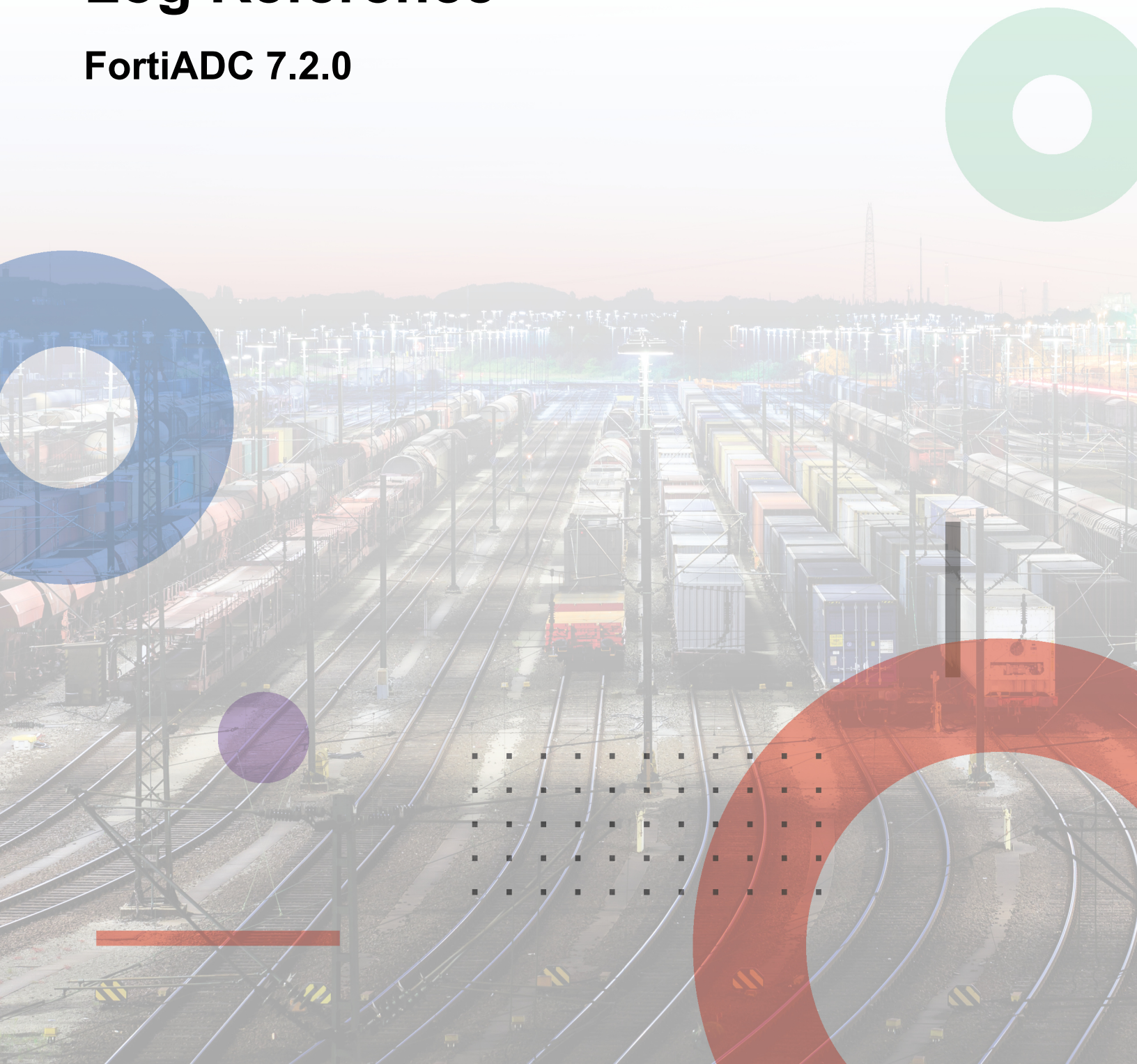
FORTINET

Log Reference

FortiADC 7.2.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 3, 2023
FortiADC 7.2.0 Log Reference
01-600-650988-20200902

TABLE OF CONTENTS

Change Log

Date	Change Description
February 3, 2023	FortiADC 7.2.0 Log Reference initial release.

Introduction

This document discusses the various types of logs that FortiADC appliance generates, describing the log formats and the data contained in the logs. The goal is to help system administrators better understand the log messages so that they can have a better idea about their network traffic and system performance.

Anatomy of a log message

This section discusses the composition of a log message.

Log message header vs. log message body

As illustrated above, a log message consists of a number of message fields, which can be separated into two part: log message header and log message body.

- Log message header—The log message header shows a log's date, time, log ID, administrative domain, type, sub-type, and priority. *These fields exist in all log types.*
- Log message body—The log message body describes the reason that the log was generated and the action that the FortiADC appliance took in response. *These fields vary by log type.*

Example log messages

The log messages below are provided to help you understand the composition of FortiADC log messages. Note that these are raw log messages that you see from the FortiADC Console or when log file you opened in a text editor. Some of the fields may look slightly different from the formatted log messages that you see on the GUI.

Note: The log message body in the following example log messages is intentionally marked in BOLD to help distinguish it from the log message header.

Event log

```
date=2018-01-23 time=16:18:15 log_id=0000000100 type=event subtype=config
pri=information vd=root msg_id=39242021 user=admin ui=GUI(172.30.16.64)
action=add cfgpath=global-load-balance data-center cfgobj=name cfgattr=dc1
logdesc=Change the configuration msg=added a new entry 'dc1' for "global-load-
balance data-center" on domain "root"
```

Traffic log

```
date=2018-01-20 time=15:27:40 log_id=0101008001 type=traffic subtype=slb_http
pri=information vd=root msg_id=39233799 duration=0 ibytes=150 obytes=258 proto=6
service=http src=192.168.1.10 src_port=50758 dst=192.168.1.141 dst_port=80 trans_
```

```
src=2.2.2.1 trans_src_port=23992 trans_dst=2.2.2.10 trans_dst_port=80
policy=test11111111111111111111111111111111 action=none http_method=get http_
host=192.168.1.141 http_agent=Wget/1.16.3 (linux-gnu) http_url=/index.html http_
qry=none http_referer=none http_cookie=none http_retcode=200 user=none
usrgrp=none auth_status=none srccountry=Reserved dstcountry=Reserved real_
server=s1
```

Security log

```
date=2018-01-11 time=09:13:21 log_id=0201006003 type=attack subtype=synflood
pri=alert vd=root msg_id=38284198 count=18287 severity=high proto=6 service=tcp
src=0.0.0.0 src_port=0 dst=192.168.1.141 dst_port=0 policy=l7vs action=deny
srccountry=Reserved dstcountry=Reserved
```

Script log

```
date=2018-02-08 time=19:31:45 log_id=0300010000 type=script subtype=slb
pri=information vd=priceminister msg_id=3291 obj_name=Virtual Server obj_
value=VIP_narcisse_443 msg="agent iphone matches UA mobile "
```

Log types and sub-types

FortiADC log messages fall into four major types or categories, each of which has a number of sub-types or sub-categories.

Major log types

The table below lists the four major log types and their functions.

Major log types and their functions

Log type	Description
Event Log	Records system or administrative events, such as downloading a backup copy of the configuration or daemon activities
Traffic Log	Records network traffic information, such as HTTP or HTTPS requests and responses, etc.
Security Log	Records attack or intrusion attempts.
Script Log	Records the use of server load-balance scripts.

Log Sub-types

The table below lists the sub-types of each major log type.

Major log types and their sub-types

Log type	Sub-type
Event Log	• Configuration • System • Admin • User • Health Check • SLB • LLB • GLB • Firewall
Traffic Log	• SLB Layer 4 • SLB HTTP • SLB TCPS • SLB RADIUS • GLB • SLB SIP • SLB RDP • SLB DNS • SLB RTSP • SLB SMTP • SLB RTMP • SLB DIAMETER • SLB MySQL
Security Log	• IP Reputation • Synflood • WAF • GEO • AV
Script Log	• SLB

Note: You can see all the log types and their sub-types from the GUI by clicking Log & Report >Log Browsing.

Log ID schema

The FortiADC log ID `(log_id)` is a 10-digit number. The first two digits stand for the major log type, the second two digits stand for the sub-type of a major log type, and the remaining six digits are specific to log content.

Log Type ID

The table below lists FortiADC's major log types and sub-types, along with their corresponding IDs numbers.

Type	Type ID	Sub-type	Sub-type ID
Event	00		
		Configuration	00
		Admin	01
		Health Check	02
		System	03
		User	04
		SLB	05
		LLB	06
		GLB	07
		Firewall	08
Traffic	01		
		SLB Layer 4	00
		SLB HTTP	01
		SLB TCPS	02
		SLB RADIUS	03
		GLB	04
			05 (Reserved)
		SLB SIP	06
		SLB RDP	07
		SLB DNS	08
		SLB RTSP	09
		SLB SMTP	10
		SLB RTMP	11
		SLB MySQL	12
		SLB DIAMETER	13
Security	02		
		IP Reputation	00
		Synflood	01
		WAF	02
		GEO	03

Type	Type ID	Sub-type	Sub-type ID
		AV	
Script	03		
		SLB	00

Event logs

This chapter covers various types of event logs, which fall into the following subcategories:

- Configuration change
- Admin
- Health check
- system
- User authentication
- Server load balancing
- Link load balancing
- Global load balancing
- Firewall

Configuration

This section describes log messages involving FortiADC system administration, which are a subcategory of the event log.

