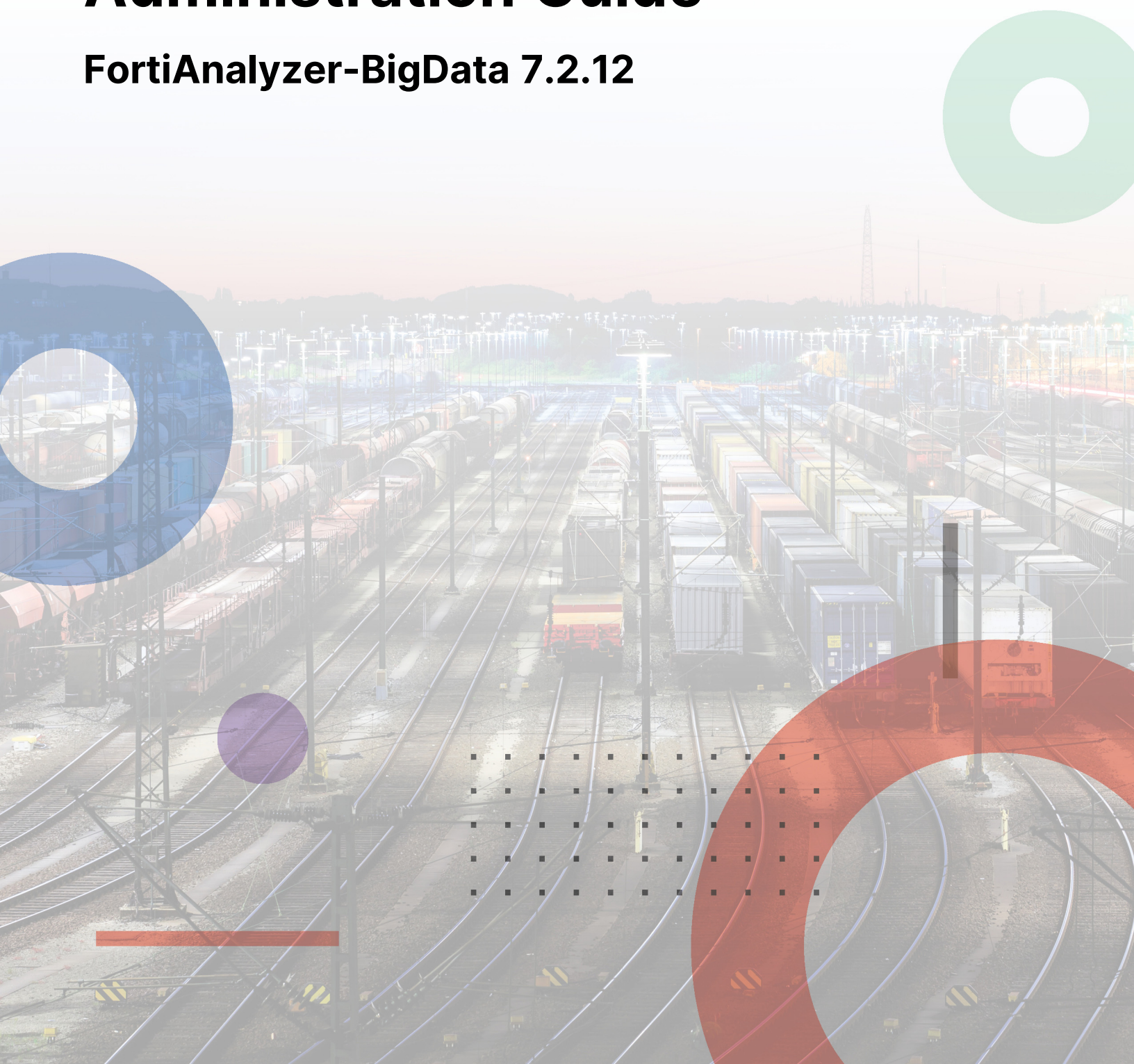
FORTINET

Administration Guide

FortiAnalyzer-BigData 7.2.12



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

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

May 21, 2026
FortiAnalyzer-BigData 7.2.12 Administration Guide
58-7212-1295320-20260521

TABLE OF CONTENTS

About FortiAnalyzer-BigData

FortiAnalyzer-BigData improves upon base FortiAnalyzer appliances and offers analytics-powered security and event log management to process large volumes of data. FortiAnalyzer-BigData is redesigned with a new distributed backend and high-end hardware. The Security Event Manager, the backend log engine of FortiAnalyzer-BigData, is a horizontally scalable, high availability (HA) system that supports the needs of large enterprise organizations. The Security Event Manager comprises multiple server blades working together as a cluster, so you can add new blades to expand and scale the Security Event Manager as your organization grows.

