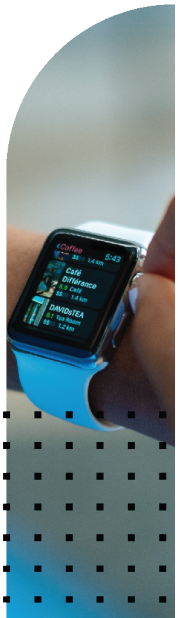
Release Notes

FortiSIEM 6.3.1



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

08/15/2022
FortiSIEM 6.3.1 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
08/26/2021	Initial version of FortiSIEM 6.3.1 Release Notes.
08/31/2021	Added Known Issue "Adding a Network Segment to a Fresh Installation of 6.3.1" to 6.3.1 Release Notes.
09/23/2021	Added "Windows Agent 4.1.4 Release" to 6.3.1 Release Notes.
10/04/2021	Added "Windows Agent 4.1.5 Release" to 6.3.1 Release Notes.
10/05/2021	Updated "Bug Fixes and Minor Enhancements" table for 6.3.1 Release Notes.
12/14/2021	Added Known Issues - Remediation Steps for CVE-2021-44228 for 6.x Release Notes.
05/12/2022	Added Known Issue Elasticsearch Based Deployments Terms Query Limit to Release Notes.
08/15/2022	Add Known Issue to 6.3.x Release Notes.

Whats New in 6.3.1

This document describes the additions for the FortiSIEM 6.3.1 release.

New Features

Disaster Recovery

This release adds back the Disaster Recovery feature that was present in FortiSIEM 5.4 release.

To set up Disaster Recovery, the user needs to set up two identical FortiSIEM instances, each with a separate license. Then FortiSIEM will replicate the CMDB (in PostgreSQL database), Configuration data (in SVN-lite), Profile database (in SQLite database) and FortiSIEM EventDB from Primary to Secondary. For Elasticsearch based deployments, procedures for out-of-band *unidirectional* Cross-cluster replication (CCR) is provided.

When the Primary fails, the user has to be manually convert the Secondary FortiSIEM to Primary. When the original Primary is back up, the user has to first make it Secondary and switch roles to make it Primary again.

Secondary is in hot Standby mode. While the user can log in to the Secondary GUI, permissions that involve writing to the PostgreSQL database are not permitted. Hence Analytical queries in the Secondary FortiSIEM is not permitted.

Disaster Recovery works for all EventDB based software deployments and hardware appliances (2000F, 3500F and 3500G) and Elasticsearch deployments using *uni-directional* Cross-cluster replication.

Details for Disaster Recovery Operations in EventDB based environments is available here.

Details for Disaster Recovery Operations in Elasticsearch based environments is available here.

Install and Upgrade in IPV6 Networks

This release enables you to install FortiSIEM in IPV4 only, IPV6 only, or a mixed IPV4/IPV6 network. Upgrading via a IPV6 network is now possible.

For details, see the Installation documentation for your platform.

Backup and Restore for Hardware Appliances

VM based FortiSIEM installs have a snapshot feature that allows customers to go back to the snapshot if an upgrade fails. In contrast, hardware appliance-based installs lack this capability – so if an upgrade fails, then it has to be fixed inline, leading to increased downtime. This release adds a backup and restore feature to hardware based installs.

For details, see the Upgrade Guide.

Key Enhancements / Bug Fixes

Max Events per Second (EPS) per Collector

Earlier releases allowed customers to set a *bandwidth limit* for Collectors sending events to Workers - this prevented a Collector from overwhelming the Workers after a prolonged loss of connectivity. However, when a Collector is newly deployed, the Collector may be able to send events at an excessive rate without violating the bandwidth limit. This can also overwhelm the Workers and the event database. This release adds a *per-Collector EPS limit* to prevent this from occurring.

A Collector is never able to send at more than the EPS limit and the bandwidth limit. When any of these limits are hit, events are buffered at the Collector and sent later. Rate limits are enforced at periodic 3 minute intervals.

To set the per-Collector EPS limit, see **Upload EPS Limit** in Adding a Collector.