0000000100 (configuration change)

This log ID represents a subtype of the event log. It could mean any changes made to the configuration of your FortiADC unit. The actions (changes) could be edit, delete, add, or backup.

All 000000100 (configuration change) log messages include the following fields:

- `cofgobj` —configuration object
- `cfgpath` —configuration path
- `cfgattr`—configuration attribute

For instance, if the administrator has changed the IP address for Port 1 from 192.168.1.99/24 to 172.30.154,141, the event will be logged as below:

```
date=2018-01-23 time=16:18:15 log_id=0000000100 type=event subtype=config
pri=information vd=root msg_id=39242021 user=admin ui=GUI(172.30.16.64)
action=add cfgpath=global-load-balance data-center cfgobj=name cfgattr=dc1
logdesc=Change the configuration msg=added a new entry 'dc1' for "global-load-
balance data-center" on domain "root"
```

0001001000 (admin login)

These log messages relate to administration login events to your FortiADC unit. The same log ID could cover any of the following events:

Admin login failed

Message:`User [name] login failed from [GUI|ssh|console]`

Meaning: Login attempt by (user name) from the GUI/SSH/Console failed.

Priority: Notification

Admin login failed for 3 times

Message:`User [name] from [GUI|ssh|console]has been tried more than 3 times.`

Meaning: Login attempts by (user name) from the GUI/SSH/Console failed for three times

Priority: Notification

Admin login failed for blockip

Message:`User [name] login failed from blocked ip [ip address]`

Meaning: Login attempt by (user name) from (IP address) was denied because this IP address was blocked.

Priority: Notification

Admin login success

Message:`User [name] login successfully from [GUI|ssh|console]`

Meaning: (User name) successfully logged into the unit from the GUI/SSH/Console.

Priority: Information

0001001001 (admin logout)

These log messages relate to administration logout events from your FortiADC unit. The same log ID could cover either of the following events:

Admin logout

Message:`User [name] logout from [GUI|ssh|console]`

Meaning: (User name) logged out from the GUI/SSH/Console.

Priority: Information.

Admin timeout

Message:`User [name] time out from [GUI|ssh|console]`

Meaning: (User name) was logged out from the GUI/SSH/Console because the session had been idle for too long.

Priority: Information.

Admin

This section describes log messages involving FortiADC system administration, which are a subcategory of the event log.

0001001000 (admin login)

These log messages relate to administration login events to your FortiADC unit. The same log ID could cover any of the following events:

Admin login failed

Message: `User [name] login failed from [GUI|ssh|console]`

Meaning: Login attempt by (user name) from the GUI/SSH/Console failed.

Priority: Notification

Admin login failed for 3 times

Message: `User [name] from [GUI|ssh|console]has been tried more than 3 times.`

Meaning: Login attempts by (user name) from the GUI/SSH/Console failed for three times

Priority: Notification

Admin login failed for blockip

Message: `User [name] login failed from blocked ip [ip address]`

Meaning: Login attempt by (user name) from (IP address) was denied because this IP address was blocked.

Priority: Notification

Admin login success

Message: `User [name] login successfully from [GUI|ssh|console]`

Meaning: (User name) successfully logged into the unit from the GUI/SSH/Console.

Priority: Information

0001001001 (admin logout)

These log messages relate to administration logout events from your FortiADC unit. The same log ID could cover either of the following events:

Admin logout

Message:`User [name] logout from [GUI|ssh|console]`

Meaning: (User name) logged out from the GUI/SSH/Console.

Priority: Information.

Admin timeout

Message:`User [name] time out from [GUI|ssh|console]`

Meaning: (User name) was logged out from the GUI/SSH/Console because the session had been idle for too long.

Priority: Information.

Health check

This section describes log messages regarding health checks. They are a subcategory of the event log.

0002001800 (health check llb)

These log messages relate to health check for link load balancing (LLB) configuration on your FortiADC unit. The same log ID could cover either of the following events:

LLB gateway change status

Message:`Gateway [name] is [up|down]`

Meaning: (Gateway name) is up/down.

Priority: Alert.

LLB virtual tunnel change status

Message:`virtual tunnel [name] member [name] is [up|down]`

Meaning: (virtual tunnel name) (member name) is up/down.

Priority: Alert.

0002001801 (health check slb)

These log messages relate to health check for server load balancing (SLB) configuration on your FortiADC unit. The same log ID could cover either of the following events:

SLB VS change status

Message:`Virtual server [name], status is [up|down]`

Meaning: (virtual server name) is up/down.

Priority: Alert

SLB RS change status

Message:`Pool name [name] realserver name [name], ip [ip address] and port [port number] was detected as [up|down] by Health Check [name]`

Meaning: The health check found (server pool name) (real server name) with (IP address) and (port number) was up/down.

Priority: Alert.

0002001802 (snmp healthcheck over threshold)

This log ID relates to a health check result involving snmp healthcheck over threshold.

Message: `Pool name [pool_name] realserver name [real server name], ip [IP] and port [port] was [over/less] snmp threshold health-check in Health Check [checker name]`

Meaning: snmp healthcheck over threshold

Priority: Alert

System

This section describes log messages involving various system events, which fall into the system sub-category of the event log.

0003000200 (certificate expired)

This log ID relate to the following event logs regarding the state of the local certificate on your FortiADC unit.

Local certificate to be expired

Message: `Local certificate [name] is going to expire in 1 week.`

Meaning: The local certificate will expire in one week.

Priority: Warning.

Local certificate expired

Message: `Local certificate [name] is expired !!`

Meaning: (Local certificate name) is expired!

Priority: Critical.

0003000201 (crl update)

This log ID relates to a system event involving the update of the CRL (certificate revocation List).

CRL update succeeded

Message:`Get/Update succeeded (CRL=[name] DP=[name])`

Meaning: (CRL name) from (DP) was successfully updated.

Priority: Information.

CRL update failed

Message:`Failed to save updated CRL[name] from DP [name]`

Meaning: The system failed to save the updated (CRL name) from (DP).

Priority: Information.

0003000202 (system reboot)

This event log ID indicates that your FortiADC unit was rebooted.

Message:`System has been restarted`

Meaning: An administrator restarted the unit using the CLI or web-based manager.

Priority: Warning

0003000203 (system shutdown)

This event log ID indicates that your FortiADC unit was shut down.

Message:`System has been shutdown`

Meaning: An administrator has shut down the unit.

Priority: Warning

0003000204 (clean isp address)

This log ID relates to a system event involving the clean-up of the restored ISP address book.

Message:`Clean restored ISP address-books`

Meaning: The restored ISP address book was cleaned.

Priority: Warning

0003000205 (configuration backup)

This log ID relates to the backup of system configuration on your FortiADC unit.

Message:`Backup configuration [config name] to FortiADC disk [failed|successful]`

Meaning: The system configuration (file name) was successfully backed up or failed to be backed up onto the FortiADC disk.

Priority: Warning (when failed) or Notice (when succeeded)

Message:`Backup files reach [file number] and overwrite is disable`

Meaning: The number of configuration backup files has reached the set limit and the system is not allowed to overwrite previous configuration backups.

Priority: Warning

Message:`Total configuration file reach maximum size and overwrite is disable`

Meaning: The size of all configuration backup files combined has reached the set limit, and the system is not allowed to overwrite previous configuration backups.

Priority: Warning

Message:`Backup the configuration to tftp server [server ip] as [file name] [failed| successful]`

Meaning: The system configuration was successfully backed up or failed to be backed up onto the TFTP server (server IP).

Priority: Warning (when failed) or Notice (when succeeded)

Message:`Backup the configuration to sftp server [server ip] as [file name] [failed| successful]`

Meaning: Backing up the system configuration (file name) onto the TFTP server (server IP) failed or succeeded.

Priority: Warning (when failed) or Notice (when succeeded)

Message:`SFTP server [server ip] is unreachable`

Meaning:The SFTP server (server IP) could not be reached during configuration backup.

Priority: Warning

Message:`Login failed to sftp server [server ip]`

Meaning: Attempt to log into the SFTP server (server IP) failed when doing configuration backup.

Priority: Warning

Action: Make sure your username and password as valid.

Message:`Unable to write file in path [directory name] of sftp server [server ip]`

Meaning: The system was unable to write files to the path (directory name) on the SFTP server.

Priority: Warning

Action: Double-check the permission settings.

0003000206 (isp address book backup)

This log ID relates to a system event involving the backup of the ISP address books.

Message:`Backup ISP address-books to tftp server [server_name] as [file_name]`

Meaning: The ISP address book (file name) was backed up onto the TFTP server (server name).