Main Features

FortiAnalyzer-BigData offers the following features:

High ingestion throughput

A single FortiAnalyzer-BigData can sustain 300k events per seconds (EPS) log ingestion.

FortiAnalyzer-BigData can sustain high throughput ingestion while continuing to perform analytics workload in the background.

Horizontal scalability backend

You can add additional appliance chassis to a running FortiAnalyzer-BigData without shutting down the system. This allows you to scale out the storage and query throughput.

Built-in high availability and fault tolerant backend

The backend, Security Event Manager, offers out-of-box fault tolerance and high availability with no need for initial configuration. All running services run under an active HA mode where data is replicated three times into different data hosts.

Easily recoverable data

By following regular backup scheduling procedures, you can recover lost data. FortiAnalyzer-BigData's backup drive configuration works with external Hadoop Distributed File System (HDFS) URLs.

Ease of management

FortiAnalyzer-BigData has a new Cluster Manager tile so you can manage and set up FortiAnalyzer-BigData from a centralized location. You can also monitor various service metrics, current host status, server logs and more from the Cluster Manager GUI.

Key terms and concepts

This section contains key terms used in FortiAnalyzer-BigData.

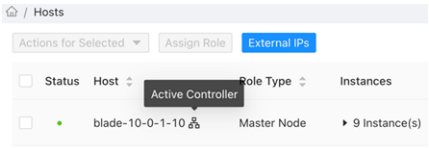
Security Event Manager

The Security Event Manager is the cluster formed by multiple server blades that serve the web GUI and performs the workload for data processing, persistence, query, and management of security log events.

Security Event Manager Controller

The Security Event Manager Controller, or cluster controller, is a single host within the Security Event Manager that functions as the main controller for the hosts. This host is responsible for the DHCP, configuration management, and lifecycle management such as upgrades, resets, and more. If this host goes down, it can automatically failover to a standby host.

To find out which of the hosts is the active Controller host, go to the Host view in the Cluster Management GUI, where the active Controller will be highlighted.



Alternatively, you can run the following CLI command:

```
fazbdctl show members
```

The controller appears in the *Role* column

Blade

This refers to the physical blade server enclosed within the FortiAnalyzer-BigData chassis.

The Chassis Management Module

The Chassis Management Module (CMM) is used to remotely manage and monitor server hosts, power supplies, cooling fans, and networking switches for the FortiAnalyzer-BigData unit. The CMM comes with a web management utility that consolidates and simplifies system management for the FortiAnalyzer-BigData chassis.

The web management utility aggregates and displays data from the CMM and provides the following key management features:

- Enables administrators to view in-depth hardware-level status information using a single interface.
- Provides an OS-independent, remote graphical console.
- Allows remote users to power control all or each of the blades.

Columnar Data Store

Unlike the traditional FortiAnalyzer data storage, FortiAnalyzer-BigData relies on the Kudu storage engine, which allows to store data in a columnar fashion.

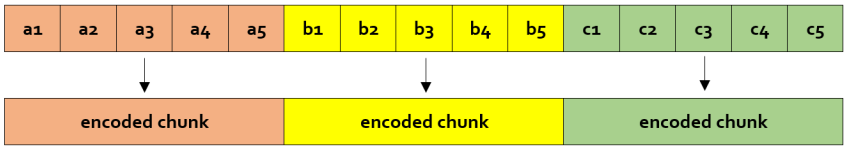
Tables are split into contiguous segments called tablets, which represent a generic logical unit ready for further replication and parallelization. The replication factor is "3", which means three copies are stored in the system: one original copy and two replicated ones. The replicas are guaranteed to spread across different nodes for fault tolerance.

A tablet with *N* replicas (usually three or five) can continue to accept writes with up to *(N – 1) / 2*.

Kudu uses the Raft consensus algorithm for the election of masters and leader tablets, as well as determining the success or failure of a given write operation, which enforces the data integrity across replicas.

Row layout:

Columnar layout:



This allows aggressive compression and possibility of querying only necessary columns.

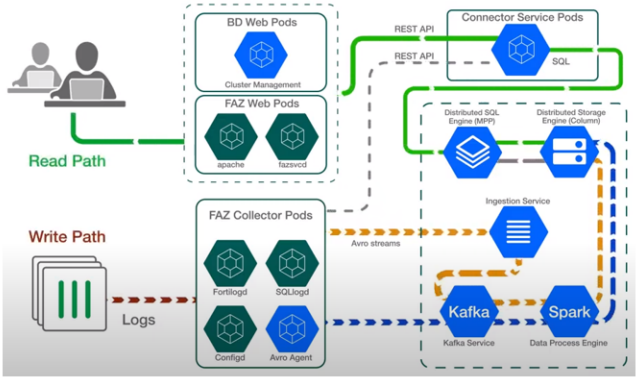
Kudu data store also makes stored log data mutable, which means that stored log events can be changed later.