Elasticsearch Enhancements

Dynamic Elasticsearch Shard Adjustment to Handle EPS Burst

A shard is the unit of parallelism for Elasticsearch deployments. When EPS is high, you want more shards to be spread across many Data Nodes to keep up with the incoming EPS. This release adds a dynamic shard adjustment mechanism to handle EPS surges. Every 5 minutes, a decision of whether to allocate more shards is made based on the incoming EPS.

This is an internal feature, so no user configuration is required.

Per Organization Elasticsearch Insert

In Service Provider deployments, you can choose to have separate Elasticsearch indices for every Organization. In earlier releases, the Worker nodes combined events from all Organizations into a single HTTPS POST insert request to Elasticsearch. This may introduce a Head-Of-Line Blocking effect – if Elasticsearch is slow in inserting one Organization's events, then all other Organization's event inserts may be delayed. This release prevents this situation by inserting different Organization's events in different HTTPS POST requests to Elasticsearch.

Case-Sensitive Regex Search

In earlier releases, searches involving **CONTAIN**, **NOT CONTAIN**, **REGEXP** and **NOT REGEXP** operators were case-insensitive. In this release, the **REGEXP** and **NOT REGEXP** operator-based searches are made case-sensitive. This allows more flexibility during threat hunting exercises.

Windows Agent 4.1.3 Bug Fixes

The two following issues are resolved.

1. When FortiSIEM monitors DNS Analytical logs, Windows Event Log service memory utilization may be high.
2. Windows Agent may stop sending events if both the Supervisor and Collector go down for more than 10 minutes and then come up.

Windows Agent 4.1.4 Bug Fixes

The two following issues are resolved.

1. File handle leak while interfacing with local SQLite database could cause Windows Agent memory usage to grow over time.
2. File handle leak while interfacing with Windows registry could cause Windows Agent memory usage to grow over time.

Windows Agent 4.1.5 Bug Fixes

The two following issues are resolved.

1. The log file contained a plain text password used to register the agent to the Supervisor. This password was not used for any other purposes.
2. An authenticated Windows user could run arbitrary Powershell scripts with Administrator permissions.

New Device Support

AWS CloudWatch Alarms

FortiProxy

Google Cloud Platform

KVM Audit

Mac OS

Microsoft Advanced Threat Analytics On Premise Platform

Otorio RAM2

UserGate UTM Firewall

Enhanced Device Support

Google Workspace / GSUITE

Zeek Network Security Monitor (Previously Known as Bro)

Bug Fixes and Minor Enhancements

Bug ID	Severity	Module	Description
636110	Major	Discovery	In AD User Discovery, the Last Login Value was incorrect if the user was not set (did not log in) to the AD Server.
749499	Major	Windows Agent	The log file contained a plain text password used to register the agent to the Supervisor. This password was not used for any other purposes. Additionally, an authenticated Windows user could run arbitrary Powershell scripts with Administrator permissions.
748252	Major	Windows Agent	File handle leak while interfacing with Windows registry could cause Windows Agent memory usage to grow over time.
746978	Major	Windows Agent	File handle leak while interfacing with local SQLite database could cause Windows Agent memory usage to grow over time.
727872	Major	Windows Agent	Windows Agent may stop sending events if both the Supervisor and Collector go down for more than 10 minutes and then come up.
723147	Major	Windows Agent	When FortiSIEM monitors DNS Analytical logs, Windows Event Log service memory utilization may be high.
739811	Minor	App Server	Incident dashboard queries could be slow for non-admin users when there were incidents over many months.
737188	Minor	App Server	External LDAP Authentication did not work after upgrading from 5.3.2 to 6.3.0 for CA Directory LDAP Server.
731150	Minor	App Server	Organization info was set incorrectly in PH_DEV_MON_LOG_ DEVICE_DELAY_HIGH events from Multi-tenant Collectors.