Priority: Warning

0003000207 (log backup)

This log ID relates to a system event involving the backup of log files.

Message:`backup log to ftp server [server ip]`

Meaning: The logs were backed up on FTP server (server IP).

Priority: Warning.

0003000208 (generate local certificate by scep)

This event log ID relates to a system event involving the generation of a local certificate by SCEP.

Message: `Local certification generated by SCEP`

Meaning: A local certificate was generated by SCEP.

Priority: Information.

0003000209 (import ca certificate)

This event log ID relates to a system event involving the import of a CA certificate.

Message:`CA certification is retrieved from SCEP server"`

Meaning: A CA certificate was retrieved from the SCEP server.

Priority: Information.

0003000210 (import crl)

This event log ID relates to a system event involving the import of a CRL (Certificate Revocation List).

Message:`CRL is retrieved from SCEP server`

Meaning: A CRL was retrieved from the SCEP server.

Priority: Information.

0003000211 (import ocsp response)

This log ID relates to a system event involving the import of an OCSP (Online Certificate Status Protocol) response.

Message:`import OCSP response through ftp log`

Meaning: A new OCSP response was updated to system through FTP server.

Priority: Information

0003000212 (set system time)

This log ID relates to a system event involving the setting of system time.

Message:`set system time to [date][time].`

Meaning: The system time was set to (date) (time).

Priority: Warning.

0003000213 (system reset)

This log ID relates to a system event involving resetting FortiADC to its factory (default) settings.

Message:`system has been reset to factory default.`

Meaning: An administrator has reset the system to its factory default from the GUI, Console, or LCD.

Priority: Warning.

0003000214 (log rebuilt)

This log ID relates to a system event involving the rebuild of logs on the system.

Message:`log rebuild on [root vdom|domain [name]] db`

Meaning: The log was rebuilt on [root VDOM | (domain name)] database.

Priority: Warning.

0003000215 (log deleted)

This log ID relates to system events involving the delete of logs.

Message:`delete type [elog|tlog|alog|all type] log`

Or Delete log [log file name]

Meaning: The log type (event/traffic/security/all) were deleted.

Priority: Warning.

Or

Message:`delete log [log file name]`

Meaning: The (log file name) deleted.

Priority: Warning.

0003000216 (system reloaded)

This log ID relates to a system event involving reloading the system with applications.

Message:`system (version) has been reloaded`

Meaning: The administrator reloaded the system (version) using the GUI/Console.

Priority: Warning

0003000217 (firmware upgraded)

This log ID relates to a system event involving the system's firmware upgrade.

Message:`system firmware has been upraded from version1 to version2`

Meaning: An administrator has upgraded the system firmware from version 1 to version 2 using the GUI/Console.

Priority: Warning.

0003000218 (firmware downgraded)

This log ID relates to a system event involving the system's firmware downgrade.

Message:`System firmware has been downgraded from version2 to version1`

Meaning: An administrator has downgraded the system's firmware from version 2 to version 1 using the GUI/Console.

Priority: Warning

0003000219 (firmware error)

This log ID relates to a system event involving a firmware error on the system.

Message:`Check image error`

Meaning: The uploaded image was not a FortiADC firmware image.

Priority: Warning

0003000220 (crypto license upgraded)

This log ID relates to a system event involving the update of the system's cryptographic license.

Message:`crypto license has been updated`

Meaning: The system's crypto license has been updated.

Priority: Warning.

0003000221 (isp address-books updated)

This log ID relates to a system event regarding update of the ISP address book.

Message:`update restored ISP address-books`

Meaning: The restored ISP address-books were updated.

Priority: Warning

0003000222 (database reset)

This log ID relates to a system event involving the reset of the statistics database.

Message:`statistics db will be reset`

Meaning: The statistics database will be reset.

Priority: Warning.

0003000223 (database restore)

This log ID relates to a system event involving the restore of the statistics database.

Message:`statistics db will be restored`

Meaning: The statistics database will be restored.

Priority: Warning.

0003000224 (alert delete)

This log ID relates to a system event involving the removal of alert messages.

Message:`delete an alert alert_for_cpu_too_high with id 3,alertname,alertid`

Meaning: The alert "`alert_for_cpu_too_high with ID 3`" is deleted from the system.

Priority: Warning

0003000225 (ca retrieved)

This log ID relates to a system event involving the retrieval of a CA.

Message:`CA was successfully retrieved from SCEP server`

Meaning: (CA) was successfully retrieved from the SCEP server.

Priority: Information.

0003000226 (intermediate ca retrieved)

This log ID relates to a system event involving the retrieval of an intermediate CA.

Message:`intermediate CA was successfully retrieved from SCEP server`

Meaning: (Intermediate CA) was successfully retrieved from the SCEP server.

Priority: Information.

0003000227 (csr vdom)

This log ID relates to a system event to generate a CSR used to create a local certificate.

Message:`generate csr log`

Meaning: A Certificate Signing Request (CSR) certificate was generated to the system.

Priority: Information

0003000228 (generate local certificate)

This log ID relates to a system event involving the generation of a local certificate.

Message:`generate local certificate log`

Meaning: local certificate was generated.

Priority: Information

See Log 0003000208.

0003000229 (import certificate)

This log ID relates to a system event involving the import of a certificate.

Message:`import local certificate log`

Meaning: A certificate was uploaded to the system as a local certificate.

Priority: Information

0003000230 (remote certificate retrieved)

This log ID relates to a system event involving the retrieval of a remote certificate.

Message:`import remote certificate log.`

Meaning: A certificate was uploaded as an OCSP-signing certificate.

Priority: Information

0003000231 (log download)

This log ID relates to a system event involving log download.

Message:`Download log successfully.`

Meaning: An attempt to download the log was successful.

Priority: Warning

Or

Message:`Download log failed.`

Meaning: Attempt to download the log failed.

Priority: Warning

0003000232 (delete report)

This log ID relates to a system event involving deleting a report file.

Message:`report [filename] is deleted`

Meaning: The report (filename) was deleted.

Priority: Warning

0003000233 (delete log table)

This log ID relates to a system event involving deleting a log table.

Message:`Upgrade the log db since the log format is changed.`

Meaning: Due to log format change, the log index table was updated (rebuilt).

Priority: Warning

0003000234 (port status changed)

This log ID relates to a system event involving the change of port status.

Message:`[port name] status changed from [up|down] to [up|down]`

Meaning: The status of (Port number) changed from (up/down) to (down/up).

Priority: Notification

0003000235 (vm license update)

This log ID relates to a system event involving the update of VM licenses.

Message:`vm license has been updated`

Meaning: The administrator has updated the VM license.

Priority: Warning

0003000236 (log db failed to start)

This log ID relates to a system event involving a failed attempt to launch the log database.

Message:`The DB server can not start correctly ...`

Meaning: The database server could not be started correctly.

Priority: Warning

0003000237 (get log version failed)

This log ID relates to a system event involving a failed attempt to get the log version.

Message:`Can not get the log file 1.admin.elog version and create new log file`

Meaning: The system could not get the version of the log file "1.admin.elog" in the file's header to create a new log file.

Priority: Critical

0003000238 (create log file)

This log ID relates to a system event involving the creation of a log file.

Message:`Create new log file 2.admin.elog for upgrade the log.`

Meaning: A new log file "`2.admin.elog`" was created when upgrading the log.

Priority: Warning

Message:`Create new log file 2.admin.elog for checking msgid wrongly.`

Meaning: A new log file "`2.admin.elog`" was created when checking the message ID of the log.

Priority: Warning

0003000239 (generate self-signed certificate)

This log ID relates to a system event involving the generation of a self-signed certificate.

Message:`generate the self signed certificate log.`

Meaning: A self-signed certificate was generated.

Priority: Information

0003000240 (temperature high)

This log ID relates a system event involving the temperature of the system's CPU.

Message:`Temperature of [CPU] is high: [number] C`

Meaning: The temperature of the CPU is high.

Priority: Critical

0003000241 (temperature critical)

This log ID relates to a system event involving extremely high CPU temperature.

Message:`[CPU ID | Device Sensor ID | PSU R/L] temperature [number] C hits threshold.`

Meaning: The temperature (digit in centigrade) of the (CPU ID | Device Sensor ID | PSU R/L) is over the threshold.

Priority: Critical

0003000242 (temperature normal)

This log ID relates to a system event involving normal CPU temperature.

Message:`Temperature of [CPU ID | Device Sensor ID | PSU R/L] back to normal`

Meaning: The temperature of the (CPU ID | Device Sensor ID | PSU R/L) is back to normal (cooling down).

Priority: Critical

0003000243 (fan bad)

This log ID relates to a system event involving the poor condition of the system cooling fan.

Message: [name] Device FAN id [number] is bad

Meaning: The system cooling fan is not working properly.

Priority: Error

0003000244 (fan slow)

This log ID relates to a system event involving the slow rotation of the system cooling fan.

Message:`[name] Device FAN id [number] is slow`

Meaning: The system (name) cooling fan (ID number) is slow.

Priority: Error

0003000245 (input voltage high)

This log ID relates to a system event involving high input voltage.