Controller

This refers to the Security Event Manager Controller.

Data Flow

The following diagram shows the logging write and read path inside the platform:



Write Path:

The write path consists of the following steps:

1. Logs generated from logging devices arrive at the Main Host where the fortilogd process stores them temporarily on a local storage that serves as a buffer before distributing them across all hosts.
2. Logs are packed into a memory-efferent binary format and then streamed by the SQLlogd daemon to the "Ingestion Services", which are Kubernetes Pods processes running on each of Security Manager hosts and

acting as an interface accepting the log data and forwarding it to the Distributed Stateful Workload engines.

3. First Distributed Stateful engine receiving the log data from Ingestion Services is Kafka processes, acting as BD buffering platform for the logs.
4. Spark distributed engine then pulls the logs from Kafka buffers in parallel streams and processes them in fault-tolerant micro-batches. These micro-batches are streamed to Kudu acting as a distribute storage engine. Kudu processes store the logs in a columnar data store, where they can be easily retrieved.

Read Path:

The read path consist of the following steps:

1. An admin tries to access the Logs via *FortiView* or *Log View*.
2. The logs are queried via REST API and Connector Services Pods that consist of Kubernetes Pods processes providing the interface between Main Host and the Security Event Manager hosts.
3. The REST API calls are translated to SQL queries and forwarded to Impala acting as a Distributed SQL Engine.
4. Impala coordinates and distributes the queries across Kudu processes, allowing so called Massively Parallel Processing (MPP).
5. The logs pulled from Kudu are then forwarded to FortiAnalyzer web services and displayed in GUI.

Data Management

The concept of "Archive logs" and "Analytics logs" is not valid for FortiAnalyzer-BigData. All logs are load-balanced across all hosts, where data is compressed, replicated, and available for immediate analytics.

Logs are stored in CFile format with a size of approximately 300 bytes post replication (x3) and compression.

Host

This refers to one of the server hosts in the FortiAnalyzer-BigData system.

Instances

Also known as Service instances. This refers to the instance serving the service. There are usually multiple instances running behind a service load balance.

Main host

The FortiAnalyzer-BigData main host is responsible for collecting logs and providing the services for FortiView, Log View, Reports, and more.

For FortiAnalyzer-BigData units, the main host runs on Blade A1.

Roles

The FortiAnalyzer-BigData hosts are categorized into different roles according to the kind of stateful services running on them. The roles are assigned automatically during the cluster initialization. The placement of those stateful services on each role is designed to achieve optimized performance, high data and service availability and scalability, and is immutable after the cluster is initialized. In a scaling-out scenario (see Scaling FortiAnalyzer-BigData on page 104), additional hosts can be added as Data nodes to the existing cluster. For

FortiAnalyzer-BigData units, the additional hosts can be added on the extender chassis to the existing cluster in the main chassis.

FortiAnalyzer-BigData has the following roles and services:

- Main Node (this role exists for FortiAnalyzer-BigData-4500G only)
  - Log Collector
  - Main Services
- Master Node
  - Consul
  - Contoller Service
  - HDFS Datanode
  - HDFS Journalnode
  - Impala
  - Kafka Broker
  - Kudu Master
  - Kudu Tablet Server
  - Zookeeper
- MetaStore Node
  - HDFS Datanode
  - HDFS Namenode
  - Hive Metastore
  - Impala
  - Impala Catolog
  - Impala Statestore
  - Kafka Broker
  - Kudu Tablet Server
- Data Node
  - HDFS Datanode
  - Impala
  - Kafka Broker
  - Kudu Tablet Server

Services

This refers to the Security Event Manager services that are responsible for security data management, security data processing, storage, cluster management, and more.

Storage Pool

A Storage Pool is a set of one or more ADOMs. Storage pools provide fine-grained control over the data retention policy and improves the query and ingestion performance. Each storage pool can have its own data retention policy that controls the maximum age (in days) and disk utilization of the data. ADOMs within the same storage pool share the storage pool resource.

We recommend grouping ADOMs with similar log rates and data retention requirements into a storage pool. For example, group small ADOMs (in terms of log rate and data volume) into one storage pool and larger ADOMs in

another. If different sized ADOMs are grouped into one storage pool, the query performance on the smaller ADOMs will be affected by the larger ADOMS.

FortiAnalyzer-BigData hardware environment

FortiAnalyzer-BigData 4500F and FortiAnalyzer-BigData 4500G units are available. Each unit is a 4U chassis with two network switch modules and 14 blades in the enclosure.