Bug ID	Severity	Module	Description
728925	Minor	App Server	Excessive errors on 2000F were caused by short user field in postgreSQL.
726689	Minor	App Server	Out-of-Range Integer error occurred when trying to change device status in CMDB.
726068	Minor	App Server	Logged In User list in database was not cleared when the Supervisor rebooted or the session closed.
724935	Minor	App Server	Windows agent events were still received after deleting an Org with windows agent.
722997	Minor	App Server	The timeline date format in exported query results did not display the chosen time format in the GUI.
722650	Minor	App Server	The CMDB Export to ServiceNow via custom transform file did not work.
722130	Minor	App Server	Pull Event Monitor Summary Reports appeared blank at org level (PDF and CSV).
722003	Minor	App Server	Technique and Tactics attributes needed to be added to the Incident XSL for customers to parse the field into ServiceNow.
721572	Minor	App Server	Incident Export (PDF) did not correctly show Tactics and Technique values.
680663	Minor	App Server	Devices in CMDB with triggered incidents could sometimes not be deleted .
514406	Minor	App Server	External Authentication via LDAP did not work for users with $ in their username.
738867	Minor	GUI	Allow Incident Firing on Approved devices only did not take effect; incidents were firing on pending device
729459	Minor	GUI	With the UI Setting set as Dark Theme, the headings in the lower table under **CMDB > Devices** were illegible.
728440	Minor	GUI	From **INCIDENTS > Overview**, if a user clicked a link, went back to **INCIDENTS > Overview**, and then switched to **INCIDENTS > List View**, a filtered list would be displayed. **Note**: The filter should be reset when switching.
727304	Minor	GUI	With the UI Setting set as Dark Theme, Diff under **Installed Software/Configure** in the lower table on the **CMDB > Devices** page was illegible.
727217	Minor	GUI	When both VirusTotal and RiskIQ integration policies were invoked on an incident, only one policy's comment was added.
726972	Minor	GUI	The user was unable to select an org level reporting device for an event dropping rule while logged in as a Super/admin with global view.

Bug ID	Severity	Module	Description
726912	Minor	GUI	After adding LDAP users to CMDB Users, if a new user was later added with a new rule exception and FortiSIEM was rebooted, while performing an Edit Rule Exception for the user, the user's value appeared indecipherable. **Note**: The exception rule worked fine, but the value displayed was indecipherable.
726816	Minor	GUI	If the user went to the **ADMIN > Settings > Event Handling > Forwarding** page, then to **DASHBOARD**, and back to **ADMIN > Settings > Event Handling > Forwarding**, a duplicate Organization column would be added to the Forwarding page.
726770	Minor	GUI	The Trend Chart Bar appeared incorrectly in PDF reports.
726228	Minor	GUI	After adding a CMDB report to a Report Bundle in Report Design, the page orientation could not be set to Landscape.
725816	Minor	GUI	After copy/pasted text is put into the text editor for a custom report in Report Design, the Preview and Export functions fail when selected.
723811	Minor	GUI	From the **ANALYTICS** page, a string containing a comma (using operators = and !=) was not allowed in filter searches.
723628	Minor	GUI	In Super Local view, on the **CMDB > Devices** page, if a user selected a collector, clicked on **Actions** and selected **Real-time Performance**, collectors for other organizations would also appear.
696824	Minor	GUI	From the **CMDB > Devices** page, with a device containing a Supervisor IP selected, if a user clicked on **Actions**, selected **Change Status**, and changed the status to **Approved**, no change would occur.
678165	Minor	GUI	On the **INCIDENTS > Overview** page, drilling down to the Incident table view from a Host under "Top Impacted Hosts" where the Incident Source, Target or Reporting IP does not include the Hostname sometimes results in no incident being shown.
578936	Minor	GUI	Reports containing a Donut Chart and Bar Chart for COUNT (DISTINCT destIpAddr) displayed a blank Donut chart and an inaccurate Bar Chart when a preview/export PDF report was generated.
727489	Minor	Linux Agent	The file owner and group parameters were empty in the file metadata for Ubuntu20. **Note**: Navigate to **CMDB > Devices**, select the ubuntu linux 20 device, select the **File** tab in the lower table, and select the file to view the file metadata.