Message:`[device name] Input Voltage [device ID] is high:[number]`

Meaning: (Device name)'s input voltage is high: (numeric value).

Priority: Critical

0003000246 (input voltage low)

This log ID relates to a system event involving low input voltage.

Message:`[device name] Input Voltage [device ID] is low:[number]`

Meaning: (Device name)'s input voltage (device ID) is high: (numeric value)

Priority: Critical

0003000247 (hdd unhealthy)

This log ID relates to a system event involving the health state of the system hard disk drive.

Message:`Hard disk is NOT healthy`

Meaning: The hard disk drive is not healthy

Priority: Critical

0003000248 (ssd reached end of life)

This log ID relates to a system event involving the SSD reaching the end of its life.

Message:`SSD life reached threshold`

Meaning: The SSD has reached the end of its life.

Priority: Critical

0003000249 (ssd near end of life)

This log ID relates to a system event involving the SSD approaching the end of its life.

Message:`SSD life near threshold, has [number] left]`

Meaning: The SSD is approaching the end of its life.

Priority: Critical

0003000250 (device usage)

This log ID relates to a system event regarding FortiADC's disk usage.

Message:`device usage hit [number]percent`

Meaning: The FortiADC appliance's disk usage reached (percentage) of its capacity.

Priority: Warning

0003000251 (hdd mount status)

This log ID relates to a system event regarding the mount status of the hard disk drive.

Message:`device is not mounted`

Meaning: The HDD is not mounted.

Priority: Warning

0003000252 (log index table broken)

This log ID relates to a system event involving a broken log index table.

Message:`The log index table [name] is broken and rebuild it.`

Meaning: The log index table (name) was broken and was rebuilt.

Priority: Warning

0003000253 (log index non-existent)

This log ID relates to a system event involving a log index that did not exist.

Message:`The unexist log table elog.000000001 is deleted it.`

Meaning: The non-existent log index table is deleted

Priority: Warning

0003000254 (log db disk full)

This log ID relates to a system event involving available space on log database disk.

Message:`The log db disk is FULL! Delete some tables.`

Meaning: The log database disk was full. Some tables were deleted.

Priority: Warning

0003000255 (statistics disk full)

This log ID relates to a system event involving the available space in the statistics disk.

Message:`The statistics disk is FULL! Delete some tables`

Meaning: The statistics disk was full. Some tables were deleted.

Priority: warning

0003000257 (mount hdd failed)

This log ID relates to a system event involving a failed attempt to mount the HDD.

Message:`Failed to mount log partition`

Meaning: An attempt to mount the HDD failed.

Priority: Error

0003000258 (update fortiguard successful)

This log ID relates to a system event involving the result of update of FortiGuard.

Message:`Update result: OK`

Meaning: FortiGuard was successfully updated.

Priority: Information

0003000259 (report disk full)

This log ID relates to a system event involving the available space of the disk used to store reports.

Message:`The report disk is full!`

Meaning: The disk used to store reports was full.

Priority: Warning

0003000260 (report expired)

This log ID relates to a system event involving an expired report.

Message:`The report On-Schedule-SLB-2018-01-05-090000 timeout`

Meaning: The report `On-Schedule-SLB-2018-01-05-090000` took too long to execute. No report was generated because it timed out.

Priority: Warning

0003000261 (ha switch console received)

This log ID relates to a system event involving the HA switch console.

Message:`Received switch console from SN.`

Meaning: An HA switch console was received from an appliance (serial number).

Priority: Information

0003000262 (ha switch console)

This log ID relates to a system event involving the HA console.

Message:`Switch console to SN.`

Meaning: Some log oAn HA switch console was received

Priority: Information

0003000263 (ha secondary sync)

This log ID relates to a system event involving the synchronization of the secondary with the primary in an HA configuration.

Messages:

```
(1) The Configuration is different from CfgPrimary, System will be
reloaded.
(2) The Secondary device synchronized failed.
(3) File (filename md5) received successfully.
(4) File (filename) received failed.
(5) File (filename md5) sending finished.
(6) File (filename) sending failed.
(7) Operated File filename Exception.
(8) System Exception:cmd commandline failed!
```

```
(9) The Secondary device has fully synchronized and will be reloaded.
```

Meaning:

- configuration sync
- file sync
- Exception of sync

Priority: Informaiton

0003000264 (ha forced sync)

This log ID relates to a system event involving forced sync of HA configuration.

Message: The Secondary device has fully synchronized and will be reloaded.

Meaning: HA forced sync

Priority: Information

0003000265 (ha system upgrade)

This log ID relates to a system event involving the system upgrade of an HA configuration.

Message:`System is upgrading`

Meaning: The system is being upgraded.

Priority: Information

0003000266 (ha received image)

This log ID relates to a system event involving the system image delivered to an HA configuration.

Message:`Received image from [dev sn]`

Meaning: The system image was received from (server name).

Priority: Information

0003000267 (ha remote IP status changed)

This log ID relates to a system event involving the HA remote IP status change.

Message:`Remote ip %s is [up|down]`

Meaning: Remote IP (address) is up/down.

Priority: Information

0003000268 (ha remote ip inactive too long)

This log ID relates to a system event involving the HA remote IP that has been inactive beyond the configured threshold.

Message:`Gateway inactive count exceed threshold`

Meaning: The HA gateway has been idle beyond the configured threshold.

Priority: Information

0003000269 (ha disk check)

This log ID relates to a system event involving an HA disk check.

Message:`Disk check failure`

Meaning: An attempt to check the HA disk failed.

Priority: Information

0003000270 (ha push image)

This log ID relates to a system event involving installing the system image onto an HA node.

Message:`Pushing image to node [name]`

Meaning: The HA image was pushed to node (name).

Priority: Information

0003000271 (ha full config sync)

This log ID relates to a system event involving full HA configuration sync.

Message:`Full configuration sync failed`

Meaning: Attempt to run a full HA sync failed.

Priority: Information

0003000272 (ha init)

This log ID relates to a system event involving the initiation of an HA node.

Message:`HA device init`

Meaning: The HA device was initiated.

Priority: Information

0003000273 (ha change mode)

This log ID relates to a system event involving an HA device's mode change.

Message:`HA device moved into [primary|secondary] mode`

Meaning: The HA device changed to (primary/secondary) mode

Priority: Information

0003000274 (ha device joined group)

This log ID relates to a system event involving a device that joined an HA group.

Message:`Member (name) join to the HA group`

Meaning: HA member device (name) joined the HA group.

Priority: Information

0003000275 (ha device left group)

This log ID relates to a system event involving a HA device that was removed from the HA configuration.

Message:`Member ([name]) leave from the HA group`

Meaning: The HA member (device name) left the HA group.

Priority: Information

0003000276 (ha interface state changed)

This log ID relates to a system event involving an HA interface's change of operating state.

Message:`[name] change state to [up|down]`

Meaning: The HA interface (name) has changed to up/down.

Priority: Information

0003000277 (ha traffic group work node changes)

This log ID relates to a system event involving the change in an HA traffic group's work node.

Message:`groupname work node change to nodeid`

Meaning: The ha traffic group work node has changed to (node ID).

Priority: Information

0003000278 (ha executed forced sync)

This log ID relates to a system event involving the execution of a forced HA sync.

Message:

(1) `sync-config`

(2) `standby`

Meaning: An HA forced sync was executed.

Priority: Information

0003000279 (arp conflict)

This log ID relates to a system event involving network traffic ARP conflict.

Message:`Detect MAC address xx:xx:xx:xx:xx:xx claims to have our IP x.x.x.x`

Meaning: An ARP conflict was detected.

Priority: Error

0003000280 (link status changed)

This log ID relates to a system event involving a network interface link status change.

Message:`Link status changed`

Meaning: A network interface link status has changed.

Priority: Notify

0003000281 (port exhausted)

This log ID relates to a system event involving unavailability of source ports.

Message:`Cannot find available source port from port range [port] to [port]`

Meaning: No source port was available from Port (number) to Port (number).

Priority: Notify

0003000282 (log disk full)

This log ID relates to a system event involving unavailability of log disk space.

Message:`The log disk is FULL`

Meaning: The system ran out of log disk space.

Priority: Notify

0003000283 (log rotate)

This log ID relates to a system event involving a log file rotation.

Message:`The log 2.admin.elog is rotated.`

Meaning: The log file "`2.admin.elog`" is too big. Close it and open the file "`3.admin.elog`" instead to record log.

Priority: Warning

0003000284 (share memory disk full)

This log ID relates to a system event involving lack of shared memory.

Message:`Share memory disk is full.`

Meaning: The system has run out shared memory.

Priority: Warning

0003000285 (ha vrrp group changed)

This log ID relates to a system event involving an HA VRRP group change.

Message:`node id [up|down] [join | leave | update] trafficgroupname`

Meaning: The node (whose status is up/down) has joined/ left the HA VRRP group.

Priority: Information

0003000286 (geoip database updated)

This log ID relates to a system event regarding update of the geography ip database.

Message:`update geography ip database`

Meaning: The geography ip database is updated

Priority: Information

0003000287 (ip reputation database updated)

This log ID relates to a system event regarding update of the ip reputation database.

