDER_BY_ATTR_EMPTY
- PH_REPORT_ORDER_BY_INVALID
- PH_REPORT_PACK_FAILED
- PH_REPORT_PACK_FAILED_COUNT
- PH_REPORT_PARSED_EVENT_LOAD_FAILED
- PH_REPORT_PGDB_CONNECT_FAILED
- PH_REPORT_PGDB_EXEC_FAILED
- PH_REPORT_PGDB_NOT_CONNECTED
- PH_REPORT_PGDB_NOT_INIT
- PH_REPORT_POINTER_NULL
- PH_REPORT_POINTER_NULL_WARNING
- PH_REPORT_POSITIVE_INTEGER_EXPECTED
- PH_REPORT_PQ_ERROR
- PH_REPORT_PROFILE_TYPE_BAD
- PH_REPORT_PROFILE_TYPE_WRONG_FORMAT
- PH_REPORT_PROFILE_UPDATE_FAILED
- PH_REPORT_ROW_LENGTH_ZERO
- PH_REPORT_RULE_ATTR_MISSING
- PH_REPORT_SCHEMA_INCOMPATIBLE
- PH_REPORT_SCHEMA_INVALID
- PH_REPORT_SCHEMA_LOAD_FAILED
- PH_REPORT_SQLITE3_BATCH_BEGIN_FAILED

- PH_REPORT_SQLITE3_BATCH_COMMIT_FAILED
- PH_REPORT_SQLITE3_BIND_VALUE_FAILED
- PH_REPORT_SQLITE3_BUSY
- PH_REPORT_SQLITE3_BUSY_TIMEOUT_ERROR
- PH_REPORT_SQLITE3_CHECKPOINT_FAILED
- PH_REPORT_SQLITE3_COMMIT_ERROR
- PH_REPORT_SQLITE3_CONFIG_FAILED
- PH_REPORT_SQLITE3_ENABLE_SHARED_CACHE_FAILED
- PH_REPORT_SQLITE3_EXEC_FAILED
- PH_REPORT_SQLITE3_EXTENDED_RESULT_CODES_ERROR
- PH_REPORT_SQLITE3_OPEN_FAILED
- PH_REPORT_SQLITE3_PREPARE_ERROR
- PH_REPORT_SQLITE3_PROFILE_ENTRY_DELETE_FAILED
- PH_REPORT_SQLITE3_PROFILE_NOT_FOUND
- PH_REPORT_SQLITE3_STEP_ERROR
- PH_REPORT_UNPACK_FAILED
- PH_REPORT_VALUE_TYPE_LOOKUP_BY_ID_FAILED
- PH_REPORT_VALUE_TYPE_LOOKUP_BY_NAME_FAILED
- PH_REPORT_VALUE_TYPE_OF_ID_UNEXPECTED
- PH_REPORT_VALUE_TYPE_OF_NAME_UNEXPECTED
- PH_REPORT_VALUE_TYPE_OF_STAT_UNEXPECTED
- PH_REPORT_VALUE_TYPE_UNSUPPORTED
- PH_REPORT_WORKER_UPLOAD_FAILED
- PH_REPORT_XML_ELEMENT_DUPLICATE
- PH_REPORT_XML_ELEMENT_MISSING
- PH_REPORT_XML_ELEMENT_PARSE_FAILED
- PH_REPORT_XML_PARSE_FAILED
- PH_REPORT_ZLIB_COMPRESSION_TYPE_UNKNOWN
- PH_REPORT_ZLIB_UNCOMPRESS_FAILED
- PH_RULEMASTER_TEST_RULES_CHECK_SYNTAX
- PH_RULEMASTER_TEST_RULES_FINALIZE_STATE
- PH_RULEMASTER_TEST_RULES_UPDATE_STATE
- PH_RULEMOD_AGGREGATOR_EMPTY
- PH_RULEMOD_ARITH_OP_ILLEGAL
- PH_RULEMOD_ATTR_ALREADY_ASSOCIATED
- PH_RULEMOD_ATTR_ID_LOOKUP_BY_NAME_FAILED
- PH_RULEMOD_ATTR_ID_UNDEFINED
- PH_RULEMOD_ATTR_MISSING
- PH_RULEMOD_ATTR_NAME_LOOKUP_BY_ID_FAILED
- PH_RULEMOD_ATTR_UNDEFINED
- PH_RULEMOD_BUFFER_EMPTY
- PH_RULEMOD_CLEAR_CONDITION_INVALID
- PH_RULEMOD_CLEAR_CONDITION_SET_FAILED

- PH_RULEMOD_CONFIG_UNDEFINED
- PH_RULEMOD_CONSTRUCTOR_ERROR
- PH_RULEMOD_CUST_ID_LIST_INVALID
- PH_RULEMOD_DATA_REQUEST_PARSE_FAILED
- PH_RULEMOD_DATA_SIZE_OVERFLOW
- PH_RULEMOD_DATA_UNSUPPORTED
- PH_RULEMOD_DB_SERVER_HOST_UNDEFINED
- PH_RULEMOD_DIR_OPEN_FAILED
- PH_RULEMOD_ENCODE_FAILED
- PH_RULEMOD_ENTITY_VERSION_MISSING
- PH_RULEMOD_EVENT_TYPE_GROUP_INVALID
- PH_RULEMOD_EVENT_TYPE_NOT_FOUND
- PH_RULEMOD_EXCEPTION_ELEMENT_INVALID
- PH_RULEMOD_EXPR_EVAL_UNKNOWN
- PH_RULEMOD_EXPR_PARSE_FAILED
- PH_RULEMOD_EXPR_UNSUPPORTED
- PH_RULEMOD_FILE_OPEN_FAILED
- PH_RULEMOD_FILE_UNSPECIFIED
- PH_RULEMOD_FORMAT_ERROR
- PH_RULEMOD_FUNC_NOT_FOUND
- PH_RULEMOD_FUNC_PARSE_FAILED
- PH_RULEMOD_GLOBAL_CONSTRAINT_INVALID
- PH_RULEMOD_GROUPBY_LIST_INVALID
- PH_RULEMOD_GROUPBY_LIST_NOT_FOUND
- PH_RULEMOD_GROUP_EVENT_CONSTRAINT_INVALID
- PH_RULEMOD_ID_LOOKUP_BY_INCIDENT_FAILED
- PH_RULEMOD_INCIDENT_ARG_INVALID
- PH_RULEMOD_INCIDENT_CACHE_NOT_FOUND
- PH_RULEMOD_INCIDENT_DEF_INVALID
- PH_RULEMOD_INCIDENT_NOT_FOUND
- PH_RULEMOD_INCIDENT_REPORT_SEND_FAILED
- PH_RULEMOD_INDEX_OVERFLOW
- PH_RULEMOD_INFO_GET_FAILED
- PH_RULEMOD_IP_GET_FAILED
- PH_RULEMOD_IP_INVALID
- PH_RULEMOD_IP_TYPE_INVALID
- PH_RULEMOD_LOAD_METHOD_UNDEFINED
- PH_RULEMOD_MEM_ALLOC_FAILED
- PH_RULEMOD_MODULE_INIT_FAILED
- PH_RULEMOD_MUTEX_ACQUIRE_FAILED
- PH_RULEMOD_NOTIF_CONNECTION_FAILED
- PH_RULEMOD_OBJ_GET_FROM_SUBPATTERN_FAILED
- PH_RULEMOD_OBJ_LOAD_FAILED

- PH_RULEMOD_OP_NOT_FUNC
- PH_RULEMOD_OP_UNKNOWN
- PH_RULEMOD_PARSED_EVENT_LOAD_FAILED
- PH_RULEMOD_PQ_ERROR
- PH_RULEMOD_PROFILE
- PH_RULEMOD_REM_BY_ZERO
- PH_RULEMOD_REM_BY_ZEROD
- PH_RULEMOD_SELECT_ATTR_PARSE_FAILED
- PH_RULEMOD_SELECT_SPEC_PARSE_FAILED
- PH_RULEMOD_SINGLE_EVENT_CONSTRAINT_INVALID
- PH_RULEMOD_SUBPATTERN_INVALID
- PH_RULEMOD_SUBPATTERN_MISSING
- PH_RULEMOD_SUBPATTERN_MORE_THAN_ONE
- PH_RULEMOD_SUBPATTERN_UNDEFINED
- PH_RULEMOD_SUMMARY_UPLOAD_FAILED
- PH_RULEMOD_THREAD_SPAWN_FAILED
- PH_RULEMOD_TOKEN_UNDEFINED
- PH_RULEMOD_TOKEN_UNEXPECTED
- PH_RULEMOD_UNPACK_FAILED
- PH_RULEMOD_VALUE_TYPE_UNEXPECTED
- PH_RULEMOD_XML_ELEMENT_EMPTY
- PH_RULEMOD_XML_ELEMENT_MISSING
- PH_RULEMOD_XML_ELEMENT_PARSE_FAILED
- PH_RULEMOD_XML_ELEMENT_UNEXPECTED
- PH_RULEMOD_XML_ELEMENT_UNKNOWN
- PH_RULEMOD_XML_LOAD_FAILED
- PH_RULEMOD_XML_PARSE_FAILED
- PH_RULEMOD_XML_POINTER_NULL
- PH_RULEWORKER_TEST_RULES_CHECK_SYNTAX
- PH_RULEWORKER_TEST_RULES_EVENT_MATCH_STATUS
- PH_Rule_AbuseCH_Botnetc2_MalwareIP_Inbound
- PH_Rule_AbuseCH_Botnetc2_MalwareIP_Outbound
- PH_Rule_Blocklist_MalwareIP_Inbound
- PH_Rule_Blocklist_MalwareIP_Outbound
- PH_Rule_C2_Tracker_MalwareIP_Inbound
- PH_Rule_C2_Tracker_MalwareIP_Outbound
- PH_Rule_CINSScore_MalwareIP_Inbound
- PH_Rule_CINSScore_MalwareIP_Outbound
- PH_Rule_CertPL_MalwareDomain_Inbound
- PH_Rule_CertPL_MalwareDomain_Outbound
- PH_Rule_Cisco_Talos_MalwareIP_Inbound
- PH_Rule_Cisco_Talos_MalwareIP_Outbound
- PH_Rule_Cluster_DBLeader_Changed

- PH_Rule_Cluster_REPL_Leader_Changed
- PH_Rule_DigitalSide_MalwareDomain_Inbound
- PH_Rule_DigitalSide_MalwareDomain_Outbound
- PH_Rule_DigitalSide_MalwareIP_Inbound
- PH_Rule_DigitalSide_MalwareIP_Outbound
- PH_Rule_DigitalSide_MalwareURL_Outbound
- PH_Rule_FML_Antispam_Malicious_File
- PH_Rule_FML_Antispam_Malicious_Url
- PH_Rule_FireHol_MalwareIP_Inbound
- PH_Rule_FireHol_MalwareIP_Outbound
- PH_Rule_FortiRecon_MalwareDomain_Inbound
- PH_Rule_FortiRecon_MalwareDomain_Outbound
- PH_Rule_FortiRecon_MalwareIP_Inbound
- PH_Rule_FortiRecon_MalwareIP_Outbound
- PH_Rule_FortiRecon_MalwareURL_Outbound
- PH_Rule_FortiSOAR_MalwareDomain_Inbound
- PH_Rule_FortiSOAR_MalwareDomain_Outbound
- PH_Rule_FortiSOAR_MalwareIP_Inbound
- PH_Rule_FortiSOAR_MalwareIP_Outbound
- PH_Rule_FortiSOAR_MalwareURL_Outbound
- PH_Rule_Greensnow_MalwareIP_Inbound
- PH_Rule_Greensnow_MalwareIP_Outbound
- PH_Rule_IPSum_MalwareIP_Inbound
- PH_Rule_IPSum_MalwareIP_Outbound
- PH_Rule_MISP_MalwareDomain_Inbound
- PH_Rule_MISP_MalwareDomain_Outbound
- PH_Rule_MISP_MalwareIP_Inbound
- PH_Rule_MISP_MalwareIP_Outbound
- PH_Rule_MISP_MalwareURL_Outbound
- PH_Rule_Mandiant_MalwareDomain_Inbound
- PH_Rule_Mandiant_MalwareDomain_Outbound
- PH_Rule_Mandiant_MalwareIP_Inbound
- PH_Rule_Mandiant_MalwareIP_Outbound
- PH_Rule_Mandiant_MalwareURL_Outbound
- PH_Rule_OPENCTI_MalDomain_Inbound
- PH_Rule_OPENCTI_MalDomain_Outbound
- PH_Rule_OPENCTI_MalwareIP_Inbound
- PH_Rule_OPENCTI_MalwareIP_Outbound
- PH_Rule_OPENCTI_MalwareURL_Outbound
- PH_Rule_OpenPhish_MalwareURL_Outbound
- PH_Rule_Proofpoint_MalwareIP_Inbound
- PH_Rule_Proofpoint_MalwareIP_Outbound
- PH_Rule_Snort_MalwareIP_Inbound