Bug ID	Severity	Module	Description
736266	Minor	Monitoring	From **CMDB > Devices**, with the **Monitor** tab selected in the lower table, the monitor status for job "Fortinet WTP Metrics" was missing even if events were coming.
738900	Minor	Parser	Event forwarding does not work when the sender IP belongs to a CMDB Device Group in the forwarding rule.
740775	Minor	Performance Monitoring	Important process matching with empty parameter was not correct, which could cause unimportant processes to become important for monitoring.
717167	Minor	Performance Monitoring	H3C Comware switches sent incomplete configuration, collected via SSH.
736907	Minor	Query	<User defined IP event attribute> IN <CMDB group> Query did not work.
730442	Minor	Query	Elasticsearch - Failed to query with Hash Code IN custom hash group while the items in this group were imported from CSV.
729467	Minor	Query	Elasticsearch - Query failed with Source IP IN custom parent Anonymity Network Group while a sub group was moved out and moved back.
729181	Minor	Query	Elasticsearch - Deactivated watch list item could still be queried under **ANALYTICS**.
729159	Minor	Query	Elasticsearch - Queries involving Custom Biz Service did not work.
728239	Minor	Query	Elasticsearch - DeviceToCMDB query did not work.
722560	Minor	Query	Incorrect results were returned by Display Field division when the numerator was small and the divisor was a whole number.
722558	Minor	Query	Display Field Expressions using COUNT DISTINCT were not evaluated correctly
720174	Minor	Query	Named value query did not return result for custom device group with deleted sub group for Elasticsearch queries.
702515	Minor	Query	Regex in Search and Rule Filter needed to be case-sensitive to allow more flexibility.
738118	Minor	System	After upgrade to 6.3.0, theget-fsm-health.py script had no information for the Details section.
733909	Minor	System	The upgrade reapplied network configuration because FortiSIEM read the DNS server configuration from the wrong location. This could cause the upgrade to fail.
696997	Minor	System	SNMP service with default community name needed to be turned off during installation.

Bug ID	Severity	Module	Description
727872	Minor	Windows Agent	No event from Windows agent if both the Supervisor and Collector went down for more than 10 minutes and then came up.
723147	Minor	Windows Agent	Windows Event would use high memory to monitor DNS Analytical logs.
570476	Minor	Windows Agent	Windows Agent registration failed if a password contained the ampersand (&) character.
726572	Minor	Windows Agent, Linux Agent	FIM File push did not work if there was a space in the file or directory name.
735848	Enhancement	API	Incident Update REST API needs to update incident status.
735820	Enhancement	API	Incident API should provide Event Attribute Name, not just the ID.
723011	Enhancement	API	The ability to delete Watch list API groups should be added, since they can be created at system level.
737205	Enhancement	App Server	Malware Updates should clean up /data/cache/ folders in addition to the other Malware directories.
731057	Enhancement	App Server	When Elasticsearch is used as storage, the Event Name field is not included in the CSV export. The Event Name field should be included in the CSV export when using Elasticsearch as storage.
517113	Enhancement	App Server	REST API queries run from the outside should not generate separate user logins in GUI.
738241	Enhancement	Data	FortiAV2 paired with FortiClient v 6.2.8 events are being recognized as unknown event type. These events should be recognized as coming from FortiClient.
735211	Enhancement	Data	Process Command Line attribute is not been parsed for some Win-Security-4688 events. Process Command Line attribute should be parsed for win4688 events.
734336	Enhancement	Data	FortiGate parser should map Xauthuser attribute to the user field if the value exists.
733110	Enhancement	Data	Generic_Unix_User_Password_Change event should be a member of group "Password Change".
730702	Enhancement	Data	REvil Rules and Reports should be added to FortiSIEM.
730657	Enhancement	Data	Unknown Linux agent events were getting stuck in collector. Parser for New Relic Linux added.
730465	Enhancement	Data	Some events for Cisco Firepower Threat Defense were not parsed.
730319	Enhancement	Data	The rule "Executable file posting from external source" made no reference to external source in the rule definition.
730301	Enhancement	Data	Cisco NX OS parser was not parsing the User field.