Message:`update ip reputation database`

Meaning: The IP reputation database is updated.

Priority: Information

0003000288 (system voltage recovered)

This log ID relates to a system event involving voltage recover from error.

Message:`[device name] Input Voltage [device id] back to normal [number]`

Meaning: The (device name) input voltage has recovered from an error.

Priority: Information

0003000289 (system fan recovered)

This log ID relates to a system event involving system fan recover from error.

Message: `[device name] Velocity of FAN back to normal`

Meaning: The (device name) system fan has recovered from an error.

Priority: Information

0003000290 (backup the GLB configuration)

These log messages relate to backup glb zone dnssec events to your FortiADC unit. The same log ID could cover any of the following events:

Backup successfully

Message: `Backup glb zone dnssec OK`

Meaning: Backup glb zone dnssec OK

Priority: Warning

Backup failed

Message: `Backup glb zone dnssec failed`

Meaning: Backup glb zone dnssec failed

Priority: Warning

Backup to server successfully

Message: `Backup glb zone dnssec to tftp server [server ip] as [filename] ok`

Meaning: Backup glb zone dnssec to server OK

Priority: Warning

Backup to server failed

Message: `Backup glb zone dnssec to tftp server [server ip] as [filename] failed`

Meaning: Backup glb zone dnssec to server failed

Priority: Warning

0003000291 (update reputation block list)

These log messages relate to update reputation block list events from your FortiADC unit. The same log ID could cover either of the following events:

Update reputation block list

Message: `update restored IP reputation block list`

Meaning: update restored IP reputation block list

Priority: Warning

0003000292 (clean restored IP reputation block list)

These log messages relate to clean reputation block list events from your FortiADC unit. The same log ID could cover either of the following events:

Clean reputation block list

Message: `clean restored IP reputation block list`

Meaning: clean restored IP reputation block list

Priority: Warning

0003000293 (backup restored IP reputation block list to tftp server)

These log messages relate to backup reputation block list events from your FortiADC unit. The same log ID could cover either of the following events:

Backup restored IP reputation block list to tftp server

Message: `Backup restored IP reputation block list to tftp server[server ip] as [filename] [ok/failed]`

Meaning: Backup restored IP reputation block list to tftp ok or failed

Priority: Warning

0003000294 (history statistics db will be upgraded)

This event log ID indicates that history statistics db will be upgrade.

Message: `history statistics db will be ugrade by [user]`

Meaning: history statistics db will be ugrade by [user]

Priority: Warning

0003000295 (history low version data in statistics db will be deleted)

This event log ID indicates that history statistics db will be upgrade.

Message: `history statistics db will be delete_low_version by [user]`

Meaning: history statistics db will be delete_low_version by [user]

Priority: Warning

0003000297 (LOG db will be upgraded)

This event log ID indicates that LOG db will be upgraded The same log ID could cover either of the following events:

Message: `log upgrade root vdom db`

Meaning: log upgrade root vdom db

Priority: Warning

Message: `log upgrade on domain [vdom name]`

Meaning: log upgrade on domain [vdom name]

Priority: Warning

00030298 (CM agent state changed)

This log ID relates to CM agent state changed on your FortiADC unit.

Message: `CM agent state changes to [status string]`

Meaning: CM agent state changes to [status string]

Priority: Information

00030299 (statistics DB upgrade cancel)

This log ID relates to a system event involving the system's statistics DB upgrade cancel.

Message: `history statistics db will be upgrade_and_cancel by user1`

Meaning: The action for upgrading the history statistics db has been canceled.

Priority: Warning

0003000300 (Traffic log is over quota)

This log ID relates to a system event involving the system's traffic log is over quota.

Message: `The traffic log is over quota! (stop to record logs)`

`Or The traffic log is over quota! (The oldest log will be overwritten)`

Meaning: The traffic log is over quota! (stop to record logs) or (The oldest log will be overwritten).

Priority: Warning

0003000301 (Attack log is over quota)

This log ID relates to a system event involving the system's attack log is over quota.

Message: `The attack log is over quota! (stop to record logs)`

`Or The attack log is over quota! (The oldest log will be overwritten)`

Meaning: The attack log is over quota! (stop to record logs) or (The oldest log will be overwritten).

Priority: Warning

0003000302 (system daemon process start or stop)

This log ID relates to a system event involving the system's process start or stop.

Message: `Daemon quarantine start`

`Or Daemon quarantine stop`

Meaning: Daemon quarantine start or stop.

Priority: Information

0003000303 (Load WAF Signature DB)

This log ID relates to a system event involving Load WAF Signature DB status.

Message: `WAF core load fail`

`Or Load WAF Signature DB successfully`

Priority: Error

0003000304 (Resolve real server FQDN)

This log ID relates to a system event involving Load WAF Signature DB status.

Message: `Primary [ Secondary] nameserver cannot be resolved, reason: "Network is unreachable`

Priority: Information

User Authentication

This section describes log messages involving user authentication events on the system. They are a subcategory of the event log.

0004001500 (user authentication)

This log ID relates to a system event involving user authentication queries.

Message:`valid authentication query`

Meaning: A valid user authentication query was received.

Priority: Information

Or

Message:`invalid authentication query`

Meaning: An invalid user authentication query was received.

Priority: Information

0004001501 (user authentication relay)

This log ID relates to authentication result when the virtual server binds to an authentication policy which uses authentication relay.

Message:`[Valid | Invalid] [authentication-relay | kerberos authentication-relay] query`

Meaning: An HTTP basic or Kerberos constrained delegation authentication succeeded or failed.

Priority: Information/Notification

Server Load Balance (SLB)

This section provides descriptions of the SLB log messages which fall into a sub-category of the event log.

0005002000 (script load file error)

This log ID relates to a system event involving error happened when loading a script file.

Message:`script file load error log`

Meaning: An error occurred when the system was loading a script file.

Priority: Error

0005002001 (script run time error)

This log ID relates to a system event involving an error that happened when running a script file.

Message:`script run-time error log`

Meaning: The system encountered an error happen when running a script file.

Priority: Error

0005002002 (slb transaction rate limit)

This log ID relates to a system event involving SLB transaction rate limit.

Message:`VS [name] has [reached|dropped below] its transaction rate limit [number]`

Meaning: Virtual server (name) has reached/dropped below its transaction rate limit (value).

Priority: Alert

Or

Message:`rs [name] has [reached|dropped below] its transaction rate limit [number]`

Meaning: Real server (name) has reached/dropped below its transaction rate limit (value).

Priority: Alert

0005002003 (slb connection rate limit)

This log ID relates to a system event involving SLB real server or virtual server connection rate limit.

Message:`VS [name] has [reached|dropped below] its connection rate limit [number]`

Meaning: Virtual server (name) has reached/dropped below its connection rate limit (value).

Priority: Alert

Or

Message:`rS [name] has [reached|dropped below] its connection rate limit [number]`

Meaning: Real server (name) has reached/dropped below its connection rate limit (value).

Priority: Alert

0005002004 (client certificate verify)

This log ID relates to a system event involving SLB client certificate verify.

Message:`client [ipaddr] with certificate CN[name] [was validated successfully|failed to be validated] by CA with CN[name] [and OCSP server [name]] [ and CRL [name]]`

Meaning: Client (IP address) with certificate CN (name) was validated successfully/failed to be validated by the CA with CN (name) and OCSP server (name) and CRL (name).

Priority: Alert

0005002005 (slb ssl handshake)

This log ID relates to a system event involving SLB SSL handshake to the real server or virtual server.

Message:`VS [name] failed to establish SSL connection with real server [name]`

Meaning: Virtual Server (name) failed to establish an SSL connection with Real Server (name).

Priority: Alert

Or

Message:`VS [name] failed to establish SSL connection with real server [name]`

Meaning: Virtual Server (name) failed to establish an SSL connection with Real Server (name).

Priority: Alert

0005002007 (vdom rps limit)

This log ID relates to a system event involving VDOM RPS limit.

Message:`In VDOM vdom1, Drop 4 packets due to L7RPS`

Meaning: Four packets were dropped from VDOM "`vdom1`" due to its L7RPS resource limit.

Priority: Warning

0005002008 (vdom cps limit)

This log ID relates to a system event involving VDOM CPC limit.

Message:`In VDOM vdom1, Drop 4 packets due to L4CPS/L7CPS/SSLCPS`

Meaning: Four packets were dropped from "vdom1" due to its L4CPS/L7CPS/SSLCPS resource limit.

Priority: warning

0005002009 (vdom tp limit)

This log ID relates to a system event involving VDOM TP limit.

Message:`In VDOM vdom1, Drop 4 packets due to SSLTP`

Meaning: Four packets were dropped from VDOM "vdom1" due to SSLTP resource limit.

Priority: Warning

0005002010 (slb connection limit)

This log ID relates to a system event involving SLB connection limit.

Message:`Virtual server vsname is [recovered from | reached ]connection limit`

Meaning: Virtual server (name) recovered from or reached its SLB connection limit.