- PH_Rule_Snort_MalwareIP_Outbound
- PH_Rule_ThreatFox_MalwareURL_Outbound
- PH_Rule_TweetFeed_MalwareDomain_Inbound
- PH_Rule_TweetFeed_MalwareDomain_Outbound
- PH_Rule_TweetFeed_MalwareURL_Outbound
- PH_Rule_Tweetfeed_MalwareIP_Inbound
- PH_Rule_Tweetfeed_MalwareIP_Outbound
- PH_SAAS_OP_COLLECTOR_DOWN
- PH_SAAS_OP_COLLECTOR_UP
- PH_SCHEDULED_RULE_QUERY_FAILED
- PH_SER_MON_SERVICE_DOWN
- PH_SHAREDSTORE_ACQUIRE_ERROR
- PH_SHAREDSTORE_WRITER_POS_UNEXPECTED_ALTERED
- PH_SHAREDSTORE_WRITE_ERROR
- PH_SSL_SHUTDOWN_ERROR
- PH_STM_ACCOUNT_UNMATCHED
- PH_STM_AUTH_TYPE_UNKNOWN
- PH_STM_BAD_ELEM
- PH_STM_BAD_ELEM_VALUE
- PH_STM_BAD_PORT
- PH_STM_BAD_RTT_LINE
- PH_STM_BAD_SSL
- PH_STM_BAD_TAG
- PH_STM_CMD_EXEC_FAILED
- PH_STM_CRED_INVALID
- PH_STM_CURL_ESCAPE_FAILED
- PH_STM_CURL_INIT_FAILED
- PH_STM_DNS_TYPE_UNSUPPORTED
- PH_STM_DUPLICATED
- PH_STM_ELEM_EMPTY
- PH_STM_ELEM_MISSING
- PH_STM_ELEM_NEGATIVE
- PH_STM_ERROR
- PH_STM_FILE_OPEN_FAILED
- PH_STM_GET_HOST_FAILED
- PH_STM_GUESS_TYPE_FAILED
- PH_STM_HTTP_RESP_FAILED
- PH_STM_METHOD_UNKNOWN
- PH_STM_MONITOR_MISSING_ACTION
- PH_STM_MONITOR_RESULT_UPLOAD_FAILED
- PH_STM_NO_ORACLE_NAME
- PH_STM_PORT_UNKNOWN
- PH_STM_PROCESS_INVOKE_FAILED

- PH_STM_PROTO_UNKNOWN
- PH_STM_PROTO_UNSUPPORT
- PH_STM_SERVER_ADDR_INVALID
- PH_STM_SPECIAL_LINE_NOT_FOUND
- PH_STM_STM_GET_PROCESS_FAILED
- PH_STM_STM_GET_PROCESS_NAME_FAILED
- PH_STM_TAG_MISSING
- PH_STM_TAG_NOT_FOUND
- PH_STM_TAG_UNKNOWN
- PH_STM_TRACEROUTE_FAILED
- PH_STM_XML_PARSE_FAILED
- PH_SYSTEM_ARCHIVE_LOW
- PH_SYSTEM_ARCHIVE_PURGED_LOW_SPACE
- PH_SYSTEM_ARCHIVE_PURGED_POLICY
- PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_FAILED
- PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_FINISHED
- PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_STARTED
- PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_SUCCESS
- PH_SYSTEM_ARCHIVE_PURGING_POLICY_FAILED
- PH_SYSTEM_ARCHIVE_PURGING_POLICY_FINISHED
- PH_SYSTEM_ARCHIVE_PURGING_POLICY_STARTED
- PH_SYSTEM_ARCHIVE_PURGING_POLICY_SUCCESS
- PH_SYSTEM_ARCHIVE_RETENTION_POLICY_VIOLATED
- PH_SYSTEM_ARCHIVE_USAGE
- PH_SYSTEM_DATAMGR_ARCHIVE_SKIP
- PH_SYSTEM_DEVAPP_EVENTS_PER_SEC
- PH_SYSTEM_DEVAPP_NO_EVENTS
- PH_SYSTEM_DEVICE_NO_EVENTS
- PH_SYSTEM_DISK_ARCHIVING_FAILED
- PH_SYSTEM_DISK_ARCHIVING_FINISHED
- PH_SYSTEM_DISK_ARCHIVING_STARTED
- PH_SYSTEM_DISK_ARCHIVING_SUCCESS
- PH_SYSTEM_DISK_PURGED
- PH_SYSTEM_DISK_PURGING_FAILED
- PH_SYSTEM_DISK_PURGING_FINISHED
- PH_SYSTEM_DISK_PURGING_STARTED
- PH_SYSTEM_DISK_PURGING_SUCCESS
- PH_SYSTEM_DISK_USAGE
- PH_SYSTEM_DISK_USAGE_EXCEED_LICENSE
- PH_SYSTEM_DISK_USAGE_WARNING
- PH_SYSTEM_DROP_UNKNOWN_ORG
- PH_SYSTEM_EPS_GLOBAL
- PH_SYSTEM_EPS_NODE

- PH_SYSTEM_EPS_ORG
- PH_SYSTEM_EVENTS_FWD_STAT
- PH_SYSTEM_EVENTS_PER_SEC
- PH_SYSTEM_EVENTS_VIA_ZMQ_EPS
- PH_SYSTEM_EVENT_RATE_EXCEED_LICENSE
- PH_SYSTEM_INTERNAL_EVENTS_PER_SEC
- PH_SYSTEM_IP_EVENTS_PER_SEC
- PH_SYSTEM_ONLINE_RETENTION_POLICY_VIOLATED
- PH_SYSTEM_PERF_EVENTS_PER_SEC
- PH_SYSTEM_RAW_EVENT_SIZE
- PH_SYSTEM_RETENTION_POLICY_EXEC_TIME
- PH_SYSTEM_RETENTION_POLICY_FAILED
- PH_SYSTEM_RETENTION_POLICY_FINISHED
- PH_SYSTEM_RETENTION_POLICY_STARTED
- PH_SYSTEM_RETENTION_POLICY_STATS
- PH_SYSTEM_RETENTION_POLICY_SUCCESS
- PH_SYSTEM_STORAGE_LOW
- PH_SYSTEM_STORED_EVENTS_PER_SEC
- PH_SYSTEM_SUMM_EVENTS_STORED_EPS
- PH_SYS_ERROR_XML_SEND_ERROR
- PH_SYS_ERROR_XML_SENT
- PH_TASK_DATA_EMPTY
- PH_TASK_DATA_IS_WRONG
- PH_TASK_FAILED
- PH_TASK_NOT_CONTAIN_LIC
- PH_TASK_NO_LICENSE
- PH_TASK_RUN_COMMAND_FAILED
- PH_TASK_SEND_FAILED
- PH_TASK_UNSUPPORT
- PH_TEST_CONN_COMPLETE
- PH_TEST_CONN_CONTACT_APP_SERVER
- PH_TEST_CONN_FAILED
- PH_TEST_CONN_FAILED_INVALID_REQUEST
- PH_TEST_CONN_FAILED_INVALID_REQUEST_XML
- PH_TEST_CONN_RECVD_VALID_REQUEST
- PH_TEST_CONN_RESULT_SENT
- PH_TEST_CONN_STARTED
- PH_TEST_RULES_PARSE_STATUS
- PH_THREAD_EXITING
- PH_THREAD_RECVD_EXIT
- PH_THREAD_STARTING
- PH_UNABLE_ACCESS_DIR
- PH_UNABLE_ALLOC_MEMORY

- PH_UNABLE_CREATE_DIR
- PH_UNABLE_CREATE_FILE
- PH_UNABLE_CREATE_TIMER
- PH_UNABLE_OPEN_DIR
- PH_UNABLE_OPEN_FILE
- PH_UNABLE_PARSE_XML
- PH_UNABLE_RENAME_FILE
- PH_UNRESOLVABLE_HOSTNAME
- PH_UNRESOLVABLE_IP
- PH_UPDATE_RULE_SUCCEED
- PH_USER_MON_SUDDEN_LOC_CHANGE
- PH_USER_MON_SUDDEN_LOGIN_DISTRIBUTION_CHANGE
- PH_USER_MON_SUDDEN_LOGIN_VOLUME_CHANGE
- PH_UTIL_BIZ_CHANGE_UPDATE_SPAWN_FAILURE
- PH_UTIL_BIZ_HTTP_REQUEST_FAILURE
- PH_UTIL_CMD_FAILURE
- PH_UTIL_CONFIG_IP_MISSING
- PH_UTIL_CONFIG_LOAD_FAILURE
- PH_UTIL_CONFIG_LOAD_FILE_ACCESS_FAILURE
- PH_UTIL_CONFIG_PARSE_FAILURE
- PH_UTIL_CONFIG_UNKNOWN_SERVER_TYPE
- PH_UTIL_CONNECTION_ERROR
- PH_UTIL_CSV_LINE_ILLEGAL
- PH_UTIL_CSV_READ_FAILURE
- PH_UTIL_CUSTOMER_COLLECTOR_MISSING
- PH_UTIL_CUSTOMER_COLLECTOR_PARSE_FAILURE
- PH_UTIL_CUSTOMER_DOMAIN_MISSING
- PH_UTIL_CUSTOMER_INFO_PARSE_FAILURE
- PH_UTIL_CUSTOMER_PARSE_FAILURE
- PH_UTIL_DASHBOARD_DUPLICATE_IP
- PH_UTIL_DASHBOARD_DUPLICATE_ITEM
- PH_UTIL_DASHBOARD_PARSE_FAILURE
- PH_UTIL_DEVICE_MAP_PROP_ERROR
- PH_UTIL_DEVICE_PROP_ERROR
- PH_UTIL_DEVICE_SIMPLE_PROP_PARSE_FAILURE
- PH_UTIL_DGA_FREQ_FILE_OPEN_FAILURE
- PH_UTIL_DGA_WHITELIST_FILE_OPEN_FAILURE
- PH_UTIL_DIR_CREATE_FAILURE
- PH_UTIL_DIR_CREATE_RETRIED
- PH_UTIL_DIR_OPEN_FAILURE
- PH_UTIL_DIR_PARENT_NOT_EXIST
- PH_UTIL_DIR_REMOVE_FAILURE
- PH_UTIL_DISK_USAGE_INFO_GET_FAILURE

- PH_UTIL_DISPATH_CMD_XML_ILLEGAL
- PH_UTIL_DISPATH_CMD_XML_PARSE_FAILURE
- PH_UTIL_EMAIL_SEND_FAILURE
- PH_UTIL_ETCD_COMPAGN_FAILED
- PH_UTIL_ETCD_GET_LEADER_FAILED
- PH_UTIL_ETCD_LEASE_FAILED
- PH_UTIL_ETCD_SET_FAILED
- PH_UTIL_EVENT_FILE_ERROR
- PH_UTIL_EVENT_GROUP_ERROR
- PH_UTIL_EVENT_STATUS_REPORTER_SPAWN_FAILURE
- PH_UTIL_EVENT_STATUS_UPLOAD_FAILURE
- PH_UTIL_EVENT_TYPE_ERROR
- PH_UTIL_FILE_NOT_EXIST
- PH_UTIL_FILE_OPEN_FAILURE
- PH_UTIL_FILE_READ_FAILURE
- PH_UTIL_FILE_SIZE_MISMATCH
- PH_UTIL_FILE_SIZE_TOO_SMALL
- PH_UTIL_FILE_STATFS_FAILURE
- PH_UTIL_FILE_STAT_FAILURE
- PH_UTIL_FILE_WRITE_FAILURE
- PH_UTIL_FORK_FAILURE
- PH_UTIL_GET_ADDR_FAILURE
- PH_UTIL_GET_ATTR_NAME_FAILED
- PH_UTIL_GET_JOB_STATUS_FAILURE
- PH_UTIL_HOSTNAME_GET_FAILURE
- PH_UTIL_INET_PTON_FAILURE
- PH_UTIL_INODE_INFO_GET_FAILURE
- PH_UTIL_INVALID_PARAM
- PH_UTIL_IOCTL_FAILURE
- PH_UTIL_IOCTL_SIOCGIFADDR_FAILURE
- PH_UTIL_IP_TYPE_INVALID
- PH_UTIL_IP_TYPE_MISMATCH
- PH_UTIL_JOB_STATUS_REPORTER_SPAWN_FAILURE
- PH_UTIL_JOB_STATUS_UPLOAD_FAILURE
- PH_UTIL_JSON_GET_NODE_FAILURE
- PH_UTIL_JSON_GET_TOTAL_COUNT_FAILURE
- PH_UTIL_JSON_OBJ_EMPTY
- PH_UTIL_JSON_PARSE_FAILURE
- PH_UTIL_KILLPG_FAILURE
- PH_UTIL_LOAD_EXT_FUNC_FILE_OPEN_FAILURE
- PH_UTIL_LOAD_EXT_FUNC_FORMAT_INVALID
- PH_UTIL_LOAD_EXT_FUNC_GET_NAME_FAILURE
- PH_UTIL_LOCAL_IP_MISSING