In the FortiAnalyzer-BigData-4500F unit:

- The first blade is responsible for log collection and services for FortiView, Log View, Reports, and more.
- The remaining 13 blades, also known as hosts, are responsible for the web GUI, log storage, data processing, and analytics.
- The switch modules are 10Gbps.

In the FortiAnalyzer-BigData-4500G unit:

- All blades are used for all functions (log collection, log storage, data processing, analytics, and so on).
- The switch modules are 25Gbps.

Unit	CPU	RAM	Storage
4500F	**Blade 1**: two 2.1GHz Intel Xeon 12 Core and 24 Thread (12C24T) CPUs **Remaining 13 blades**: two 2.1GHz Intel Xeon 8 Core 16 Thread (8C16T) CPUs per blade	128GB per blade	**Blade 1**: two 750GB NVMe SSD **Remaining 13 blades**: two 7.68TB NVMe SSD per blade
4500G	two 2.3GHz Intel Xeon 16 Core 32 Thread (16C32T) CPUs per blade	196GB per blade	two 7.68TB NVMe SSD per blade

The two network switch modules on the back of the chassis have different functions.

- Switch Module #1 connects to the FortiAnalyzer-BigData cluster's internal network.
  Use this switch only when you need to scale the existing Security Event Manager by adding new appliances.
- Switch Module #2 is the External Switch Module used to expose the FortiAnalyzer-BigData to external networks.

The Chassis Management Module (CMM) sits between the two switch modules in the middle of the back panel.

For more information about the CMM, see the appripriate FortiAnalyzer-BigData Getting Started Guide for your appliance on the Fortinet Document Library.

Connect to the FortiAnalyzer-BigData CLI

After configuring the FortiAnalyzer-BigData network, you can use the IP addresses to access the FortiAnalyzer-BigData Main CLI or the Security Event Manager Controller and manage the system.

To connect to the FortiAnalyzer-BigData Main CLI:

1. Establish an SSH connection to the *Main Host* IP you configured in the set up process.
   For the set up process, see the FortiAnalyzer-BigData Getting Started Guide for your appliance on the Fortinet Document Library.
2. Log in using the administrator credentials you created when setting up the administrator account.
   If you did not create a new administrator credential, use the default credentials of username `admin` with no password.

To connect to the Security Event Manager Controller:

1. Establish an SSH connection to the Cluster Management IP you configured in the set up process.
   For the set up process, see the FortiAnalyzer-BigData Getting Started Guide for your appliance on the Fortinet Document Library.

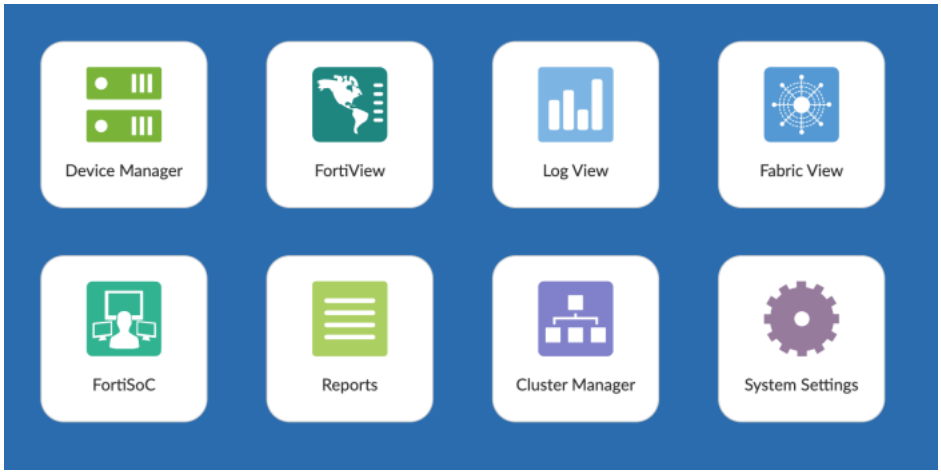
   If the Cluster Management IP is not reachable, you can SSH to the Main CLI first (see *To connect to the FortiAnalyzer-BigData Main CLI*.) and then SSH to the Controller host or any of the cluster hosts using its internal IP. (For example, to SSH to the Controller host, use `exec ssh root@198.18.1.2`).
   The IP it is in can be determined by this format: `198.18.{chassis_id}.{blade_id}` where 198.18* is the default internal subnet.
2. Log in using the default username `root` and password `fortinet@123`.
3. After establishing a connection, you can use the `fazbdctl` CLI commands to manage the cluster. For more information, see the FortiAnalyzer-BigData CLI Reference on the Fortinet Doc Library.

   Fortinet strongly recommends that you update the password with the `fazbdctl set password` command.