Priority: Warning

0005002011 (slb source port exhausted)

This log ID relates to a system event regarding the availability of SLB source port.

Message:`Virtual server vsname is [recovered from | out of] source ports`

Meaning: Virtual server (name) recovered or ran out of source ports.

Priority: Warning

0005002012 (slb ip pool exhausted)

This log ID relates to slb ip pool exhausted

Message:

```
(1) Virtual server rsname is no source pool configured on the
interface to real server rsname
```

```
(2) Virtual server vsname to real server vsname is recovered from bad
source pool list configuration
```

Meaning: Virtual server (name) had exhausted its SLB IP pool (no IP is available for SLB).

Priority: Warning

0005002013 (slb config error)

This log ID relates to a system event regarding use of invalid arguments for SLB configuration.

Message:`Invalid configuration arguments`

Meaning: Invalid configuration arguments were used for SLB configuration.

Priority: Alert

0005002014 (slb memory allocation error)

This log ID relates to a system event regarding memory allocation in SLB configuration.

Message:`Failed to allocate memory`

Meaning: No (enough) memory was allocated for SLB configuration.

Priority: Alert

0005002015 (slb mkdir error)

This log ID relates to a system event regarding mkdir in SLB configuration.

Message:`Failed to make directory`

Meaning: The system was unable to create the directory for SLB configuration.

Priority: Alert

0005002016 (slb open file error)

This log ID relates to a system event regarding set SLB configuration.

Message:`Failed to open file`

Meaning: The system failed to open the file.

Priority: Alert

0005002017 (slb write file error)

This log ID relates to a system event regarding set SLB configuration.

Message:`Failed to write file`

Meaning: The system failed to generate the configuration.

Priority: Alert

0005002018 (slb drop log)

This log ID relates to a L4 SLB kernel packet drop.

Message:`SLB packet is dropped in IPVS`

Meaning: There is a L4 SLB packet drop in IPVS.

Priority: Warning

0005002019 (vitrual server restart)

This log ID relates to a system event involving vitrual server restart.

Message: `restart vsname vitrual server`

Meaning: restart vsname vitrual server.

Priority: Notice

0005002020 (terminate httproxy [process id] for out of memory)

This log ID relates to a system event involving the restart of a httproxy for out of memory.

Message: `terminate httproxy [process id] for out of memory`

Meaning: terminate httproxy [process id] for out of memory.

Priority: Alert

0005002021 (Resolve real server FQDN)

This log ID relates to a system event involving Resolve real server FQDN.

Message: `realserver name [name], fqdn:[fqdn], ip6 [ipv6 addr]/ip[ipv4 addr]`

Meaning: Resolve real server FQDN.

Priority: Alert

Link load balance

This section describes log messages involving link load balance, which is a subcategory of the event log.

0006003000 (llb bandwidth usage)

This log ID relates to a bandwidth usage in link load-balancing operations.

Message:

gateway [name][

"exceed inbound bandwidth",

"exceed outbound bandwidth",

"exceed inbound spillover bandwidth",

"exceed outbound spillover bandwidth",

"exceed total spillover bandwidth"]

Meaning: Gateway (name) exceeded its allocated inbound/outbound/inbound spillover/outbound spillover bandwidth.

Priority: Warning

Global load balance

This section describes log messages involving global load balancing operation, which is are a subcategory of the event log.

0007005000 (glb peer status change)

This log ID relates to peer status change in a GLB operation.

Message:`GLB Peer [name] is [Connected:Disconnected]`

Meaning: GLB peer (name) is connected/disconnected.

Priority: Alert

0007005001 (glb remote server status change)

This log ID relates to the remote server's status change in a GLB operation.

Message:`Server [name] is [Online|Off]`

Meaning: GLB server (name) is online/offline.

Priority: Alert.

Firewall

This section describes log messages about FortiADC firewall, which is a subcategory of the event log.

0008004000 (firewall snat source port exhausted)

This log ID relates to a firewall event.

Message: `SNAT rule [name] run out of source port and can't open new connection with others`

Meaning: SNAT Rule (name) ran out of source ports and could not open new connections with others.

Priority: Warning

Traffic logs

This section discusses the traffic logs that FortiADC generates.

0100008000 (traffic: SLB L4VS)

This log ID relates to SLB Layer-4 traffic.

Priority: Information

Example:

```
date=2020-08-19 time=17:13:37 log_id=0100008000 type=traffic subtype=slb_layer4
pri=information vd=root msg_id=8891139290341374 duration=3 ibytes=398 obytes=1075
proto=6 service=tcp src=20.20.0.1 src_port=55442 dst=20.20.0.100 dst_port=80 trans_
src=20.20.0.1 trans_src_port=55442 trans_dst=20.20.2.3 trans_dst_port=80 policy=VS1
action=none srccountry=United States dstcountry=United States real_server=pool1-3
```

0100008001 (traffic: SLB HTTP)

This log ID relates to SLB HTTP traffic.

Priority: Information

Example:

```
date=2020-08-19 time=17:09:45 log_id=0101008001 type=traffic subtype=slb_http
pri=information vd=root msg_id=8891139290341323 duration=12 ibytes=78 obytes=776
proto=6 service=http src=20.20.0.1 src_port=55438 dst=20.20.0.100 dst_port=80 trans_
src=20.20.2.10 trans_src_port=24820 trans_dst=20.20.2.1 trans_dst_port=80 policy=VS1
action=none http_method=get http_host=20.20.0.100 http_agent=none http_url=/ http_
qry=none http_referer=none http_cookie=none http_retcode=200 user=none usrgrp=none
auth_status=none srccountry=United States dstcountry=United States real_server=pool1-
1
```

0102008002 (traffic: SLB TCPS)

This log ID relates to a SLB TCPS traffic.

Priority: Information

Example:

```
date=2020-08-19 time=18:24:55 log_id=0102008002 type=traffic subtype=slb_tcps
pri=information vd=root msg_id=8891139290341888 duration=432 ibytes=79 obytes=804
proto=6 service=tcps src=20.20.0.1 src_port=52564 dst=20.20.0.100 dst_port=150 trans_
src=20.20.2.10 trans_src_port=27022 trans_dst=20.20.2.1 trans_dst_port=80
policy=VS150-status-healthy-green-rs-healthy-tcps action=none srccountry=United
States dstcountry=United States real_server=pool1-1
```

0103008003 (traffic: SLB RADIUS)

This log ID relates to SLB RADIUS traffic.

Priority: Information

Example:

```
date=2020-08-19 time=18:54:23 log_id=0103008003 type=traffic subtype=slb_radius
pri=information vd=root msg_id=8891139290342517 duration=0 ibytes=45 obytes=29
proto=17 service=radius src=20.20.0.1 src_port=59786 dst=20.20.0.100 dst_port=1812
trans_src=20.20.2.10 trans_src_port=49207 trans_dst=20.20.2.3 trans_dst_port=1812
policy=VS1 action=auth user=user1 srccountry=United States dstcountry=United States
real_server=d3
```

0104009000 (traffic: GLB)

This log ID relates to GLB traffic.

Priority: Information

Example:

```
date=2020-08-19 time=19:19:45 log_id=0104009000 type=traffic subtype=dns
pri=information vd=root msg_id=520765 proto=17 src=10.101.0.1 src_port=41084
dst=20.16.0.40 dst_port=53 policy=policy1 action=none fqdn=app1.autotest1.com
resip=20.16.0.200 srccountry=Reserved dstcountry=United States
```

0106008004 (traffic: SLB SIP)

This log ID relates to SLB SIP traffic.

Priority: Information

Example:

```
date=2020-08-19 time=19:13:10 log_id=0106008004 type=traffic subtype=slb_sip
pri=information vd=root msg_id=8891139290342822 duration=0 ibytes=363 obytes=360
proto=17 service=sip src=20.20.0.1 src_port=5060 dst=20.20.0.100 dst_port=5060 trans_
src=20.20.2.10 trans_src_port=1777 trans_dst=20.20.2.1 trans_dst_port=5062 policy=VS1
action=none sip_method=BYE sip_uri=sip:service@20.20.0.100:5060 SIP/2.0 sip_from=sipp
<sip:sipp@20.20.0.1:5060>;tag=28432SIPpTag009 sip_to= service
```

```
<sip:service@20.20.0.100:5060>;tag=26303SIPpTag013 sip_callid= 9-28432@20.20.0.1 sip_
retcode=200 srccountry=United States dstcountry=United States real_server=d1
```

0107008005 (traffic: SLB RDP)

This log ID relates to SLB RDP traffic.

Priority: Information

Example:

```
date=2020-08-19 time=18:24:45 log_id=0107008005 type=traffic subtype=slb_rdp
pri=information vd=root msg_id=8891139290341887 duration=12 ibytes=79 obytes=804
proto=6 service=rdp src=20.20.0.1 src_port=60890 dst=20.20.0.100 dst_port=152 trans_
src=20.20.2.10 trans_src_port=27008 trans_dst=20.20.2.1 trans_dst_port=80
policy=VS152-rdp action=none srccountry=United States dstcountry=United States real_
server=pool1-1
```

0108008006 (traffic: SLB DNS)

This log ID relates to SLB DNS traffic.