- PH_UTIL_LOOKUP_TABLES_DUPLICATE
- PH_UTIL_LOOKUP_TABLES_DUPLICATE_COLUMN
- PH_UTIL_LOOKUP_TABLES_DUPLICATE_KEY
- PH_UTIL_MAIL_CMD_RUN_FAILURE
- PH_UTIL_MAIL_SMTP_INIT_FAILURE
- PH_UTIL_MD5_ERROR
- PH_UTIL_MEM_ALLOC_FAILURE
- PH_UTIL_MKDTEMP_FAILURE
- PH_UTIL_MKSTEMP_FAILURE
- PH_UTIL_MMAP_FAILURE
- PH_UTIL_MOVE_FILE_FAILURE
- PH_UTIL_NOTIFICATION_SENDER_SPAWN_FAILURE
- PH_UTIL_NOTIFICATION_SERVER_INIT_FAILURE
- PH_UTIL_NOTIFICATION_UPLOAD_FAILURE
- PH_UTIL_PCRE_COMPILE_FAILED
- PH_UTIL_PHOENIX_CONFIG_ITEM_MISSING
- PH_UTIL_PIPE_FAILURE
- PH_UTIL_PROP_DEF_SET_PARSE_FAILURE
- PH_UTIL_REDIS_CONNECTION_ERROR
- PH_UTIL_REGEX_PATTERN_EMPTY
- PH_UTIL_REGEX_PATTERN_TOO_LONG
- PH_UTIL_SEND_DATA_FAILED
- PH_UTIL_SEND_TO_UDP_PORT_FAILURE
- PH_UTIL_SETPGRP_FAILURE
- PH_UTIL_SET_JOB_STATUS_FAILURE
- PH_UTIL_SOCKET_FAILURE
- PH_UTIL_STR_TO_IP_FAILURE
- PH_UTIL_SVN_DIFF_FAILURE
- PH_UTIL_SYS_ERROR_REPORTER_INIT_FAILURE
- PH_UTIL_TIME_RANGE_INVALID
- PH_UTIL_TIME_STR_FORMAT_INVALID
- PH_UTIL_TLS_SERVER_RECV_FAILED
- PH_UTIL_UNKNOWN_PHOENIX_ERROR_NUMBER
- PH_UTIL_VALUE_GROUP_ERROR
- PH_UTIL_WAITPID_FAILURE
- PH_UTIL_WAITPID_LAST_TRY_FAILURE
- PH_UTIL_WINDOWS_BID_LOAD_FAILURE
- PH_UTIL_WRITE_BIN_FILE_OPEN_FAILURE
- PH_UTIL_WRITE_FILE_OPEN_FAILURE
- PH_UTIL_XML_HANDLING_ERROR
- PH_UTIL_ZIP_DECOMPRESS_FAILED
- PH_VA_EVENTS_PER_SEC
- PH_VA_LICENSE_UPDATE

- [PH_VULN_LOAD_ERROR](#)
- [PH_VULN_UPDATE_ERROR](#)
- [PH_WORKER_DOWN](#)
- [PH_WORKER_PROVISION_FAILED](#)
- [PH_WORKER_UP](#)
- [PH_WS_COMM_ERROR](#)
- [WEBSense_MAIL_JDBC_PULL_STAT](#)
- [WEBSense_WEB_JDBC_PULL_STAT](#)

EventType: PH_QUERY_REPORTEXPORT_TASK_CREAT_FAILED

Description: Query Master failed to create task for exporting CSV/PCAP formatted Query request from App Server - export will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_REPORTEXPORT_TASK_INSERT_FAILED

Description: Query Master failed to insert task for exporting CSV/PCAP formatted Query request from App Server into internal task queue - export will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_REPORT_RESULTS_LOAD_FAILED

Description: Query Master failed to load inline query report results from file - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_REPORT_RESULTS_POST_FILTER_FAILED

Description: Query Master failed to post-filter inline query report results - no post-filtering is going to occur

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_REPORT_RESULT_FILE_NOT_EXIST

Description: Query report result file not exist

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_QUERY_REQUEST_BAD

Description: FortiSIEM Query Engine received bad request

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
queryId	Query Id	string	

EventType: PH_QUERY_RESULT_FILES_MERGE_FAILED

Description: Query Master failed to merge inline query result files - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_RESULT_GET_FAILED

Description: Query Master failed to produce inline query result / CSV export - operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.

EventType: PH_QUERY_RESULT_NOT_READY

Description: Query Master failed to find Query result directory for CSV export

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_RESULT_PARSE_FAILED

Description: Query Master failed to parse trigger event query result from Data Manager

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.
queryId	Query Id	string	

EventType: PH_QUERY_RESULT_REJECTED

Description: Query Master rejected query result upload from Query Worker

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
httpStatusCode	HTTP Status	string	

EventType: PH_QUERY_RESULT_SAVE_FAILED

Description: FortiSIEM Query Engine failed to save query result

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.

EventType: PH_QUERY_RESULT_UPLOAD_FAILED

Description: Query Worker failed to upload query result to Query Master - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
queryId	Query Id	string	
filePath	File Path	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_RT_ERROR

Description: Query Worker spawned excessive threads to handle real time search and will exit (delete)

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_QUERY_SORT_SPEC_GET_FAILED

Description: Query Master failed to get sort specification for cached query result - query will automatically rerun

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_START_FAILED

Description: Query Worker failed to start a query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.
queryId	Query Id	string	
reportName	Report Name	string	FortiSIEM report name.

EventType: PH_QUERY_STATE_BAD

Description: Query Master encounters invalid query state - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_STATUS_LOAD_FAILED

Description: Query Master failed to load query status from disk - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_STATUS_SAVE_FAILED

Description: Query Master failed to save query status to disk - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_SUMM_ATTR_BAD

Description: Query Master encountered bad attribute in Summary Dashboard data cache - cache will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_SUMM_ATTR_MISSING

Description: Query Master failed to locate an attribute in Summary Dashboard data cache - cache will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_SUMM_ATTR_UPDATE_FAILED

Description: Query Master failed to update certain host attribute in Summary Dashboard data cache - cache will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_QUERY_SUMM_COLUMN_UNSUPPORTED

Description: Query Master encountered unsupported attribute in Summary Dashboard data cache - cache will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_SUMM_EVENT_SKIPPED

Description: Query Master skipped a bad event for Summary Dashboard data cache - performance metrics will be partially updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_SUMM_PARSE_FAILED

Description: Query Master failed to parse Summary Dashboard Query XML - one query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_QUERY_SUMM_PERF_ETINFO_UNSUPPORTED

Description: Query Master encountered unsupported perfETInfo in Summary Dashboard Query - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_TASK_INVALID

Description: FortiSIEM Query task and worker IP are not matched

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
clientIpAddr	Client IP	IP	

EventType: PH_QUERY_TASK_REROUTED

Description: FortiSIEM Query task is rerouted

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_QUERY_TASK_REROUTE_FAILED

Description: FortiSIEM Query Task Reroute failed

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_VALUE_TYPE_UNSUPPORTED

Description: FortiSIEM Query Engine encountered bad value type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_QUERY_WORKERS_GET_FAILED

Description: Query Master failed to get the list of query workers - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_QUERY_WORKERS_SPLIT_AMONG_FAILED

Description: Query Master failed to split query among workers - query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_QUERY_WORKER_CHANGED_TO_OFFLINE

Description: FortiSIEM Query Worker Status Changed from online to offline

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_QUERY_WORKER_CHANGED_TO_ONLINE

Description: FortiSIEM Query Worker Status Changed from offline to online

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_QUERY_XML_PARSE_FAILED

Description: Query Master / Worker failed to parse query XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_READER_BLOCK_WRITE

Description: Reader is blocking writer&Restart

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptProcName	Reported Process Name	string	

EventType: PH_REPORT_ACTION_STATUS

Description: Record action result for report notification

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ACT_FAILED

Description: Query Master/Query Worker/Report Worker/Report Loader failed to perform requested ACTION from App Server, i.e. UPDATE, REMOVE. Event Role will not be updated.

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
roleId	Role ID	uint32	

EventType: PH_REPORT_AGGR_FIELDS_EMPTY

Description: Report Master/Report Worker encountered empty aggregate fields. Report file will be incomplete

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_REPORT_AGGR_FIELD_NOT_ADDED

Description: Query Master/Report Master/Report Worker failed to add certain aggregate field to report schema. The schema will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_AGGR_FUNC_EMPTY

Description: Report Master/Report Worker encountered empty aggregate function. Report file will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_AGGR_TYPE_ERROR

Description: Report Master/Report Worker encountered aggregate type error. Report file will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_AGGR_TYPE_UNDEFINED

Description: Report Master/Report Worker encountered undefined aggregate type. Report file will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ATTR_ID_UNSUPPORTED

Description: Report Master/Report Worker encountered unsupported attribute ID. Report file will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ATTR_MISSING

Description: Report Master/Report Worker failed to locate certain attribute. Report file will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ATTR_UNDEFINED

Description: Report Master/Report Worker encountered undefined attribute. Report file will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_BUFFER_OVERFLOW

Description: Report buffer overflow

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
size	Size	uint32	

EventType: PH_REPORT_CHECKSUM_MISMATCH

Description: Query Master encountered checksum mismatch in report results. The inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_CONFIG_UPDATE_NULL

Description: Report Worker/Report Loader encountered NULL object in config update. Config update will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_CONVERT_FAILED

Description: FortiSIEM internal error used for testing

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	

EventType: PH_REPORT_DATA_INIT_FAILED

Description: Query Master/Report Master failed to initialize report results block data. This inline query or report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_DATA_SIZE_MISMATCH

Description: Query Master/Report Master/Report Worker/Report Loader encountered size mismatch between two pieces of data. The affected operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_DATA_SIZE_OVERFLOW

Description: Query Master/Report Master/Report Worker/Report Loader encountered data size overflow. The affected operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_DATA_SIZE_UNEXPECTED

Description: Query Master/Report Master/Report Worker/Report Loader encountered unexpected data type. The affected operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_DATA_SIZE_UNKNOWN

Description: Query Master/Report Master/Report Worker/Report Loader encountered unknown data size. The affected operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_DATA_TYPE_UNEXPECTED

Description: Query Master/Report Master/Report Worker/Report Loader encountered unexpected data type. The affected operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_DIR_CREATE_FAILED

Description: FortiSIEM Report Engine failed to create directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_DIR_OPEN_FAILED

Description: FortiSIEM Report Engine failed to open directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_DIR_REMOVE_FAILED

Description: FortiSIEM Report Engine failed to remove directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_ES_BUCKETS_EMPTY

Description: Data Manager encountered empty Elastic Search buckets. Report data will not be written to disk

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ES_POST_FAILED

Description: Report Master/Report Worker failed to POST Elastic Search data to App Server. Report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
httpStatusCode	HTTP Status	string	

EventType: PH_REPORT_ES_PROFILE_EMPTY

Description: Report Master encountered empty Elastic Search profile. Report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_REPORT_ES_PROFILE_TIMEOUT

Description: Report Master encountered timeout in Elastic Search profile response. This profile will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_ES_PURGE_INDEX_FAILED

Description: Elastic Search Purge Inline Report Index Failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ES_TIME_RANGE_INVALID

Description: Report Master encountered invalid time range in Elastic Search profile query. This query will failed to be built

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_EXPR_PARSE_FAILED

Description: Query Master failed to parse schema expression. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_REPORT_FILE_CONTENT_MISSING

Description: Report Master failed to locate certain content in report file. Report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_COPY_FAILED

Description: Report Master/Report Worker failed to copy report file. Report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_HEADER_BAD

Description: Query Master/Report Master/Report Worker encountered bad report file header. This inline query or report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_INIT_FAILED

Description: Report Master/Report Worker failed to initialize report file. Report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_LINK_FAILED

Description: Report Master failed to link report file. Report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_MAGIC_BAD

Description: Query Master/Report Master/Report Worker encountered bad report file magic. Inline query or report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_MMAP_FAILED

Description: Query Master/Report Master failed to memory-map report file. This inline query or report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_NAME_BAD

Description: Report Master/Report Loader encountered bad report file name. This report rolling or loading will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_OPEN_FAILED

Description: Query Master/Report Master/Report Worker/Report Loader failed to open report file. Related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_PARSE_FAILED