GUI overview

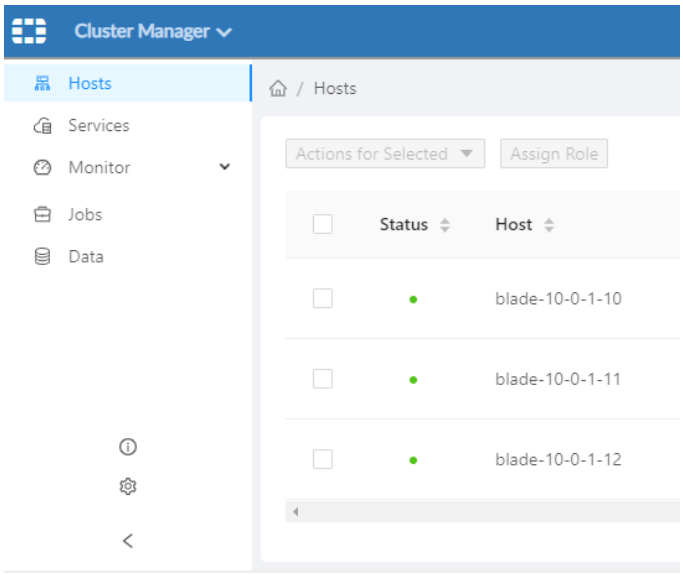
FortiAnalyzer-BigData retains the same general GUI as the base FortiAnalyzer. In addition, there is a *Cluster Manager* tile.



Cluster Manager	The Cluster Manager module enables you to manage hosts, services, logs, queries, jobs, and data resources in the Security Event Manager. See Cluster Manager on page 13.
System Settings	Configure system settings such as network interfaces, administrators, system time, server settings, and others. You can also perform maintenance and firmware operations. See the FortiAnalyzer administration guide.

Cluster Manager

The Cluster Manager module enables you to manage hosts, services, logs, queries, jobs, and data resources in the Security Event Manager.



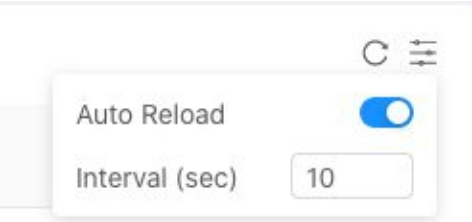
Use the navigation bar to access all the pages within the module.

Section name	Description
Hosts	The Host page enables you to centralize Security Event Manager. It also shows the service assignments as well as resource usage of each host within the Security Event Manager. For more information, see Host management on page 17.
Services	The Services page enables you to manage the configurations and life cycle of the Security Event Manager. For more information, see Service management on page 21.
Monitor	The Monitor section contains three pages: • **Dashboard:** Provides a customizable visualization for system metrics. • **Log and Metrics:** Contains an Explorer tool that enables you to search the logs and metrics that FortiAnalyzer-BigData produces. • **Health:** Provides push notifications for system health checks and other events. For more information, see Monitor on page 26.
Jobs	The Jobs page manages system jobs and custom jobs. • System jobs include data retention jobs which removes data outside of the retention period. From this page, you can run jobs, and see the status and history of all your jobs. • Custom jobs can be set up with built-in templates or customizable playbooks. For more information, see Job management and automation on page 67.
Data	The Data page enables you to manages the data life cycle of your storage pools as well as data backups and restores. For more information, see Data management on page 75.
System Information	Click to see the current system version number.

Section name	Description
System Upgrade	Click to see your current system version and to upgrade FortiAnalyzer-BigData.

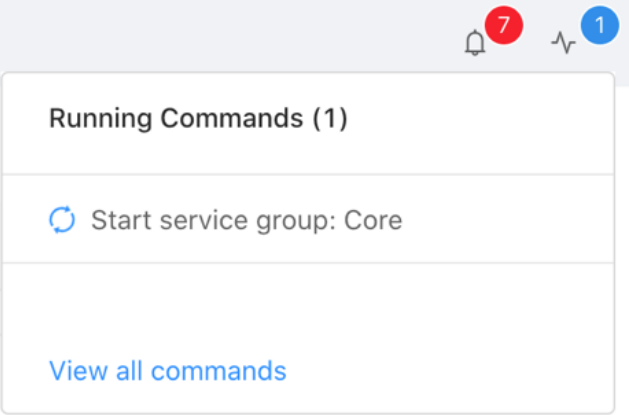
Custom refresh settings

When viewing tables in the Cluster Manager, you can manually refresh the data in a table by clicking *Refresh*, or you can set up an automatic reload timer. Click *Custom Settings* at the top-right corner of a table to configure the refresh setting.