Priority: Information

Example:

```
date=2020-08-19 time=19:17:57 log_id=0108008006 type=traffic subtype=slb_dns
pri=information vd=root msg_id=8891139290342975 duration=0 ibytes=34 obytes=83
proto=17 service=dns src=20.20.0.1 src_port=35648 dst=20.20.0.100 dst_port=80 trans_
src=20.20.2.10 trans_src_port=62713 trans_dst=20.20.2.3 trans_dst_port=53 policy=VS1
action=accept dns_req=Request domain www.fortiadc.com. type 1 dns_resp=Get response
srccountry=United States dstcountry=United States real_server=d3
```

0109008007 (traffic: SLB RTSP)

This log ID relates to SLB RTSP traffic.

Priority: Information

Example:

```
date=2020-08-19 time=15:51:15 log_id=0109008007 type=traffic subtype=slb_rtsp
pri=information vd=root msg_id=50937772 duration=192 ibytes=164 obytes=504 proto=6
service=rtsp src=28.21.6.13 src_port=10047 dst=28.21.6.7 dst_port=554 trans_
src=28.21.6.13 trans_src_port=10047 trans_dst=28.221.7.74 trans_dst_port=554
policy=tester-28-21-6-L7-rtsp554 action=none rtsp_method=SETUP rtsp_
uri=rtsp:/test.mp3 rtsp_sessionid=7121D1C3 rtsp_retcode=200 rtsp_info=Transport:
RTP/AVP;unicast;client_port=54445-54446;server_port=6970-6971;source=28.21.6.7
srccountry=United States dstcountry=United States real_server=d21-7-74
```

0110008008 (traffic: SLB SMTP)

This log ID relates to SLB SMTP traffic.

Priority: Information

Example:

```
date=2020-08-19 time=17:17:53 log_id=0110008008 type=traffic subtype=slb_smtp
pri=information vd=root msg_id=8891139290341464 duration=4 ibytes=128 obytes=23
proto=6 service=smtp src=20.20.0.1 src_port=60302 dst=20.20.0.100 dst_port=25 trans_
src=20.20.2.10 trans_src_port=41466 trans_dst=20.20.2.1 trans_dst_port=25 policy=VS1
action=none smtp_cmd=EHLO smtp_subject=none smtp_from=none smtp_to=none smtp_cc=none
smtp_retcode=250 smtp_attachname=none smtp_starttls=INACTIVE smtp_bodylen=0
srccountry=United States dstcountry=United States real_server=pool1-1
```

0111008010 (traffic: SLB RTMP)

This log ID relates to SLB RTMP traffic.

Priority: Information

Example:

```
date=2020-08-20 time=10:58:02 log_id=0111008010 type=traffic subtype=slb_rtmp
pri=information vd=root msg_id=68464437 duration=144 ibytes=3252 obytes=3364 proto=6
service=rtmp src=16.1.1.11 src_port=62288 dst=16.1.1.100 dst_port=1935 trans_
src=16.1.2.1 trans_src_port=27828 trans_dst=16.1.2.41 trans_dst_port=1935
policy=RTMP_VS1 action=none rtmp_cmd=connect rtmp_tcurl=rtmp://16.1.1.100/live rtmp_
streamname=none rtmp_retcode=NetConnection.Connect.Success srccountry=United States
dstcountry=United States real_server=16.1.2.41
```

0112008011 (traffic: SLB MYSQL)

This log ID relates to SLB MYSQL traffic.

Priority: Information

Example:

```
date=2020-08-19 time=19:23:20 log_id=0112008011 type=traffic subtype=slb_mysql
pri=information vd=root msg_id=8891139290343112 duration=3 ibytes=151 obytes=214
proto=6 service=mysql src=20.20.0.1 src_port=57432 dst=20.20.0.100 dst_port=3306
trans_src=20.20.2.10 trans_src_port=48466 trans_dst=20.20.2.3 trans_dst_port=3306
policy=VS1 action=none mysql_transid=  16782356574320000000000001597890200 mysql_
action=Read Only mysql_sql=select name from autotest where id = 1 mysql_retcode=OK
mysql_groupid=0 srccountry=United States dstcountry=United States real_server=d3
```

0113008009 (traffic: SLB Diameter)

This log ID relates to SLB Diameter traffic.

Priority: Information

Example:

```
date=2020-08-19 time=17:15:47 log_id=0113008009 type=traffic subtype=slb_diameter
pri=information vd=root msg_id=8891139290341439 duration=2006 ibytes=0 obytes=224
proto=6 service=diameter src=20.20.0.1 src_port=36692 dst=20.20.0.100 dst_port=3868
trans_src=20.20.2.10 trans_src_port=31142 trans_dst=20.20.2.3 trans_dst_port=3868
policy=VS1 action=none dm_cmdcode=271 dm_appid=0 dm_e2eid=1332224237 dm_orihost=none
dm_orirealm=none dm_desthost=server.free.com dm_destrealm=free.com dm_
sessionid=client_10.free.com;380998399;2;fortiadc_client dm_retcode=2001
srccountry=United States dstcountry=United States real_server=pool1-3
```

0114000000 (traffic: LLB)

This log ID relates to LLB traffic.

Priority: Information

Example:

```
date=2020-08-19 time=19:21:53 log_id=0114000000 type=traffic subtype=llb
pri=information vd=root msg_id=8891139290205825 duration=0 ibytes=0 obytes=229
proto=17 service=udp src=10.106.139.154 src_port=138 dst=10.106.139.255 dst_port=138
policy=llb_adc1 action=linkgrp srccountry=Reserved dstcountry=Reserved gateway=none
```

0115008012 (traffic: SLB FTP)

This log ID relates to SLB FTP traffic.

Priority: Information

Example:

```
date=2020-08-19 time=17:19:41 log_id=0115008012 type=traffic subtype=slb_ftp
pri=information vd=root msg_id=8891139290341503 duration=4 ibytes=0 obytes=20 proto=6
service=ftp src=20.20.0.1 src_port=53838 dst=20.20.0.100 dst_port=21 trans_
src=20.20.2.10 trans_src_port=32524 trans_dst=20.20.2.1 trans_dst_port=21 policy=VS1
action=none ftp_username=N/A ftp_mode=N/A ftp_cmd=N/A ftp_retcode=220 ftp_d_sport=N/A
ftp_d_dport=N/A ftp_dtr_sport=N/A ftp_dtr_dport=N/A ftp_pathname=N/A
srccountry=United States dstcountry=United States real_server=pool1-1
```

0116008013 (traffic: SLB ISO8583)

This log ID relates to SLB ISO8583 traffic.

Priority: Information

Example:

```
date=2019-07-30 time=13:44:59 log_id=0116008013 type=traffic subtype=slb_iso8583
pri=information vd=root msg_id=291086895 duration=5 ibytes=79 obytes=79 proto=6
service=iso8583 src=16.1.1.22 src_port=34632 dst=16.1.1.79 dst_port=8584 trans_
src=16.1.2.3 trans_src_port=29320 trans_dst=16.1.2.41 trans_dst_port=8583 policy=ISO_
VS2 action=none reqmsglen=77 reqmti=0800 respmsglen=77 respmti=0810 srccountry=United
States dstcountry=United States real_server=16.1.2.41
```

0117008014 (traffic: SLB MSSQL)

This log ID relates to SLB MSSQL traffic.

Priority: Information

Example:

```
date=2020-07-13 time=10:42:24 log_id=0117008014 type=traffic subtype=slb_mssql
pri=information vd=root msg_id=63208635 duration=1 ibytes=1124 obytes=446 proto=6
service=mssql src=172.24.204.172 src_port=53330 dst=10.106.169.100 dst_port=1433
trans_src=16.1.2.1 trans_src_port=55698 trans_dst=16.1.2.43 trans_dst_port=1433
policy=MSSQL_VS2 action=none mssql_action=Read Write mssql_sql=DECLARE @edition
sysname;                SET @edition = cast(SERVERPROPERTY(N'EDITION') as sysname);             SELE
when @edition = N'SQL Azure' then 2 else 1 end as 'DatabaseEngineType',
SERVERPROPERTY('EngineEdition') AS DatabaseEngineEdition,               SERVERPROPERTY('Produ
mssql_response=OK srccountry=Reserved dstcountry=Reserved real_server=16.1.2.43
```

Security logs

This section describes the various security log messages FortiADC generates.

IP Reputation

This section describes security log messages involving IP reputation—a subcategory of the security log.

0200006001 (security: ip reputation)

This log ID relates to a security incident involving IP reputation rules.

Message: `IP Reputation Violation: [Block List | Botnet | Anonymous Proxy | Phishingnm | Spam | Others]`

Meaning: IP reputation rule violation: (The name of the specific violation)

Priority: Warning

Geo

This section describes log messages about FortiADC geo logs.

0203006002 (security: geo)

This log ID relates to security incident involving GEO rules.

Message:`Security rule name, category, subcategory, and description of the attack.`

Meaning: The GEO rule was violated.