Bug ID	Severity	Module	Description
729278	Enhancement	Data	Some McAfee EPO syslog events were not parsed.
726784	Enhancement	Data	Sysmon Create Process Event CommandLine Parsing was incorrect.
723892	Enhancement	Data	Improved the output legibility of Trend Micro Deep Discovery Inspector Parser and added more event types.
694867	Enhancement	Data	FortiClientParser did not handle EMS messages forwarded through FortiAnalyzer.
686294	Enhancement	Data	PaloAltoParser needed to parse other attribute for PaloAlto Config Syslogs EventType.
674101	Enhancement	Data	Improved the output legibility of Sophos Central Parser.
670223	Enhancement	Data	Added AWS CloudWatch logs for parsing beyond VPC flow log.
660630	Enhancement	Data	FortiGate Parser created incorrect Event Type and Names for a few LogIDs.
659038	Enhancement	Data	Unix parser did not correctly categorize Installed Software.
658139	Enhancement	Data	IIS Parser needed to support logs received via Event Tracing for Windows.
649287	Enhancement	Data	CheckpointCEF Parser did not extract Action (act) field.
632880	Enhancement	Data	ApacheViaSnareParser did not parse the Username field.
624076	Enhancement	Data	Win-Security-5136 needed to parse further details.
738158	Enhancement	Data	Added more event types for Google App Suite.
720699	Enhancement	GUI	Increased the limit of PAYG Report email recipients from 3 to 5.
726733	Enhancement	Linux Agent	User File Monitoring did not pickup new content when written to the same line.

Rule and Report Modifications since 6.3.0

The following rules were added:

- GCP: Firewall Rule Created
- GCP: Firewall Rule Deleted
- GCP: Firewall Rule Patched
- GCP: IAM Custom Role Created
- GCP: IAM Custom Role Deleted
- GCP: IAM Member assigned role of type admin or owner
- GCP: Logging Sink Deleted
- GCP: Logging Sink Updated

- GCP: Pub/Sub Subscription Created
- GCP: Pub/Sub Subscription Deleted
- GCP: Pub/Sub Topic Created
- GCP: Pub/Sub Topic Deleted
- GCP: Service Account Access Key Created
- GCP: Service Account Access Key Deleted
- GCP: Service Account Created
- GCP: Service Account Deleted
- GCP: Service Account Disabled
- GCP: Storage Bucket IAM Permissions Modified
- GCP: Storage Bucket Updated
- GCP: Storage or Logging Bucket Deleted
- GCP: VPC Network Deleted
- GCP: VPC Route Added
- GCP: VPC Route Deleted
- Google Workspace: 2FA Enforcement Disabled for Organization
- Google Workspace: 2FA Verification Disabled for Organization
- Google Workspace: API Access Permitted for OAUTH Client
- Google Workspace: Application Added to Domain
- Google Workspace: Domain added to Trusted Domains List
- Google Workspace: Password Management Policy Changed
- Google Workspace: Role Assigned to User
- Google Workspace: Role Created by User
- Google Workspace: Role Deleted by User
- Google Workspace: Role Modified by User
- Kaseya REvil Ransomware File Activity Detected on Host
- Kaseya REvil Ransomware File Activity Detected on Network
- Kaseya REvil Suspicious File Hash Found on Host
- Kaseya REvil Suspicious File Hash Found on Network
- Microsoft ATA Center: Security Alert Triggered
- Otorio RAM2 Alert has Triggered
- Otorio RAM2 Vulnerability Discovered
- Palo Alto Config Change Failed
- Palo Alto Config Change Succeeded
- Palo Alto Config Change Unauthorized
- Print Nightmare Activity Detected on Host
- Print Nightmare Activity Detected on Network
- UserGate UTM IDPS Alert Detected

The following reports were added:

- FortiProxy Admin Authentication Events
- FortiProxy App Control App Group Name Summary
- FortiProxy App Control App Name Summary