Commands management

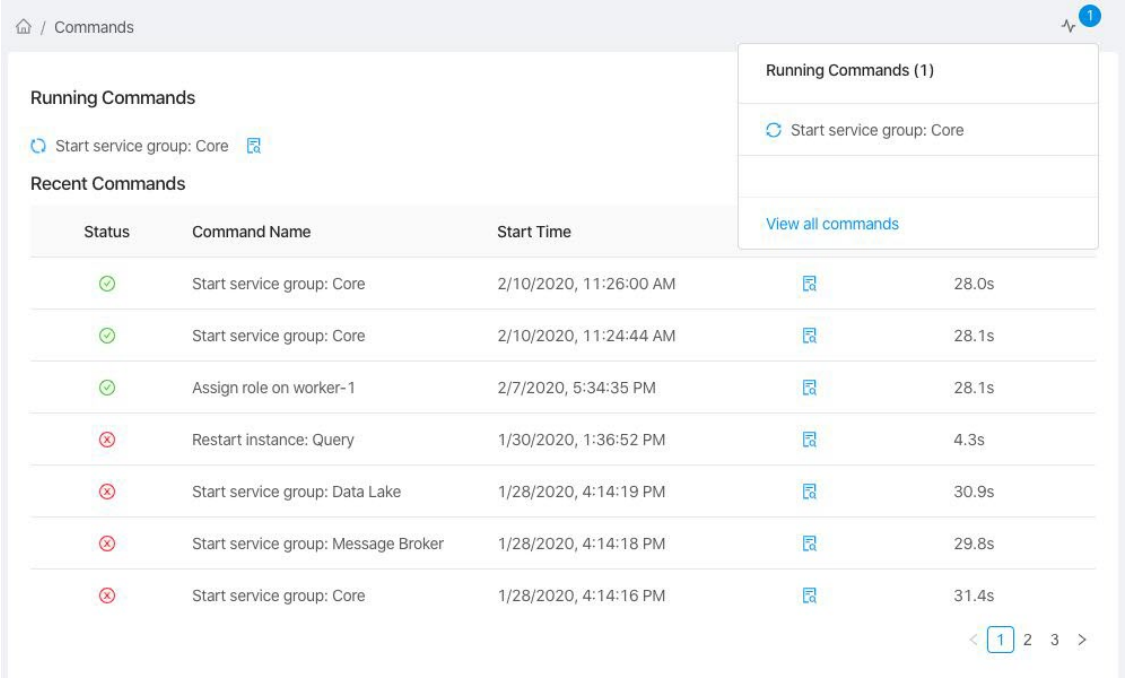
There is a Commands icon in the top-right corner of each page that notifies you whenever a command is running in the background. You can click the icon to expand the Commands snapshot view and see all currently running commands.



To access the Commands Manager page

1. Click *Commands* in the top-right of each page.
   The Commands snapshot view loads, showing all the currently running commands.

2. Click *View all commands* at the bottom of the snapshot to view the full list of commands.

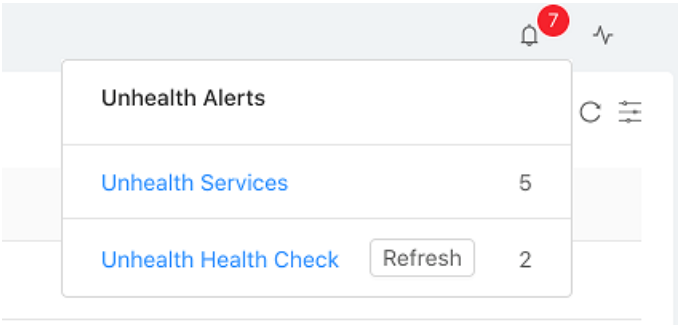


The icon by each command indicates if the command was executed successfully.

	The command was successfully executed.
	The command failed.