Description: FortiSIEM Report Engine failed to parse file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_READ_FAILED

Description: Identity Master/Identity Worker failed to read entry IDs file. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_REMOVE_FAILED

Description: Report Master failed to remove report file. Disk will eventually be full

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_RENAME_FAILED

Description: Report Master failed to rename report file. This report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_RSYNC_FAILED

Description: Report Master failed to rsync report file to remote super

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
targetHostName	Target Host Name	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_STAT_FAILED

Description: Report Worker/Report Loader failed to stat report file. This report writing or loading will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FILE_TYPE_UNKNOWN

Description: Report Worker/Report Loader encountered unknown report file type. This report writing or loading will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_REPORT_FILE_UNSPECIFIED

Description: Report Master/Report Worker encountered unspecified report file. Report data will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_FILE_WRITE_FAILED

Description: Identity Master/Identity Worker failed to write entry IDs to file. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_REPORT_FUNC_OBJ_DEF_ERROR

Description: Internal error and highly generic. Refer to [procName] and [phLogDetail] tags in the actual log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_FUNC_OBJ_DEF_GET_FAILED

Description: Internal error and highly generic. Refer to [procName] and [phLogDetail] tags in the actual log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_FUNC_OBJ_DEF_UNKNOWN

Description: Internal error and highly generic. Refer to [procName] and [phLogDetail] tags in the actual log

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ID_LOC_DEVICE_EXCLUDED_INVALID

Description: FortiSIEM Identity and location module encountered invalid excluded device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ID_LOC_EVENT_SEND_FAILED

Description: FortiSIEM Identity and location module failed to upload events

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_REPORT_ID_LOC_RESULT_UPLOAD_FAILED

Description: FortiSIEM Identity and location module failed to upload results to App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
httpStatusCode	HTTP Status	string	

EventType: PH_REPORT_ID_LOC_SYNCH_DATA_UPLOAD_FAILED

Description: FortiSIEM Identity and location module failed to upload Synch Data (Worker to Master)

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_REPORT_ID_LOC_USER_ALREADY_EXCLUDED

Description: FortiSIEM Identity and location module found already excluded user

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	

EventType: PH_REPORT_ID_LOC_USER_EXCLUDE_FAILED

Description: FortiSIEM Identity and location module failed to exclude user

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
user	User	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_REPORT_INDEX_OVERFLOW

Description: Query Master/phRuleMaster/Report Master/Report Worker/Report Loader/Data Manager/Identity Master/Identity Worker encountered index out of bound. Related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.
size	Size	uint32	

EventType: PH_REPORT_IP_GET_FAILED

Description: Failed to get host IP

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_REPORT_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_KEY_LOAD_FAILED

Description: FortiSIEM Report module failed to load event attribute keys

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_REPORT_MODULE_INIT_FAILED

Description: Report Master/Report Worker/Report Loader/Identity Master/Identity Worker failed to initialize certain module. Related operation will fail

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_REPORT_MODULE_UNCONFIGURED

Description: Report Worker encountered unconfigured item. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	

EventType: PH_REPORT_OLD_REPORT_DATA

Description: Report Master encountered older report data from Worker, might enlarge block_collection_window

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_REPORT_OP_UNEXPECTED

Description: Query Master/Report Master/Report Worker encountered unexpected operator type. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ORDER_BY_ATTR_EMPTY

Description: Query Master/phRuleMaster/Report Master encountered empty order-by attributes in report. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_ORDER_BY_INVALID

Description: Query Master/phRuleMaster/Report Master encountered invalid order-by attributes in report. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_PACK_FAILED

Description: Failed to pack data

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_REPORT_PACK_FAILED_COUNT

Description: Failed to pack or unpack data

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_REPORT_PARSED_EVENT_LOAD_FAILED

Description: FortiSIEM Report module failed to load event

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_PGDB_CONNECT_FAILED

Description: Report Loader failed to connect to Postgres DB. Report loading will fail

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_REPORT_PGDB_EXEC_FAILED

Description: Report Loader failed to execute SQL statement in Postgres DB. This report loading will fail

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbQuery	Database Query	string	

EventType: PH_REPORT_PGDB_NOT_CONNECTED

Description: Query Master/Report Loader encountered disconnected Postgres DB while executing SQL statement. This incident query or report loading will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbQuery	Database Query	string	

EventType: PH_REPORT_PGDB_NOT_INIT

Description: Query Master/Report Loader encountered uninitialized Postgres DB connection manager. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_REPORT_POINTER_NULL

Description: Query Master/phRuleMaster/Report Master/Report Worker/Report Loader/Data Manager/Identity Master/Identity Worker encountered NULL pointer. Related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_POINTER_NULL_WARNING

Description: NULL pointer detected

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_POSITIVE_INTEGER_EXPECTED

Description: Query Master/Data Manager expected positive integer in performance data but got other value. Default value will be set instead

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.

EventType: PH_REPORT_PQ_ERROR

Description: Query Master/Report Loader encountered PQ function error in Postgres DB. This incident query or report loading will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_PROFILE_TYPE_BAD

Description: FortiSIEM Report module encountered bad profile

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_PROFILE_TYPE_WRONG_FORMAT

Description: Query Master encountered wrong format of profile. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_PROFILE_UPDATE_FAILED

Description: FortiSIEM Report module failed to upload profile

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	

EventType: PH_REPORT_ROW_LENGTH_ZERO

Description: Query Master encountered empty row for given report ID. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	

EventType: PH_REPORT_RULE_ATTR_MISSING

Description: Query Master failed to locate certain rule attribute in profile. This profile query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_REPORT_SCHEMA_INCOMPATIBLE

Description: Query Master/Report Master encountered incompatible report schema. This inline query or report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_SCHEMA_INVALID

Description: Query Master/Report Master encountered invalid report schema. This inline query or report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_SCHEMA_LOAD_FAILED

Description: Query Master/Report Master failed to load report schema. This inline query or report rolling will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_SQLITE3_BATCH_BEGIN_FAILED

Description: Report Master failed to begin SQLite3 batch transaction. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
profDateType	Profile Date Type	uchar	
hourOfDay	Hour Of Day	uint16	This attribute is not used

EventType: PH_REPORT_SQLITE3_BATCH_COMMIT_FAILED

Description: Report Master failed to commit SQLite3 batch transaction. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
profDateType	Profile Date Type	uchar	
hourOfDay	Hour Of Day	uint16	This attribute is not used

EventType: PH_REPORT_SQLITE3_BIND_VALUE_FAILED

Description: Report Master failed to bind certain value to SQLite3. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
tableName	DB Tablespace Name	string	
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_SQLITE3_BUSY

Description: Report Master encountered SQLite3 busy state. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_SQLITE3_BUSY_TIMEOUT_ERROR

Description: Report Master encountered SQLite3 busy timeout. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbRetCode	DB Return Code	uint32	

EventType: PH_REPORT_SQLITE3_CHECKPOINT_FAILED

Description: FortiSIEM Report module failed to checkpoint profile

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_SQLITE3_COMMIT_ERROR

Description: Report Master encountered commit error in SQLite3. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
tablespaceName	DB Tablespace Name	string	

EventType: PH_REPORT_SQLITE3_CONFIG_FAILED

Description: Report Master failed to configurate SQLite3 with multi-thread mode. Performance will degrade

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_SQLITE3_ENABLE_SHARED_CACHE_FAILED

Description: Report Master failed to enable shared cache for SQLite3. Performance will degrade

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbRetCode	DB Return Code	uint32	

EventType: PH_REPORT_SQLITE3_EXEC_FAILED

Description: Report Master failed to execute SQLite3 statement. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbQuery	Database Query	string	
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
tableName	DB Tablespace Name	string	

EventType: PH_REPORT_SQLITE3_EXTENDED_RESULT_CODES_ERROR

Description: Report Master failed to enable extended result codes for SQLite3. Maintainability will degrade

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbRetCode	DB Return Code	uint32	

EventType: PH_REPORT_SQLITE3_OPEN_FAILED

Description: Report Master failed to open SQLite3. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_SQLITE3_PREPARE_ERROR

Description: Report Master failed to prepare SQLite3 statement. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
tablename	DB Tablespace Name	string	
dbQuery	Database Query	string	

Id	Display name	Type	Description
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_SQLITE3_PROFILE_ENTRY_DELETE_FAILED

Description: Report Master failed to delete profile entry from SQLite3. Profile or Daily DB will contain redundant data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
reportId	Report ID	uint32	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
profDateType	Profile Date Type	uchar	
hourOfDay	Hour Of Day	uint16	This attribute is not used

EventType: PH_REPORT_SQLITE3_PROFILE_NOT_FOUND

Description: Report Master failed to find profile ID in SQLite3. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbName	DB Name	string	
reportId	Report ID	uint32	

EventType: PH_REPORT_SQLITE3_STEP_ERROR

Description: Report Master failed to step SQLite3 statement. Profile or Daily DB will not be updated

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
tableName	DB Tablespace Name	string	
dbRetCode	DB Return Code	uint32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_REPORT_UNPACK_FAILED

Description: Rule Master failed to unpack rule data from Rule Workers, causing potential incident loss.

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_REPORT_VALUE_TYPE_LOOKUP_BY_ID_FAILED

Description: Report-related process failed to lookup value type by attribute ID. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_VALUE_TYPE_LOOKUP_BY_NAME_FAILED

Description: Report-related process failed to lookup value type by attribute name. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_VALUE_TYPE_OF_ID_UNEXPECTED

Description: Report-related process encountered unexpected value type of certain attribute ID. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_VALUE_TYPE_OF_NAME_UNEXPECTED

Description: Report-related process encountered unexpected value type of certain attribute name. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_VALUE_TYPE_OF_STAT_UNEXPECTED

Description: Report-related process encountered unexpected value type of stat item. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_VALUE_TYPE_UNSUPPORTED

Description: Report-related process encountered unsupported value type. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_WORKER_UPLOAD_FAILED

Description: Failed to upload a data block buffer

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reportId	Report ID	uint32	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_REPORT_XML_ELEMENT_DUPLICATE

Description: Query Master encountered duplicate XML element. This performance metrics update will not be complete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.

EventType: PH_REPORT_XML_ELEMENT_MISSING

Description: Report Master failed to locate certain XML element. This report rolling will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_REPORT_XML_ELEMENT_PARSE_FAILED

Description: Query Master failed to parse certain XML element. This performance metrics update will not be complete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.

EventType: PH_REPORT_XML_PARSE_FAILED

Description: Report-related process failed to parse certain XML. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_REPORT_ZLIB_COMPRESSION_TYPE_UNKNOWN

Description: Query Master encountered unknown Zlib compression type for report results file. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_REPORT_ZLIB_UNCOMPRESS_FAILED

Description: Query Master failed to uncompress Zlib report results file. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
exitValue	Command exit value	int32	

EventType: PH_RULEMASTER_TEST_RULES_CHECK_SYNTAX

Description: Rule master starts to check syntax

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_RULEMASTER_TEST_RULES_FINALIZE_STATE

Description: Rule master finalizes state report summary

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_RULEMASTER_TEST_RULES_UPDATE_STATE

Description: Rule master updates state report summary

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_RULEMOD_AGGREGATOR_EMPTY

Description: Rule Master/Rule Worker encountered empty aggregator. This rule definition will be incomplete

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_ARITH_OP_ILLEGAL

Description: Rule Master/Rule Worker encountered illegal arithmetic operation. This rule evaluation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_ATTR_ALREADY_ASSOCIATED

Description: Rule Master/Rule Worker encountered attribute already associated with given event type in '/opt/phoenix/bin/evtTypeAttrMapForSimpleRule.xml'. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
compEventType	Component Event Type	string	This is the event type in the Incident event. Since Incident itself is an event with its own event type, this variable is needed to capture the event type of the triggering events in the IncidentDetail attribute.