Priority: Warning

Web Application Firewall (WAF)

This section describes security log messages related to Web Application Firewall—a subcategory of the security log.

0202006004 (security: waf signature)

This log ID relates to a security incident involving WAF signature attack.

Message:`Find Attack ID: 100*** Desc: "Web Application Joomla! SQL Injection Attempt -- category.php catid SELECT" Module: "SQL Injection" Check Type: "Coldfusion Injection"`

Meaning: A web generic attack was detected.

Priority: Alert

0202006005 (security: http protocol constraint)

This log ID relates to a security incident involving HTTP protocol constraint rule.

Message:`"Attack ID: 101*** Desc: "HTTP Method Violation" Module: "HTTP Protocol Constraint" Check Type: "Request Method Rule""`

Meaning: A violation is triggered due to a match of one or more of the HTTP protocol constraint options.

Priority: Alert

0202006006 (security: waf sql injection)

This log ID relates to a security incident involving the violation of the WAF SQL injection rule.

Message:`"Attack ID: 102*** Desc: "Cross Site Scripting Attack" Module: "Heuristic SQL/XSS Injection Detection" Check Type: "XSS Injection Detection""`

Meaning: A MySQL injection or cross-site injection was detected.

Priority: Alert

0202006007 (security: waf url protection)

This log ID relates to a security incident involving the violation of URL protection rules.

Message:`"Attack ID: 103*** Desc: "Request URL Pattern Violation" Module: "URL Protection" Check Type: "URL Access Rule""`

Meaning: A violation is triggered due to a match of one or more of the url protection rules.

Priority: Alert

0202006008 (security: waf bot)

This log ID relates to a security incident involving Bot detection.

Message:`Attack ID: 104*** Desc: "Bad Robot Attack" Module: "Bot Detection" Check Type: "Bad Robot"`

Meaning: A bad robot or content scraper is detected.

Priority: Alert

0202006009 (security: waf xml validation)

This log ID relates to a security incident involving XML validation.

Message:`"Attack ID: 105*** Desc: "XML schema is invalid" Module: "XML validation detection" Check Type: "XML schema check""`

Meaning: A violation is triggered due to a match of one or more of the XML options.

Priority: Alert

0202006010 (security: waf json validation)

This log ID relates to a security incident involving WAF JSON validation rules.

Message:`"Attack ID: 106*** Desc: "possible cross-site scripting attacks" Module: "JSON validation detection" Check Type: "JSON cross-site scripting check"`

Meaning: A violation is triggered due to a match of one or more of the JSON options.

Priority: Alert

0202006011 (security: waf soap validation)

This log ID relates to a security incident involving SOAP validation.

Message:`"Attack ID: 1050*** Desc: "SOAP content is invalid for WSDL" Module: "XML validation detection" Check Type: "SOAP WSDL validate""`

Meaning: A violation is triggered due to a match of one or more of the SOAP options.

Priority: Alert

0202006012 (security: waf_web_scraping)

This log ID relates to a security incident involving Web Scrapping Attack.

Message: `"Attack ID: 1070*** Desc: "Web Scrapping Attack" Module: "Advanced-Protection" Check Type: "Content-Scraping""`

Meaning: A violation is triggered due to a match of one or more of Advanced Protection rule.

Priority: Alert

0202006013 (security: waf_cookie_security)

This log ID relates to a security incident involving the violation of Cookie Security rule.

Message: `"Attack ID: 1080*** Desc: "The COOKIE SIGNATURE is invalid" Module: "Cookie Security" Check Type: "SIGNED COOKIE""`

Meaning: A violation is triggered due to a match of one or more of Cookie Security rule.

Priority: Alert

0202006014 (security: waf_csrf_protection)

This log ID relates to a security incident involving CSRF attack.

Message: `"Attack ID: 1090*** Desc: "Request CSRF Violation" Module: "CSRF Protection" Check Type: "CSRF Protection""`

Meaning: A violation is triggered due to a match of one or more of CSRF Protection rule.

Priority: Alert

0202006015 (security: waf_brute_force)

This log ID relates to a security incident involving Brute Force Attack.

Message: `"Attack ID: 1100*** Desc: "Brute Protection" Module: "Brute Force Login Protection" Check Type: "BRUTE FORCE LOGIN PROTECTION""`

Meaning: A violation is triggered due to a match of one or more of Brute Force rule.

Priority: Alert

0202006016 (security: waf_data_leak_prevention)

This log ID relates to a security incident involving the violation of Data Leak Prevention rule.

Message: `"Attack ID: 1110*** Desc: "Data Leak Violation" Module: "Data Leak Prevention" Check Type: "Data Leak""`

Meaning: A violation is triggered due to a match of one or more of Data Leak Prevention rule.

Priority: Alert

0202006017 (security: waf_html_input_validation)

This log ID relates to a security incident involving HTTP request input validation.

Message: `"Attack ID: 1120*** Desc: "Request Input parameter" Module: " HTML Input Validation" Check Type: "Input Parameter""`

Meaning: A violation is triggered due to a match of one or more of HTML Input Validation rule.

Priority: Alert

0202006018 (security: waf_anti_defacement)

This log ID relates to a security incident involving Web page defacement.

Message: `"file [/test/bigfile2_3] on site [wad1] of vdom root has been deleted. Acknowledge successfully."`

Meaning: A page defacement detection of one or more Anti defacement profile.

Priority: Alert

0202006020 (security: waf_openapi_check)

This log ID relates to a security incident involving waf_openapi_check.

Message: `"Attack ID: 1140*** Desc: "OpenAPI schema is invalid" Module: "OpenAPI validation detection" Check Type: "OpenAPI schema check""`

Meaning: A violation is triggered due to a match of one or more of the OpenAPI schema check rules.

Priority: Alert

DDOS

This section describes security log messages involving synflood attacks—a subcategory of the security log.

0201006150 (security: synflood)

This log ID relates to a security incident involving synflood attack.

Message: N/A

Meaning:

Meaning: this is a synflood attack.

Priority: Alert

0201006151 (security: IP fragment)

This log ID relates to a security incident involving IP fragment attack.

Message: N/A

Meaning: this is a IP fragment attack.

Priority: Alert

0201006152 (security: TCP slow data)

This log ID relates to a security incident involving TCP slow data attack.

Message: N/A

Meaning: this is a TCP slow data attack.

Priority: Alert

0201006153 (security: TCP access flood)

This log ID relates to a security incident involving TCP access flood attack.

Message: N/A

Meaning: this is a TCP access flood attack.

Priority: Alert

0201006154 (security: DoS HTTP Connection Flood)

This log ID relates to a security incident involving DoS HTTP Connection Floodattack.

Message: DoS HTTP Connection Flood

Meaning: this is a DoS HTTP Connection Floodattack.

Priority: Alert

0201006155 (security: DoS HTTP Request Flood)

This log ID relates to a security incident involving DoS HTTP Request Flood attack.

Message: DoS HTTP Connection Flood

Meaning: this is a DoS HTTP Request Flood attack.

Priority: Alert

0201006156 (security: DoS HTTP Access Limit)

This log ID relates to a security incident involving DoS HTTP Access Limit.

Message: DoS HTTP Access Limit

Meaning: this is a DoS HTTP Access Limit.

Priority: Alert

Anti-virus (AV)

This section describes log messages related to the anti-virus module.

0204006500 (security: av detected virus)

This log ID relates to a virus is detected by AV.

Message:`AV detected virus`

Meaning: The AV module detected a virus attack.

Priority: Alert

0204006501 (security: av heuristic)

This log ID relates to AV heuristic detected virus.

Message:`AV heuristic detected virus`

Meaning: The AV heuristic module detected a virus attack.

Priority: Alert

0204006502 (security: av upload request to fortisandbox)

This log ID relates to AV upload request to FortiSandbox to do analytics.

Message: AV upload FortiSandbox to do analytics

Meaning: The AV module uploaded the request to FortiSandbox for data analysis.

Priority: Alert

0204006503 (security: av scan length oversize)

This log ID relates to AV scan length oversize.

Message:`AV scan length oversize`

Meaning: The AV scan length oversize is exceeded.

Priority: Alert

0204006504 (security: av error)

This log ID relates to an AV engine error.

Message:`AV engine meet error, code x.`

Meaning: The AV engine has encountered an error, Code X.

Priority: Alert

0204006507 (security: Delete quarantined file)

This log ID relates to AV: Delete quarantined file

Message: `Delete quarantined file, checksum:[number]`

Meaning: Delete quarantined file.

Priority: Notification

IPS

This section describes log messages related to the Intrusion Prevention System module.

0205006600 (security: Find a IPS attack and pass/drop it)

This log ID relates to IPS: Find a IPS attack and then pass/drop it

Message: `Attack: [rule name] detected, action [pass/drop]`

Meaning: Find a IPS attack and pass/drop it

Priority: Notification

Script logs

This section describes the script logs that FortiADC generates.

0300010000 (script)

This log ID relates to a script event involving error system load a script file.

Message:`script log`

Meaning: The system loaded a script.

Priority: information

www.fortinet.com