- FortiProxy App Control Detailed
- FortiProxy UTM Event Summary
- FortiProxy Web Filter Detailed
- FortiProxy Web Filter Events by Web Category, User, and Count
- FortiProxy Web Filter User Hit Count
- FortiProxy WebFilter Blocked and Passthrough Event Count
- FortiProxy WebFilter Blocked Event Count
- FortiProxy Webfilter Group by Action,Category, and Count
- FortiProxy WebFilter Passthrough Event Count
- GCP: Firewall Rule Created, Deleted, or Changed
- GCP: IAM Custom Roles Created or Deleted
- GCP: IAM Policy Change Audit Report
- GCP: Logging Sinks Created, Updated, or Deleted
- GCP: Pub/Sub Subscriptions Created or Deleted
- GCP: Pub/Sub Topic Created or Deleted
- GCP: Service Account Access Keys Created or Deleted
- GCP: Service Accounts Created,Deleted, or Disabled
- GCP: Storage Bucket IAM Permissions Modified
- GCP: Storage Buckets Updated
- GCP: Storage or Logging Bucket Deleted
- GCP: Top Admin Activity Events by Principal
- GCP: Top Admin Activity Events by Source IP
- GCP: Top Data Access Events by Principal
- GCP: Top Data Access Events by Source IP
- GCP: Top Event Types by Count
- GCP: Top Traffic by Country
- GCP: VPC Network Created or Deleted
- GCP: VPC Routes Created or Deleted
- Google Workspace: Password Management Policy Changed Audit Report
- Google Workspace: Top Event Types by Count
- Google Workspace: Top Events by Source Country
- Google Workspace: Top Events by Source IP
- Google Workspace: Top Events by User
- Kaseya REvil Ransomware File Activity Detected on Host
- Kaseya REvil Ransomware File Activity Detected on Network
- Kaseya REvil Suspicious File Hash Found on Host
- Kaseya REvil Suspicious File Hash Found on Network
- Microsoft ATA (Advanced Threat Analytics) Center - Change Audit Events
- Microsoft ATA (Advanced Threat Analytics) Center - Security Alerts
- Otorio RAM2 Alerts
- Otorio RAM2 Vulnerabilities Discovered
- Palo Alto Config Change Succeeded
- Print Nightmare Vulnerability Activity Seen on Host

- Print Nightmare Vulnerability Activity Seen on Network
- UserGate UTM - IDPS Events
- UserGate UTM - Web Access Logs

The following reports were renamed:

- FortiSIEM Rule Activated/Deactived -> FortiSIEM Rule Activated/Deactivated

Known Issues

Shutting Down Hardware

On hardware appliances running FortiSIEM 6.6.0 or earlier, FortiSIEM `execute shutdown` CLI does not work correctly. Please use the Linux `shutdown` command instead.

Remediation Steps for CVE-2021-44228

Three FortiSIEM modules (SVNLite, phFortiInsightAI and 3rd party ThreatConnect SDK) use Apache log4j version 2.14, 2.13 and 2.8 respectively for logging purposes, and hence are vulnerable to the recently discovered Remote Code Execution vulnerability (CVE-2021-44228).

These instructions specify the steps needed to mitigate this vulnerability without upgrading Apache log4j to the latest stable version 2.16 or higher. Actions need to be taken on the Supervisor and Worker nodes only.

On Supervisor Node

1. Logon via SSH as root.
2. Mitigating SVNLite module:
   a. Run the script `fix-svnlite-log4j2.sh` (here). It will restart SVNlite module with `Dlog4j2.formatMsgNoLookups=true` option and print the success/failed status.
3. Mitigating 3rd party ThreatConnect SDK module:
   a. Delete these log4j jar files under `/opt/glassfish/domains/domain1/applications/phoenix/lib`
      i. log4j-core-2.8.2.jar
      ii. log4j-api-2.8.2.jar
      iii. log4j-slf4j-impl-2.6.1.jar
4. Mitigating phFortiInsightAI module:
   a. Delete these log4j jar files under `/opt/fortiinsight-ai/lib/`
      i. log4j-core-2.13.0.jar
      ii. log4j-api-2.13.0.jar
5. Restart all Java Processes by running: "`killall -9 java`"

On Worker Node

1. Logon via SSH as root.
2. Mitigating phFortiInsightAI module:
   a. Delete these log4j jar files under `/opt/fortiinsight-ai/lib/`
      i. log4j-core-2.13.0.jar
      ii. log4j-api-2.13.0.jar
3. Restart all Java Processes by running: "`killall -9 java`"

Slow Event Database Operations Using Azure Managed NFS File Share Service

If you are running a FortiSIEM 6.3.0 or 6.3.1 Cluster in Microsoft Azure Cloud using **Azure Managed NFS File Share Service**, then FortiSIEM will not work correctly. Symptoms are file build up in the `/data` directory and slow GUI queries. A bug was introduced in the Linux kernel (affecting Redhat CentOS 8.4 and FortiSIEM 6.3.0) that slows NFS operations. For details, see the section titled "*Is hangs for large directory enumeration on some kernels*" in this URL document: https://docs.microsoft.com/en-us/azure/storage/files/storage-troubleshooting-files-nfs

Note: If you deploy your own NFS V3 or V4, then FortiSIEM 6.3.0 or 6.3.1 is not impacted.