EventType: PH_RULEMOD_ATTR_ID_LOOKUP_BY_NAME_FAILED

Description: Rule Master/Rule Worker failed to lookup attribute ID by name in '/opt/phoenix/bin/evtTypeAttrMapForSimpleRule.xml'. The process could terminate depending on the attribute type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_ATTR_ID_UNDEFINED

Description: Rule Master/Rule Worker encountered undefined attribute ID. This rule evaluation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_ATTR_MISSING

Description: Rule Master/Rule Worker failed to locate certain attribute in '/opt/phoenix/bin/evtTypeAttrMapForSimpleRule.xml'. This attribute will be skipped

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_ATTR_NAME_LOOKUP_BY_ID_FAILED

Description: Query Master/Rule Master/Rule Worker failed to lookup attribute name by ID. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_ATTR_UNDEFINED

Description: Query Master/Rule Master/Rule Worker encountered undefined event attribute. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_BUFFER_EMPTY

Description: Rule Master/Rule Worker encountered empty buffer in loading '/opt/phoenix/bin/evtTypeAttrMapForSimpleRule.xml'. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_CLEAR_CONDITION_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid clear condition in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_CLEAR_CONDITION_SET_FAILED

Description: Query Master/Rule Master/Rule Worker failed to set clear condition in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_CONFIG_UNDEFINED

Description: Rule Master encountered undefined config item of db_server_host. Incident processing will not work

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configName	Config Name	string	

EventType: PH_RULEMOD_CONSTRUCTOR_ERROR

Description: Rule Master/Rule Worker encountered error in constructor of given module. This rule evaluation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	

EventType: PH_RULEMOD_CUST_ID_LIST_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid customer ID list in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_RULEMOD_DATA_REQUEST_PARSE_FAILED

Description: Query Master failed to parse data request from App Server. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_RULEMOD_DATA_SIZE_OVERFLOW

Description: Rule Master/Rule Worker encountered data size exceeding its capacity. This rule parsing or evaluation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_DATA_UNSUPPORTED

Description: Rule Master/Rule Worker encountered unsupported data. This rule parsing or evaluation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_DB_SERVER_HOST_UNDEFINED

Description: Database server host not defined for rule master

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
configName	Config Name	string	

EventType: PH_RULEMOD_DIR_OPEN_FAILED

Description: Rule Master/Rule Worker failed to open rule XML directory. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_RULEMOD_ENCODE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to encode given data. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_ENTITY_VERSION_MISSING

Description: Query Master/Rule Master/Rule Worker failed to identify entity version of rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_EVENT_TYPE_GROUP_INVALID

Description: Rule Worker failed to parse certain event type group in rules. Affected rule evaluation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventTypeGrp	Event Type Group	string	This field is not used

EventType: PH_RULEMOD_EVENT_TYPE_NOT_FOUND

Description: Query Master/Rule Master/Rule Worker failed to find certain event type in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_EXCEPTION_ELEMENT_INVALID

Description: Rule Master encountered invalid element in rule exception. This rule exception parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
description	Description	string	

EventType: PH_RULEMOD_EXPR_EVAL_UNKNOWN

Description: Query Master encountered unknown expression evaluation of given operator type. This incident query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_EXPR_PARSE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to parse certain expression. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_RULEMOD_EXPR_UNSUPPORTED

Description: Query Master/Rule Master/Rule Worker encountered unsupported expression in aggregate function. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_RULEMOD_FILE_OPEN_FAILED

Description: Rule Master/Rule Worker failed to open rule-related file. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_RULEMOD_FILE_UNSPECIFIED

Description: Rule Master/Rule Worker encountered unspecified rule XML file. This rule update will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_RULEMOD_FORMAT_ERROR

Description: Query Master/Rule Master/Rule Worker encountered format error in given expression. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_FUNC_NOT_FOUND

Description: Query Master/Rule Master/Rule Worker failed to locate certain function in given expression. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_RULEMOD_FUNC_PARSE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to parse certain function in given expression. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_RULEMOD_GLOBAL_CONSTRAINT_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid global constraint in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.
task	Task	string	

EventType: PH_RULEMOD_GROUPBY_LIST_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid group-by list in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_RULEMOD_GROUPBY_LIST_NOT_FOUND

Description: Query Master/Rule Master/Rule Worker failed to find group-by list in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_GROUP_EVENT_CONSTRAINT_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid group event constraint in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_RULEMOD_ID_LOOKUP_BY_INCIDENT_FAILED

Description: Rule Master failed to lookup rule ID by incident ID. This incident firing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
incidentId	Incident ID	uint64	Unique ID of a FortiSIEM Incident
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_RULEMOD_INCIDENT_ARG_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid incident argument in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_RULEMOD_INCIDENT_CACHE_NOT_FOUND

Description: Rule Master failed to find incident cache for given incident ID. This incident will not be cleared

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
incidentId	Incident ID	uint64	Unique ID of a FortiSIEM Incident
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_INCIDENT_DEF_INVALID

Description: Query Master/Rule Master encountered invalid incident definition in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_INCIDENT_NOT_FOUND

Description: Rule Master failed to find given incident ID. This incident will not be cleared

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
incidentId	Incident ID	uint64	Unique ID of a FortiSIEM Incident

EventType: PH_RULEMOD_INCIDENT_REPORT_SEND_FAILED

Description: Rule Master failed to send incident report to phParser. This incident will be missing in eventdb

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_RULEMOD_INDEX_OVERFLOW

Description: Query Master encountered out-of-bound index in certain data. This incident query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
seqNum	Sequence Number	uint64	TCP Sequence number field in TCP header.
size	Size	uint32	

EventType: PH_RULEMOD_INFO_GET_FAILED

Description: FortiSIEM Report module failed to get statistics

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_IP_GET_FAILED

Description: Rule Worker failed to get host IP of Supervisor. Incident firing will not work

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_RULEMOD_IP_INVALID

Description: Query Master/Rule Master/Rule Worker found invalid IP in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_RULEMOD_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_LOAD_METHOD_UNDEFINED

Description: Rule Master/Rule Worker encountered undefined rule load method. Rule loading will fail

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_MEM_ALLOC_FAILED

Description: Query Master/Rule Master/Rule Worker failed to allocate memory. The related operation will fail

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_MODULE_INIT_FAILED

Description: Rule Master/Rule Worker failed to be initialized. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
module	Module Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_MUTEX_ACQUIRE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to acquire mutex. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id				Display name				Type				Description			
module				Module Name				string							

EventType: PH_RULEMOD_NOTIF_CONNECTION_FAILED

Description: Rule Master failed to establish notification connection to phParser. This incident will be missing in eventdb

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id				Display name				Type				Description			
destName				Destination Host Name				string				Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.			
destIpPort				Destination TCP/UDP Port				uint16				This is the destination TCP or UDP port as identified in the event			

EventType: PH_RULEMOD_OBJ_GET_FROM_SUBPATTERN_FAILED

Description: Rule Master failed to get certain object from subpattern. This incident cache update will be incomplete

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_OBJ_LOAD_FAILED

Description: Query Master/Rule Master/Rule Worker failed to load certain object in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_OP_NOT_FUNC

Description: Rule Master encountered an operator of non-function type. This incident initialization will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_OP_UNKNOWN

Description: Query Master/Rule Master/Rule Worker encountered unknown operator. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_PARSED_EVENT_LOAD_FAILED

Description: Rule Worker failed to load and skipped a parsed event, causing potential incident loss.

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_PQ_ERROR

Description: Rule Master encountered PQ function error in Postgres DB. Incident processing will not work

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_RULEMOD_PROFILE

Description: FortiSIEM Rule resource usage profile

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleName	Rule Name	string	FortiSIEM rule name.
usedMemKB	Used Memory	uint32	
updateQueueSize	Update Queue Size	uint32	

EventType: PH_RULEMOD_REM_BY_ZERO

Description: Rule Master/Rule Worker caught remainder-by-zero exception. Default value will be set instead

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_REM_BY_ZEROD

Description: FortiSIEM Report module failed to produce statistics

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_SELECT_ATTR_PARSE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to parse and skipped certain select attribute. This rule parsing will be incomplete

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_SELECT_SPEC_PARSE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to parse at least one select spec field. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_SINGLE_EVENT_CONSTRAINT_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid single event constraint in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_RULEMOD_SUBPATTERN_INVALID

Description: Query Master/Rule Master/Rule Worker encountered invalid subpattern in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_SUBPATTERN_MISSING

Description: Query Master/Rule Master/Rule Worker failed to locate certain subpattern in XML. The related operation will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_SUBPATTERN_MORE_THAN_ONE

Description: Query Master/Rule Master/Rule Worker encountered more than one subpattern in simple rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_SUBPATTERN_UNDEFINED

Description: Query Master/Rule Master/Rule Worker encountered undefined subpattern in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_SUMMARY_UPLOAD_FAILED

Description: Rule Worker failed to upload rule summary to Rule Master, causing potential incident loss.

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_THREAD_SPAWN_FAILED

Description: Rule Master/Rule Worker failed to spawn thread during initialization. The process will terminate

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	

EventType: PH_RULEMOD_TOKEN_UNDEFINED

Description: Query Master/Rule Master/Rule Worker encountered undefined token of given type in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_TOKEN_UNEXPECTED

Description: Query Master/Rule Master/Rule Worker encountered unexpected token of given type in rule. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_UNPACK_FAILED

Description: Rule Master failed to unpack rule data from Rule Workers, causing potential incident loss.

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_RULEMOD_VALUE_TYPE_UNEXPECTED

Description: Query Master encountered unexpected value type of certain attribute. This incident query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_XML_ELEMENT_EMPTY

Description: Query Master/Rule Master/Rule Worker encountered empty XML element. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_XML_ELEMENT_MISSING

Description: Query Master/Rule Master/Rule Worker encountered missing XML element. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_XML_ELEMENT_PARSE_FAILED

Description: Query Master failed to parse certain XML element. This inline query will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_XML_ELEMENT_UNEXPECTED

Description: Query Master/Rule Master/Rule Worker encountered unexpected XML element. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_RULEMOD_XML_ELEMENT_UNKNOWN

Description: Query Master/Rule Master/Rule Worker encountered unknown XML element. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEMOD_XML_LOAD_FAILED

Description: Rule Master/Rule Worker failed to load rule XML from file. This rule loading will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_RULEMOD_XML_PARSE_FAILED

Description: Query Master/Rule Master/Rule Worker failed to parse rule XML. This rule parsing will fail

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_RULEMOD_XML_POINTER_NULL

Description: NULL pointer in XML detected

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_RULEWORKER_TEST_RULES_CHECK_SYNTAX

Description: Rule worker starts to check syntax

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_RULEWORKER_TEST_RULES_EVENT_MATCH_STATUS

Description: Rule worker event test status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventId	Event ID	uint64	This is a globally unique ID assigned to every raw event ingested into the SIEM. This is used by the system for tying events to incidents, and is typically not needed by end users.

EventType: PH_Rule_AbuseCH_Botnetc2_MalwareIP_Inbound

Description: Permitted Traffic from AbuseCH Botnet C2 Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_AbuseCH_Botnetc2_MalwareIP_Outbound

Description: Traffic to AbuseCH Botnet C2 Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Blocklist_MalwareIP_Inbound

Description: Permitted Traffic from Blocklist DE Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Blocklist_MalwareIP_Outbound

Description: Traffic to Blocklist DE Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_C2_Tracker_MalwareIP_Inbound

Description: Permitted Traffic from C2 Tracker Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_C2_Tracker_MalwareIP_Outbound

Description: Traffic to C2 Tracker Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_CINSScore_MalwareIP_Inbound

Description: Permitted Traffic from CINS Score Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_CINSScore_MalwareIP_Outbound

Description: Traffic to CINS Score Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_CertPL_MalwareDomain_Inbound

Description: Permitted Traffic from CertPL Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_CertPL_MalwareDomain_Outbound

Description: Traffic to CertPL Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Cisco_Talos_MalwareIP_Inbound

Description: Permitted Traffic from Cisco Talos Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Cisco_Talos_MalwareIP_Outbound

Description: Traffic to Cisco Talos Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Cluster_DBLeader_Changed

Description: FortiSIEM DB Leader Changed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_Rule_Cluster_REPL_Leader_Changed

Description: FortiSIEM Replication Leader Changed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_Rule_DigitalSide_MalwareDomain_Inbound

Description: Permitted Traffic from DigitalSide Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_DigitalSide_MalwareDomain_Outbound

Description: Traffic to DigitalSide Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_DigitalSide_MalwareIP_Inbound

Description: Permitted Traffic from DigitalSide Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_DigitalSide_MalwareIP_Outbound

Description: Traffic to DigitalSide Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_DigitalSide_MalwareURL_Outbound

Description: Traffic to DigitalSide Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FML_Antispam_Malicious_File

Description: FortiMail: Malicious Spam File Attachment Found

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FML_Antispam_Malicious_Url

Description: FortiMail: Antispam Malicious URL found

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FireHol_MalwareIP_Inbound

Description: Permitted Traffic from FireHol Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FireHol_MalwareIP_Outbound

Description: Traffic to FireHol Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiRecon_MalwareDomain_Inbound

Description: Permitted Traffic from FortiRecon Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiRecon_MalwareDomain_Outbound

Description: Traffic to FortiRecon Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiRecon_MalwareIP_Inbound

Description: Permitted Traffic from FortiRecon Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiRecon_MalwareIP_Outbound

Description: Traffic to FortiRecon Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiRecon_MalwareURL_Outbound

Description: Traffic to FortiRecon Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiSOAR_MalwareDomain_Inbound

Description: Permitted Traffic from FortiSOAR Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiSOAR_MalwareDomain_Outbound

Description: Traffic to FortiSOAR Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiSOAR_MalwareIP_Inbound

Description: Permitted Traffic from FortiSOAR Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiSOAR_MalwareIP_Outbound

Description: Traffic to FortiSOAR Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_FortiSOAR_MalwareURL_Outbound

Description: Traffic to FortiSOAR Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Greensnow_MalwareIP_Inbound

Description: Permitted Traffic from Greensnow Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Greensnow_MalwareIP_Outbound

Description: Traffic to Greensnow Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_IPSum_MalwareIP_Inbound

Description: Permitted Traffic from IPSum Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_IPSum_MalwareIP_Outbound

Description: Traffic to IPSum Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_MISP_MalwareDomain_Inbound

Description: Permitted Traffic from MISP Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_MISP_MalwareDomain_Outbound

Description: Traffic to MISP Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_MISP_MalwareIP_Inbound

Description: Permitted Traffic from MISP Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_MISP_MalwareIP_Outbound

Description: Traffic to MISP Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_MISP_MalwareURL_Outbound

Description: Traffic to MISP Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Mandiant_MalwareDomain_Inbound

Description: Permitted Traffic from Mandiant Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Mandiant_MalwareDomain_Outbound

Description: Traffic to Mandiant Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Mandiant_MalwareIP_Inbound

Description: Permitted Traffic from Mandiant Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Mandiant_MalwareIP_Outbound

Description: Traffic to Mandiant Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Mandiant_MalwareURL_Outbound

Description: Traffic to Mandiant Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_OPENCTI_MalDomain_Inbound

Description: Permitted Traffic from OpenCTI Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_OPENCTI_MalDomain_Outbound

Description: Traffic to OpenCTI Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_OPENCTI_MalwareIP_Inbound

Description: Permitted Traffic from OpenCTI Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_OPENCTI_MalwareIP_Outbound

Description: Traffic to OpenCTI Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_OPENCTI_MalwareURL_Outbound

Description: Traffic to OpenCTI Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_OpenPhish_MalwareURL_Outbound

Description: Traffic to OpenPhish Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Proofpoint_MalwareIP_Inbound

Description: Permitted Traffic from Proofpoint Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Proofpoint_MalwareIP_Outbound

Description: Traffic to Proofpoint Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Snort_MalwareIP_Inbound

Description: Permitted Traffic from Snort Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Snort_MalwareIP_Outbound

Description: Traffic to Snort Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_ThreatFox_MalwareURL_Outbound

Description: Traffic to ThreatFox Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_TweetFeed_MalwareDomain_Inbound

Description: Permitted Traffic from TweetFeed Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_TweetFeed_MalwareDomain_Outbound

Description: Traffic to TweetFeed Malware Domain List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_TweetFeed_MalwareURL_Outbound

Description: Traffic to TweetFeed Malware URL List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Tweetfeed_MalwareIP_Inbound

Description: Permitted Traffic from TweetFeed Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_Rule_Tweetfeed_MalwareIP_Outbound

Description: Traffic to TweetFeed Malware IP List

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_SAAS_OP_COLLECTOR_DOWN

Description: Collector down

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SAAS_OP_COLLECTOR_UP

Description: Collector up

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SCHEDULED_RULE_QUERY_FAILED

Description: Failed to run query for scheduled rule

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
queryId	Query Id	string	
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_SER_MON_SERVICE_DOWN

Description: PH process down

Severity: 8 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SHAREDSTORE_ACQUIRE_ERROR

Description: A module failed to acquire shared store. The module will abort

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_SHAREDSTORE_WRITER_POS_UNEXPECTED_ALTERED

Description: Shared store writer position altered unexpectedly

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_SHAREDSTORE_WRITE_ERROR

Description: Parser module encountered error while writing to shared store. Events will be lost

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_SSL_SHUTDOWN_ERROR

Description: PH system ssl shutdown error

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_ACCOUNT_UNMATCHED

Description: Perf / STM module encountered unmatched LOOP_EMAIL_42 account in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_AUTH_TYPE_UNKNOWN

Description: Perf / STM module encountered unknown auth type in monitor in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_BAD_ELEM

Description: Perf / STM module encountered bad element in monitor in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_BAD_ELEM_VALUE

Description: Perf / STM module encountered bad element values in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_BAD_PORT

Description: Perf / STM module encountered bad port in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_BAD_RTT_LINE

Description: Perf / STM module encountered bad RTT line in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_BAD_SSL

Description: Perf / STM module encountered bad SSL in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_BAD_TAG

Description: Perf / STM module encountered bad Tag in XML received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_CMD_EXEC_FAILED

Description: Perf / STM module failed to execute command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
exitValue	Command exit value	int32	

EventType: PH_STM_CRED_INVALID

Description: Perf / STM module found that credential doesn't match with Custom Perf Object

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_CURL_ESCAPE_FAILED

Description: Perf / STM module found that curl_easy_escape() returned NULL

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_CURL_INIT_FAILED

Description: Perf / STM module failed to init curl - HTTP based communication will fail

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_STM_DNS_TYPE_UNSupport

Description: Perf / STM module found unsupported dns resource record type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_DUPLICATED

Description: Perf / STM module found duplicated svcMonitor name or id

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_ELEM_EMPTY

Description: Perf / STM module found empty XML element received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_ELEM_MISSING

Description: Perf / STM module found missing XML element received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_ELEM_NEGATIVE

Description: Perf / STM module found negative XML element received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_ERROR

Description: Perf / STM module encountered STM monitor error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event
ipPort	IP Port	uint16	IP port number
user	User	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_STM_FILE_OPEN_FAILED

Description: Perf / STM module failed to open file during STM operation

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
exitValue	Command exit value	int32	

EventType: PH_STM_GET_HOST_FAILED

Description: Perf / STM module failed to get outgoing host

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_STM_GUESS_TYPE_FAILED

Description: Perf / STM module could not guess resource record type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_HTTP_RESP_FAILED

Description: Perf / STM module did not find response time from command output

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_STM_METHOD_UNKNOWN

Description: Perf / STM module found unknown url method in monitor

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_MONITOR_MISSING_ACTION

Description: Perf / STM module found that No action is specified for monitor

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_MONITOR_RESULT_UPLOAD_FAILED

Description: Perf / STM module failed to upload test service monitor result xml to APP server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_NO_ORACLE_NAME

Description: Perf / STM module found missing instance name and service name for Oracle server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
serverIpAddr	Server IP	IP	

EventType: PH_STM_PORT_UNKNOWN

Description: Perf / STM module found unknown service monitor port

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_PROCESS_INVOKE_FAILED

Description: Perf / STM module failed to invoke SrvMonJobExec::execute

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_PROTO_UNKNOWN

Description: Perf / STM module encountered unknown proto in STM job definition

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_PROTO_UN SUPPORT

Description: Perf / STM module encountered unsupported mail protocol in STM job definition

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_SERVER_ADDR_INVALID

Description: Perf / STM module encountered invalid server address in STM job definition

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_SPECIAL_LINE_NOT_FOUND

Description: Perf / STM module could not find either RTT line or packet loss line in ping response from device

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_STM_GET_PROCESS_FAILED

Description: Perf / STM module cannot get process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_STM_GET_PROCESS_NAME_FAILED

Description: Perf / STM module cannot get process name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_TAG_MISSING

Description: Perf / STM module found missing tag XML element received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_TAG_NOT_FOUND

Description: Perf / STM module found missing tag XML element received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_TAG_UNKNOWN

Description: Perf / STM module found unknown tag XML element received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_TRACEROUTE_FAILED

Description: Perf / STM module failed to parse traceroute output

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_STM_XML_PARSE_FAILED

Description: Perf / STM module failed to parse xml file received from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_SYSTEM_ARCHIVE_LOW

Description: FortiSIEM EventDB Archive disk space low

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGED_LOW_SPACE

Description: Event database archive files purged to make room for new archive

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGED_POLICY

Description: Event database archive files purged by policy

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_FAILED

Description: Failed to purge Archive FortiSIEM EventDB - purge caused by low available space

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_FINISHED

Description: Successfully purged Archive FortiSIEM EventDB -purge caused by low available space

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_STARTED

Description: Started to purge Archive FortiSIEM EventDB because of low available space

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_LOW_SPACE_SUCCESS

Description: Successfully purged Archive FortiSIEM EventDB because of low available space

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_FAILED

Description: Failed to purge Archive FortiSIEM EventDB - purge caused by policy

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_FINISHED

Description: Successfully purged Archive FortiSIEM EventDB - purge caused by policy

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_STARTED

Description: Started to purge Archive FortiSIEM EventDB - purge caused by policy

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_PURGING_POLICY_SUCCESS

Description: Successfully purged Archive FortiSIEM EventDB - purge caused by policy

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_ARCHIVE_RETENTION_POLICY_VIOLATED

Description: Archive retention policy violation

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_SYSTEM_ARCHIVE_USAGE

Description: Archive disk usage

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
diskUsage	Disk Used MB	uint64	

EventType: PH_SYSTEM_DATAMGR_ARCHIVE_SKIP

Description: Online FortiSIEM EventDB Archiving skipped since the directory has data

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DEVAPP_EVENTS_PER_SEC

Description: FortiSIEM per application EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptVendor	Reporting Vendor	string	This field captures the vendor of the reported event

Id	Display name	Type	Description
reptModel	Reporting Model	string	This field captures the model of the reported event
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_SYSTEM_DEVAPP_NO_EVENTS

Description: No events from a reporting module in last 1 hour

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptVendor	Reporting Vendor	string	This field captures the vendor of the reported event
reptModel	Reporting Model	string	This field captures the model of the reported event
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.

EventType: PH_SYSTEM_DEVICE_NO_EVENTS

Description: No events from a device in last 1 hour

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_ARCHIVING_FAILED

Description: Online FortiSIEM EventDB Archiving encountered errors

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_ARCHIVING_FINISHED

Description: Online FortiSIEM EventDB Archiving completed

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_ARCHIVING_STARTED

Description: Online FortiSIEM EventDB Archiving started

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_ARCHIVING_SUCCESS

Description: Online FortiSIEM EventDB Archiving success

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_PURGED

Description: Event database files purged

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_SYSTEM_DISK_PURGING_FAILED

Description: Online FortiSIEM EventDB Purging encountered errors

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_PURGING_FINISHED

Description: Online FortiSIEM EventDB Purging completed

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_PURGING_STARTED

Description: Online FortiSIEM EventDB Purging started

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_PURGING_SUCCESS

Description: Online FortiSIEM EventDB Purging success

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_DISK_USAGE

Description: Disk usage of customer

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
diskUsage	Disk Used MB	uint64	

EventType: PH_SYSTEM_DISK_USAGE_EXCEED_LICENSE

Description: Event database disk usage exceeded limit

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_SYSTEM_DISK_USAGE_WARNING

Description: FortiSIEM EventDB disk usage close to limit

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_SYSTEM_DROP_UNKNOWN_ORG

Description: Dropped events which belong to unknown organization

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_EPS_GLOBAL

Description: FortiSIEM Global event handling statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
licenseEventsPerSec	License EPS	uint64	
incomingEventsPerSec	Incoming Event Rate	double	This is a FortiSIEM event ingestion rate calculated every 3 minutes, divided by 180 to generate a rolling EPS (Events Per Second) interval.
peakIncomingEventsPerSec	Peak Incoming Event Rate	double	This is the spike or max event ingestion rate seen during a 3 minute interval averaged overall data points.
dropLicenseEventsPerSec	License Dropped Event Rate	double	The number of events dropped due to exceeding license in past 3 minutes.
peakDropLicenseEventsPerSec	Peak License Dropped Event Rate	double	The max value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.
unusedEvents	Unused Event Count	uint64	The difference between licenseEventsPerSec and incomingEventsPerSec accumulated.

EventType: PH_SYSTEM_EPS_NODE**Description:** FortiSIEM per Node event handling statistics**Severity:** 1 (Low)**Event Category:** 3 (System Logs)**Attributes:**

Id	Display name	Type	Description
role	Role	string	
hostName	Host Name	string	This is the hostname of the device of interest in the event
guaranteedEventsPerSec	Guaranteed EPS	uint64	
incomingEventsPerSec	Incoming Event Rate	double	This is a FortiSIEM event ingestion rate calculated every 3 minutes, divided by 180 to generate a rolling EPS (Events Per Second) interval.