Redhat has not yet published a patch for this issue. The current workaround is to manually downgrade the Linux kernel from 8.4 to 8.3.

Download and install the Linux 8.3 kernel by following these steps on **each** Supervisor and **all** your Worker nodes.

1. On your system, login as user root, and run the following commands.
   Note: The order of the commands is important. If your system is offline without internet access, you can download the RPM to a flash drive or file share to upload to the Supervisor and Workers.
   a. `cd /tmp`
   b. `mkdir downgrade`
   c. `cd downgrade`
   d. `wget https://os-pkgs-cdn.fortisiem.fortinet.com/centos83/baseos/Packages/kernel-core-4.18.0-240.10.1.el8_3.x86_64.rpm`
   e. `yum localinstall kernel-core-4.18.0-240.10.1.el8_3.x86_64.rpm`
      Click 'y' to confirm when prompted.
   f. `grub2-mkconfig -o /boot/grub2/grub.cfg`
   g. `awk -F\' '$1=="menuentry" {print $2}' /boot/grub2/grub.cfg`
      Note: Entries are ordered 0,1,2,3,4 from top to bottom.
      If the kernel `4.18.0-240.10.1.el8_3.x86_64` is third in the list, use the command below to set it as the default.
   h. `grub2-set-default 2`
   i. Reboot the system with the following command:
      `reboot`
2. Log back in as user root and check the kernel version that is running with the following command:
   `uname -r`
   In the `uname -r` output, notate the new kernel. It should be:
   `4.18.0-240.10.1.el8_3.x86_64`

After the Linux kernel downgrade is done for the Supervisor and Workers, take the following steps:

1. Login to the Supervisor FortiSIEM GUI.
2. Go to the **ANALYTICS** tab.
3. Run a query for 10-30 minutes and confirm that the speed of the query execution is relatively fast.

Adding a Network Segment to a Fresh Installation of 6.3.1

A newly discovered device cannot be added into the network segment of a freshly installed 6.3.1 FortiSIEM.

Take the following steps before discovering devices.

1. Navigate to **CMDB > Devices > Network Segment**.
2. Click **New** to create a new device in the network segment group.
3. In the **Name** field, enter a name for the device.
4. In the **Access IP** field, enter the IP address of the device.
5. From the **Importance** drop-down list, select a priority.
6. Click the **Interfaces** tab.
7. Click **New** to configure the interface.
8. In the **Name** field, enter a name for the interface.
9. In the **IP address** field, enter the interface IP address.
10. In the **Mask/Prefix** field, enter the interface network mask.
11. Click **Save** to save the interface information.
12. Click **Save** to save the new device information.

After these steps are completed, FortiSIEM is ready to discover devices, and network segments are created automatically.

Elasticsearch Based Deployments Terms Query Limit

In Elasticsearch based deployments, queries containing "IN Group X" are handled using Elastic Terms Query. By default, the maximum number of terms that can be used in a Terms Query is set to 65,536. If a Group contains more than 65,536 entries, the query will fail.

The workaround is to change the “max_terms_count” setting for each event index. Fortinet has tested up to 1 million entries. The query response time will be proportional to the size of the group.

Case 1. For already existing indices, issue the REST API call to update the setting

```
PUT fortisiem-event-*/_settings
{
  "index" : {
    "max_terms_count" : "1000000"
  }
}
```

Case 2. For new indices that are going to be created in the future, update fortisiem-event-template so those new indices will have a higher max_terms_count setting

1. `cd /opt/phoenix/config/elastic/7.7`
2. Add `"index.max_terms_count": 1000000` (including quotations) to the “settings” section of the `fortisiem-event-template`.

Example:

...

```
  "settings": {
    "index.max_terms_count": 1000000,
```

...

3. Navigate to **ADMIN > Storage > Online** and perform **Test** and **Deploy**.
4. Test new indices have the updated terms limit by executing the following simple REST API call.

```
GET fortisiem-event-*/_settings
```

www.fortinet.com