Id	Display name	Type	Description
peakIncomingEventsPerSec	Peak Incoming Event Rate	double	This is the spike or max event ingestion rate seen during a 3 minute interval averaged overall data points.
ingestedEventsPerSec	Ingested Event Rate	double	
dropPolicyEvents	Policy Dropped Events	uint64	The number of events dropped by Event Dropping Rules in the last 3 minutes.
dropPolicyEventsPerSec	Policy Droppped Event Rate	double	This is the per second count of events dropped by policy, which is calculated as dropPolicyEvents (3min interval) / 180 seconds.
peakDropPolicyEventsPerSec	Peak Policy Dropped Event Rate	double	The max value of dropPolicyEventsPerSec, over all 3-minute periods, since phParser started.
dropLicenseEvents	License Dropped Events	uint64	This is the total count of events dropped due to exceeding license over all 3 minute intervals since phParser started.
dropLicenseEventsPerSec	License Dropped Event Rate	double	The number of events dropped due to exceeding license in past 3 minutes.
peakDropLicenseEventsPerSec	Peak License Dropped Event Rate	double	The max value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.
dropLicenseEventRatio	License Dropped Event Ratio	uint16	Ratio of dropped events due to license to total incoming events in last 3 minutes.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.

EventType: PH_SYSTEM_EPS_ORG

Description: FortiSIEM per Organization event handling statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
incomingEventsPerSec	Incoming Event Rate	double	This is a FortiSIEM event ingestion rate calculated every 3 minutes, divided by 180 to generate a rolling EPS (Events Per Second) interval.
peakIncomingEventsPerSec	Peak Incoming Event Rate	double	This is the spike or max event ingestion rate seen during a 3 minute interval averaged overall data points.
dropLicenseEventsPerSec	License Dropped Event Rate	double	The number of events dropped due to exceeding license in past 3 minutes.
peakDropLicenseEventsPerSec	Peak License Dropped Event Rate	double	The max value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.

EventType: PH_SYSTEM_EVENTS_FWD_STAT

Description: Forwarded EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
role	Role	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
customer	Organization Name	string	This is the FortiSIEM Organization Name, which is unique to each tenant. It identifies the tenant this event belongs to.
fwdEventsPerSec	Forwarded Event Rate	double	This field represents the average rate (events per sec) over a 3 minute window, at which events are forwarded from FortiSIEM to an external system

Id	Display name	Type	Description
peakFwdEventsPerSec	Peak Forwarded Event Rate	double	This field represents the maximum rate (events per sec) over a 3 minute window, at which events are forwarded from FortiSIEM to an external system
dropFwdEventsPerSec	Dropped Forwarded Event Rate	double	
peakDropFwdEventsPerSec	Peak Dropped Forwarded Event Rate	double	
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
reptDevName	Reporting Device	string	This is the hostname of the device that originated the log or event packet.

EventType: PH_SYSTEM_EVENTS_PER_SEC

Description: Received EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
peakEventsPerSec	Peak Event Rate	double	
guaranteedEventsPerSec	Guaranteed EPS	uint64	

EventType: PH_SYSTEM_EVENTS_VIA_ZMQ_EPS

Description: Events Pushed by ZMQ EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totEventCount	Total Event Count	uint32	
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_SYSTEM_EVENT_RATE_EXCEED_LICENSE

Description: System event rate exceeds licensed event rate

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_INTERNAL_EVENTS_PER_SEC

Description: FortiSIEM Internal EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
peakEventsPerSec	Peak Event Rate	double	

EventType: PH_SYSTEM_IP_EVENTS_PER_SEC

Description: FortiSIEM per device EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_SYSTEM_ONLINE_RETENTION_POLICY_VIOLATED

Description: Online data retention policy violation

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
policyName	Policy Name	string	

EventType: PH_SYSTEM_PERF_EVENTS_PER_SEC

Description: FortiSIEM performance monitoring EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
peakEventsPerSec	Peak Event Rate	double	

EventType: PH_SYSTEM_RAW_EVENT_SIZE

Description: Total event size in the last fifteen minutes

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phRecvTime	Event Receive Time	Date	This is the timestamp the collector records, when an event is ingested. This is converted and stored as epoch milliseconds. FortiSIEM uses this time in all its analytics. This time is obtained from NTP.
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.
hostName	Host Name	string	This is the hostname of the device of interest in the event
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_SYSTEM_RETENTION_POLICY_EXEC_TIME

Description: Data retention policy enforcement time

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
runTime	Run Time	uint64	

EventType: PH_SYSTEM_RETENTION_POLICY_FAILED

Description: Data retention policy enforcement failed

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_SYSTEM_RETENTION_POLICY_FINISHED

Description: Data retention policy enforcement finished

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_RETENTION_POLICY_STARTED

Description: Data retention policy enforcement started

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_RETENTION_POLICY_STATS

Description: Data retention policy enforcement statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
totBytes64	Total Bytes64	uint64	Total number of sent and received bytes by a host. This has 64bit resolution.

EventType: PH_SYSTEM_RETENTION_POLICY_SUCCESS

Description: Data retention policy enforcement succeeded

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_SYSTEM_STORAGE_LOW

Description: System data storage is low

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
diskName	Disk Name	string	
freeDiskMB	Free Disk MB	uint32	
diskUtil	Disk Capacity Util	double	

EventType: PH_SYSTEM_STORED_EVENTS_PER_SEC

Description: Stored EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
peakEventsPerSec	Peak Event Rate	double	

EventType: PH_SYSTEM_SUMM_EVENTS_STORED_EPS

Description: Summary Events Stored EPS statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
totEventCount	Total Event Count	uint32	
eventsPerSec	Event Rate	double	A generic attribute for recording event ingestion or handling rate.

EventType: PH_SYS_ERROR_XML_SEND_ERROR

Description: Error in sending system error to app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_SYS_ERROR_XML_SENT

Description: System error sent to app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_TASK_DATA_EMPTY

Description: Task data is empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_TASK_DATA_IS_WRONG

Description: Task data is wrong

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	

EventType: PH_TASK_FAILED

Description: Task Failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_TASK_NOT_CONTAIN_LIC

Description: Task data doesn't contain license data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_TASK_NO_LICENSE

Description: There is no license

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_TASK_RUN_COMMAND_FAILED

Description: Failed to run command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	

EventType: PH_TASK_SEND_FAILED

Description: Failed to send task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
task	Task	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event
procName	Process Name	string	

EventType: PH_TASK_UN SUPPORT

Description: Unsupport this task

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_TEST_CONN_COMPLETE

Description: Test Connectivity completed

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_TEST_CONN_CONTACT_APP_SERVER

Description: Test Connectivity module contacting app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_TEST_CONN_FAILED

Description: Test Connectivity failed

Severity: 9 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_TEST_CONN_FAILED_INVALID_REQUEST

Description: Test Connectivity failed - invalid discovery request from App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_TEST_CONN_FAILED_INVALID_REQUEST_XML

Description: Test Connectivity failed - invalid discovery request XML from App Server

Severity: 9 (High)

Event Category: 3 (System Logs)

EventType: PH_TEST_CONN_RECVD_VALID_REQUEST

Description: Received valid test connectivity request from app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_TEST_CONN_RESULT_SENT

Description: Test Connectivity results sent to app server

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_TEST_CONN_STARTED

Description: Starting test connectivity for a device

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.

EventType: PH_TEST_RULES_PARSE_STATUS

Description: Syntax check status

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.

EventType: PH_THREAD_EXITING

Description: Module exiting thread

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
threadName	Thread Name	string	

EventType: PH_THREAD_RECVD_EXIT

Description: Thread received exit request

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
threadName	Thread Name	string	

EventType: PH_THREAD_STARTING

Description: Module starting thread

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
threadName	Thread Name	string	

EventType: PH_UNABLE_ACCESS_DIR

Description: Unable to access archive directory

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_UNABLE_ALLOC_MEMORY

Description: Unable to allocate memory

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UNABLE_CREATE_DIR

Description: Unable to create dir

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_UNABLE_CREATE_FILE

Description: Unable to create file

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_UNABLE_CREATE_TIMER

Description: Unable to create timer

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UNABLE_OPEN_DIR

Description: Unable to open dir

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_UNABLE_OPEN_FILE

Description: Unable to open file

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_UNABLE_PARSE_XML

Description: Unable to parse xml

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	

EventType: PH_UNABLE_RENAME_FILE

Description: Unable to rename file

Severity: 6 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
srcFilePath	Source File Path	string	
destFilePath	Destination File Path	string	
errorNo	Error Number Unsigned	uint32	This is an unsigned integer error number

EventType: PH_UNRESOLVABLE_HOSTNAME

Description: FortiSIEM module failed to resolve host name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostName	Host Name	string	This is the hostname of the device of interest in the event

EventType: PH_UNRESOLVABLE_IP

Description: FortiSIEM module failed to resolve ip to get host name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
hostIpAddr	Host IP	IP	This is the IP of the device of interest in the event.

EventType: PH_UPDATE_RULE_SUCCEED

Description: Rule update succeeded

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
opName	Operation Name	string	
ruleId	Rule ID	uint64	Unique ID of a FortiSIEM rule.
ruleName	Rule Name	string	FortiSIEM rule name.

EventType: PH_USER_MON_SUDDEN_LOC_CHANGE

Description: User location anomaly detected

Notes: FortiSIEM Identity and Location Module keeps track of (Source IP, Longitude, Latitude, User, Last Seen Time). For every new Identity and Location event (See docs on Dashboard identity location), the Haversine distance (https://en.wikipedia.org/wiki/Haversine_formula) between the new and existing Longitude and Latitudes is calculated. Then the speed required to attain this distance is calculated by dividing the Haversine distance by the elapsed time between current event and event stored in Identity and Location module. If this value exceeds 575 miles/hour, which is a reasonable limit on commercial Jetliners), then the event is generated.

This event can indicate the specific user credential is likely shared or stolen, which can be a security violation.

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	

Id	Display name	Type	Description
eventSource	Event Source	string	
srcIpAddr	Source IP	IP	Source IP of a device as identified in the event.
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
startTime	Start Time	Date	This is the start time of a given item or task, and is stored in epoch milliseconds
endTime	End Time	Date	This is the end time of a given item or task, stored in epoch milliseconds.
durationMSec	Duration	uint32	Duration of a connection (in msec)

EventType: PH_USER_MON_SUDDEN_LOGIN_DISTRIBUTION_CHANGE

Description: Change in user login distribution pattern

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
computer	Computer	string	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
oldDistrib	Old Distribution	string	Old Distribution is the profiled login distribution that is computed based on statistics from previous days. It is the probability mass function for the logins at various hours of the day and represented in a comma separated set of values, one for each hour. For each hour of the day (0 representing 12AM-1AM, 1 representing 1AM-2AM etc), the value represents the probability of login during that hour.
newDistrib	New Distribution	string	New Distribution is the login distribution for the current day. It is the probability mass function for the logins at various hours of the day and represented in a comma separated set of values, one for each hour. For each hour of the day (0 representing 12AM-1AM, 1 representing 1AM-2AM etc), the value represents the probability of login during that hour.

EventType: PH_USER_MON_SUDDEN_LOGIN_VOLUME_CHANGE

Description: Increase in User Login Volume

Severity: 5 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
profDateType	Profile Date Type	uchar	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant
user	User	string	
computer	Computer	string	
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.
oldValue	Old Value	uint64	
newValue	New Value	uint64	

EventType: PH_UTIL_BIZ_CHANGE_UPDATE_SPAWN_FAILURE

Description: phMonitor encountered error in spawning thread

Severity: 10 (High)

Event Category: 3 (System Logs)

EventType: PH_UTIL_BIZ_HTTP_REQUEST_FAILURE

Description: HTTP Request Error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_CMD_FAILURE

Description: FortiSIEM system command execution failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
command	Command	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_CONFIG_IP_MISSING

Description: Found empty IP address

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_CONFIG_LOAD_FAILURE

Description: Failed to load configuration type from the app server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
objType	Object Type	string	

EventType: PH_UTIL_CONFIG_LOAD_FILE_ACCESS_FAILURE

Description: Failed to load configuration type from the app server - tmp file not accessible

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
objType	Object Type	string	

EventType: PH_UTIL_CONFIG_PARSE_FAILURE

Description: Failed to parse system/phoenixServer.xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_UTIL_CONFIG_UNKNOWN_SERVER_TYPE

Description: Found unknown server type in App server returned XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
objType	Object Type	string	

EventType: PH_UTIL_CONNECTION_ERROR

Description: Failed to initialize connection

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_UTIL_CSV_LINE_ILLEGAL

Description: Found illegal line in csv file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
lineContent	Line Content	string	

EventType: PH_UTIL_CSV_READ_FAILURE

Description: Failed to open CSV file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_CUSTOMER_COLLECTOR_MISSING

Description: Failed to parse collectors and no collector found

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_CUSTOMER_COLLECTOR_PARSE_FAILURE

Description: Failed to parsephCustomerDevice Collector info

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_CUSTOMER_DOMAIN_MISSING

Description: No domain item found in xml file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_CUSTOMER_INFO_PARSE_FAILURE

Description: Failed to parse value group xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_UTIL_CUSTOMER_PARSE_FAILURE

Description: Failed to parse phCustomerDevice Customer info in XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_DASHBOARD_DUPLICATE_IP

Description: Encountered duplicate ip in device info for same customer Id

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
reptDevIpAddr	Reporting IP	IP	This is the device that originated the log or event packet, also known as the reporting device.
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_UTIL_DASHBOARD_DUPLICATE_ITEM

Description: Encountered duplicate item id in device info for same custId

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
item	Item	string	
phCustId	Organization ID	uint32	This is the FortiSIEM organization ID unique to each tenant

EventType: PH_UTIL_DASHBOARD_PARSE_FAILURE

Description: Failed to parse dashboard device info xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_UTIL_DEVICE_MAP_PROP_ERROR

Description: Encountered device map property error in XML

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_DEVICE_PROP_ERROR

Description: Encountered device property error in XML

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_DEVICE_SIMPLE_PROP_PARSE_FAILURE

Description: Failed to parse NULL element for property in XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propName	Property Name	string	

EventType: PH_UTIL_DGA_FREQ_FILE_OPEN_FAILURE

Description: Failed to open DGA freq file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_UTIL_DGA_WHITELIST_FILE_OPEN_FAILURE

Description: Failed to open DGA white list file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_UTIL_DIR_CREATE_FAILURE

Description: Failed to create directory after a few attempts

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_DIR_CREATE_RETRIED

Description: Retried to created dir

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

Id	Display name	Type	Description
count	Count	uint32	A general count variable. A common use case is for incidents. Count represents how many times an Incident occurred in a time interval. When an Incident with the same group by parameters occurs again. The count is incremented and the Last Seen time is advanced. Count can be used for other events also.

EventType: PH_UTIL_DIR_OPEN_FAILURE

Description: Failed to open directory after a few attempts

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_DIR_PARENT_NOT_EXIST

Description: Failed to locate Parent directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_UTIL_DIR_REMOVE_FAILURE

Description: Failed to remove directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	
errReason	Reason for Error	string	This is the reason for an error if given.
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_DISK_USAGE_INFO_GET_FAILURE

Description: Unable to get disk usage information

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dirName	Directory Name	string	

EventType: PH_UTIL_DISPATH_CMD_XML_ILLEGAL

Description: Encountered malformed XML

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_UTIL_DISPATH_CMD_XML_PARSE_FAILURE

Description: Encountered XML parsing failure

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_UTIL_EMAIL_SEND_FAILURE

Description: Failed to send email to server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_UTIL_ETCD_COMPAGN_FAILED

Description: etcd.compaign has error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_ETCD_GET_LEADER_FAILED

Description: Failed to get super leader

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_ETCD_LEASE_FAILED

Description: etcd.leasekeepalive has error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_ETCD_SET_FAILED

Description: etcd.set has error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_EVENT_FILE_ERROR

Description: Encountered Event file error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_EVENT_GROUP_ERROR

Description: Encountered Event Group error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_EVENT_STATUS_REPORTER_SPAWN_FAILURE

Description: Failed to initialize external event status reporter thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_EVENT_STATUS_UPLOAD_FAILURE

Description: Failed to upload external event status xml after 3 retries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_EVENT_TYPE_ERROR

Description: Encountered Event type error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_FILE_NOT_EXIST

Description: File doesn't exist

Severity: 3 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_UTIL_FILE_OPEN_FAILURE

Description: Failed to open file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_FILE_READ_FAILURE

Description: Error reading file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_FILE_SIZE_MISMATCH

Description: File size mismatch

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_FILE_SIZE_TOO_SMALL

Description: File size too small

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
fileSize64	File Size64 Bytes	uint64	

EventType: PH_UTIL_FILE_STATFS_FAILURE

Description: Failed to run statfs() command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_FILE_STAT_FAILURE

Description: Failed to stat file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_FILE_WRITE_FAILURE

Description: Error writing file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_FORK_FAILURE

Description: System fork failed - likely system highly utilized

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_GET_ADDR_FAILURE

Description: Failed to run Getaddrinfo command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_UTIL_GET_ATTR_NAME_FAILED

Description: Failed to get attribute

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
details	Details	string	

EventType: PH_UTIL_GET_JOB_STATUS_FAILURE

Description: Failed to get job status to status file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
paraName	Param Name	string	

EventType: PH_UTIL_HOSTNAME_GET_FAILURE

Description: Failed to look up Host name

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_INET_PTON_FAILURE

Description: Failed to run inet_ntop command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_INODE_INFO_GET_FAILURE

Description: Unable to get inode information

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
osObjName	Object Name	string	

EventType: PH_UTIL_INVALID_PARAM

Description: Invalide parameter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
details	Details	string	

EventType: PH_UTIL_IOCTL_FAILURE

Description: Failed to run ioctl commands

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_IOCTL_SIOCGIFADDR_FAILURE

Description: Failed to run ioctl SIOCGIFADDR command

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_IP_TYPE_INVALID

Description: Invalid IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_IP_TYPE_MISMATCH

Description: Mismatch IP type

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_JOB_STATUS_REPORTER_SPAWN_FAILURE

Description: Failed to initialize job status reporter thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_JOB_STATUS_UPLOAD_FAILURE

Description: Failed to upload job status xml after 3 retries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_JSON_GET_NODE_FAILURE

Description: Failed to get JSON node value from App Server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
jsonBody	JSON Body	string	

EventType: PH_UTIL_JSON_GET_TOTAL_COUNT_FAILURE

Description: Failed to fetch total_count

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_JSON_OBJ_EMPTY

Description: JSON object empty

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_JSON_PARSE_FAILURE

Description: Failed to parse JSON

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason
jsonBody	JSON Body	string	

EventType: PH_UTIL_KILLPG_FAILURE

Description: Failed to send SIGKILL to child process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_LOAD_EXT_FUNC_FILE_OPEN_FAILUE

Description: Dynamic loaded function load failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_LOAD_EXT_FUNC_FORMAT_INVALID

Description: Dynamic loaded function name should be fileName.functionName format

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propValue	Property Value	string	

EventType: PH_UTIL_LOAD_EXT_FUNC_GET_NAME_FAILUE

Description: Dynamic loaded function in file failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
funName	Function Name	string	
filePath	File Path	string	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_LOCAL_IP_MISSING

Description: Failed to get ip address of this machine

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_LOOKUP_TABLES_DUPLICATE

Description: Duplicate lookup table found

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbTable	Database Table	string	

EventType: PH_UTIL_LOOKUP_TABLES_DUPLICATE_COLUMN

Description: Duplicate lookup table column found

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbTable	Database Table	string	
dbColumn	Database Column	string	

EventType: PH_UTIL_LOOKUP_TABLES_DUPLICATE_KEY

Description: Duplicate lookup table key found

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
dbTable	Database Table	string	
dbId	DB ID	uint32	

EventType: PH_UTIL_MAIL_CMD_RUN_FAILURE

Description: Failed to send email to server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destName	Destination Host Name	string	Destination device's hostname as identified in the log, can also be enriched using reverse lookup of the destination IP address.

EventType: PH_UTIL_MAIL_SMTP_INIT_FAILURE

Description: Fail to initialize SMTP server problem

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_MD5_ERROR

Description: Failed to calculate MD5

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_MEM_ALLOC_FAILURE

Description: Could not allocate memory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileSize64	File Size64 Bytes	uint64	

EventType: PH_UTIL_MKDTEMP_FAILURE

Description: Failed to create directory

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
filePath	File Path	string	

EventType: PH_UTIL_MKSTEMP_FAILURE

Description: Failed to create temporary filename

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
filePath	File Path	string	

EventType: PH_UTIL_MMAP_FAILURE

Description: Failed to mmap file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
fileSize64	File Size64 Bytes	uint64	
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_MOVE_FILE_FAILURE

Description: Failed to rename file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_NOTIFICATION_SENDER_SPAWN_FAILURE

Description: Failed to initialize notification sender thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_NOTIFICATION_SERVER_INIT_FAILURE

Description: Failed to initialize notification reporter

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_NOTIFICATION_UPLOAD_FAILURE

Description: Failed to Send Notification

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msg	Message	string	

EventType: PH_UTIL_PCRE_COMPILE_FAILED

Description: pcre_compile regex error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_PHOENIX_CONFIG_ITEM_MISSING

Description: Could not find specific item in phoenix_config.txt

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propName	Property Name	string	

EventType: PH_UTIL_PIPE_FAILURE

Description: The command pipe() returned error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_PROP_DEF_SET_PARSE_FAILURE

Description: Failed to parse propertyDefs xml

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
xmlBody	XML Body	string	

EventType: PH_UTIL_REDIS_CONNECTION_ERROR

Description: redis connection error

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_REGEX_PATTERN_EMPTY

Description: Regex Pattern is NULL

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_REGEX_PATTERN_TOO_LONG

Description: Regex Pattern too long

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
msgLen	Message Length	uint64	

EventType: PH_UTIL_SEND_DATA_FAILED

Description: Failed to sent data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpAddr	Destination IP	IP	Destination IP of a device as identified in the event.
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_UTIL_SEND_TO_UDP_PORT_FAILURE

Description: Failed to send message to udp port

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
destIpPort	Destination TCP/UDP Port	uint16	This is the destination TCP or UDP port as identified in the event

EventType: PH_UTIL_SETPGRP_FAILURE

Description: Failed to run system comand setpgrp()

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_SET_JOB_STATUS_FAILURE

Description: Failed to set job status to status file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
fileName	File Name	string	
paraName	Param Name	string	

EventType: PH_UTIL_SOCKET_FAILURE

Description: Failed to run system command socket()

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_STR_TO_IP_FAILURE

Description: Failed to run system call inet_pton

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propValue	Property Value	string	

EventType: PH_UTIL_SVN_DIFF_FAILURE

Description: Failed to execute system command svn diff

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_SYS_ERROR_REPORTER_INIT_FAILURE

Description: Failed to initialize system error reporter thread

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_UTIL_TIME_RANGE_INVALID

Description: Found Invalid time range

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
propValue	Property Value	string	

EventType: PH_UTIL_TIME_STR_FORMAT_INVALID

Description: Found incorrect time string parameters

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
paraName	Param Name	string	

EventType: PH_UTIL_TLS_SERVER_RECV_FAILED

Description: Tls server failed to receive data

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorString	Error String	string	This is the error message, synonymous to attribute errReason

EventType: PH_UTIL_UNKNOWN_PHOENIX_ERROR_NUMBER

Description: Found incorrect PH error number

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_UTIL_VALUE_GROUP_ERROR

Description: Encountered Value group error

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_WAITPID_FAILURE

Description: Failed to run system command waitpid on child process

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_WAITPID_LAST_TRY_FAILURE

Description: Failed to run system command waitpid on child process after several tries

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_WINDOWS_BID_LOAD_FAILURE

Description: Failed to load Windows Built In SID file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_UTIL_WRITE_BIN_FILE_OPEN_FAILURE

Description: Failed to open binary file

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	

EventType: PH_UTIL_WRITE_FILE_OPEN_FAILURE

Description: Failed to open file for write

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
filePath	File Path	string	
errorNoInt	Error Number Int	int32	

EventType: PH_UTIL_XML_HANDLING_ERROR

Description: Found Invalid xml from App Server

Severity: 10 (High)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_UTIL_ZIP_DECOMPRESS_FAILED

Description: Failed to decompress zip string

Severity: 3 (Low)

Event Category: 3 (System Logs)

EventType: PH_VA_EVENTS_PER_SEC

Description: Total event rate to an FortiSIEM VA

Severity: 1 (Low)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
peakEventsPerSec	Peak Event Rate	double	

EventType: PH_VA_LICENSE_UPDATE

Description: License on VA has been updated

Severity: 5 (Medium)

Event Category: 3 (System Logs)

EventType: PH_VULN_LOAD_ERROR

Description: Parser module failed to load external scanner-found vulnerabilities from App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_VULN_UPDATE_ERROR

Description: Parser module failed to upload external scanner-found vulnerabilities to App server

Severity: 7 (Medium)

Event Category: 3 (System Logs)

Attributes:

Id	Display name	Type	Description
errReason	Reason for Error	string	This is the reason for an error if given.

EventType: PH_WORKER_DOWN

Description: Worker down

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_WORKER_PROVISION_FAILED

Description: Phoenix worker provision failed

Severity: 7 (Medium)

Event Category: 3 (System Logs)

EventType: PH_WORKER_UP

Description: Worker up

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: PH_WS_COMM_ERROR

Description: Web service communication error

Severity: 6 (Medium)

Event Category: 3 (System Logs)

EventType: WEBSENSE_MAIL_JDBC_PULL_STAT

Description: JDBC Event pull statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)

EventType: WEBSENSE_WEB_JDBC_PULL_STAT

Description: JDBC Event pull statistics

Severity: 1 (Low)

Event Category: 3 (System Logs)



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.