Notifications management

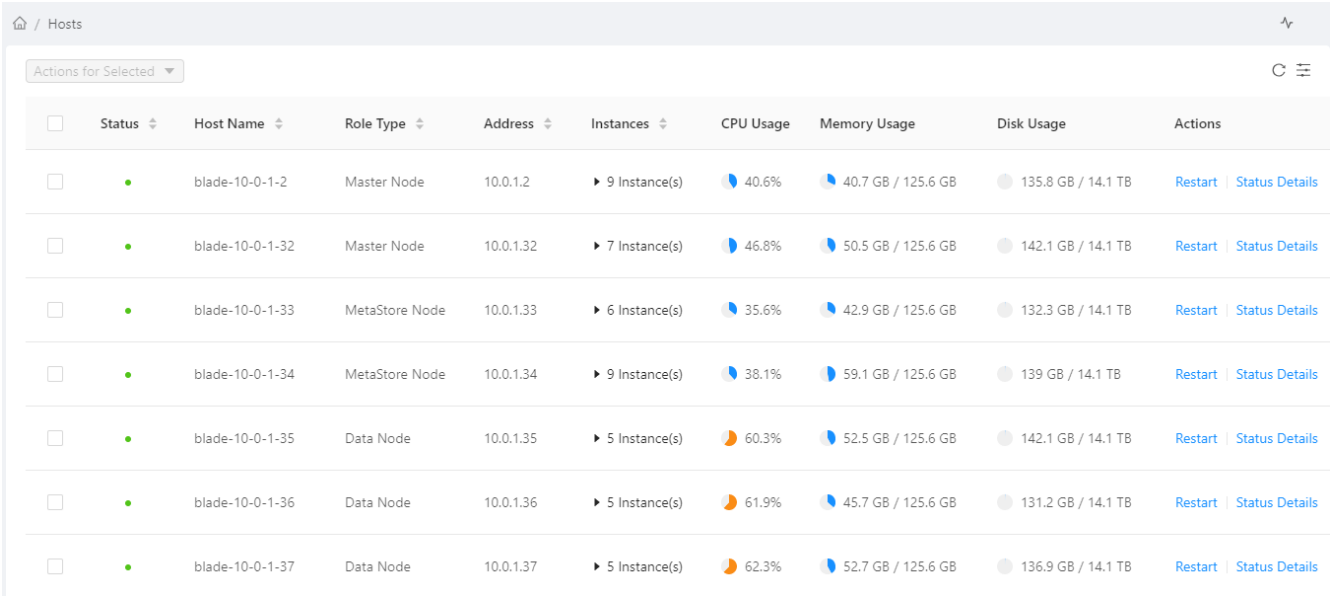
There is a *Notifications* icon in the top-right corner of each page that notifies you each time there is a notification. You can click the icon to expand the Notification snapshot view and see more details. Clicking a notification item directs you to the page related to the notification event.



For the specific alerts such as the "Unhealth Health Check" alert, you can click the *Refresh* button to refresh all information related to that check.

Host management

The Host page has a table that provides an overview of all the hosts in the Security Event Manager. You can use the *Actions* column to manage hosts.



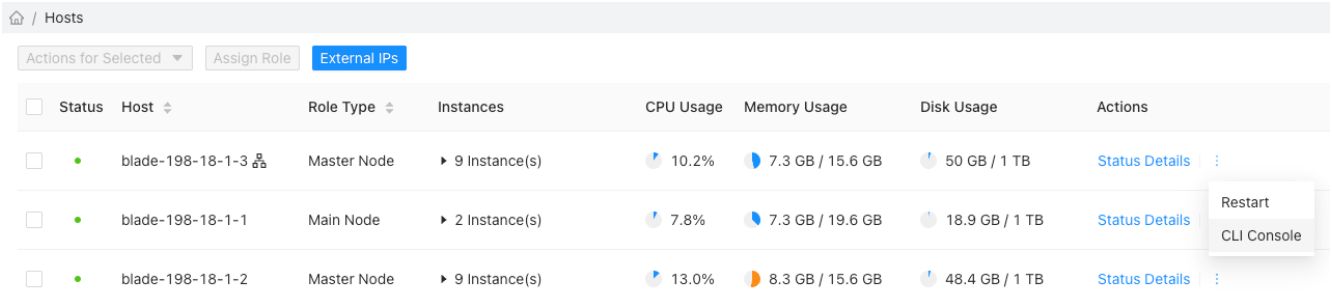
The Host table contains the following columns:

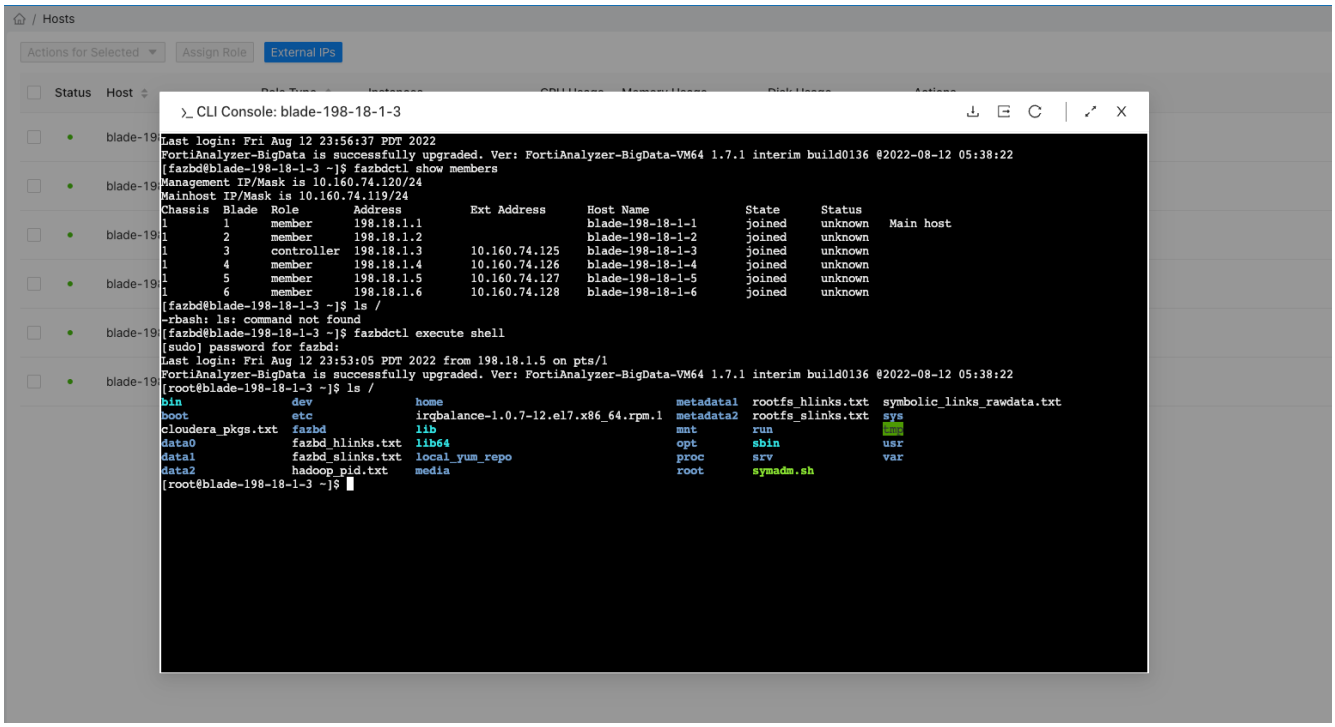
Column header	Description
Status	There are three icons that represent the status of the host: The host is healthy. The host is in poor health. A command is currently running on the host.
Host Name	The name of the host.
Role Type	Each host can have one role. For more information about each role, see Roles on page 9. • **Main Node** (for FortiAnalyzer-BigData-4500G only) • **Master Node** • **MetaStore Node** • **Data Node** • **Unassigned:** The host is new and does not have an assigned role. Click *new* to assign a role to that host (see Role assignment on page 19).
Address	The IP address of the host.

Column header	Description
Instances	The number of Service instances on each host. You can expand the row to see which instances are on each host and their current status.
CPU Usage	The percentage of the CPU being used.
Memory Usage	How much memory is being used.
Disk Usage	How much space is being used on a disk.
Actions	You can perform the following actions on each host: • **Restart:** Restart the host. • **Status Details:** See the full metrics view of the host. • **Assign Role:** Assign a role to a new host.

CLI Remote Console

You can remotely enter the CLI console of a FortiAnalyzer-BigData cluster host on *Cluster Manager* web GUI. To enter the CLI console of a host, click the *CLI Console* in the menu under the *Actions* column. Each host has its own CLI console and multiple consoles can be opened at the same time.





The CLI Console view supports the following actions:

Button	Action	Description
	Download History	Download the current console output.
	Open as new tab	The CLI console will open in a new browser tab.
	Reconnect	Reconnect to the host's CLI console.
	Maximize	Click to expand the console to fit the window. Click again to restore the window size.

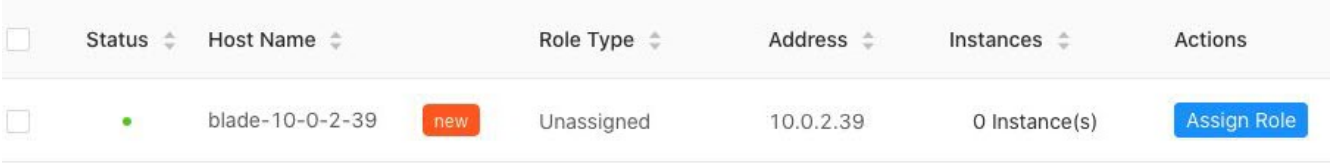
By default, the CLI console has limited access to the shell that allows only some of the `fazbdctl` and `fazbdadm` commands. You can enter the secure shell with the following command:

```
fazbdctl execute shell
```

FortiAnalyzer-BigData cluster host's OS password will be prompted. For more information, see *Set Cluster Hosts OS password* and *Enable Secure Shell* in the *FortiAnalyzer-BigData CLI Reference Guide*.

Role assignment

Hosts that have an Unassigned role type are flagged with a *new* notification.



You can assign a role to a host by clicking *Assign Role* in the Actions column.

To assign a role to a host

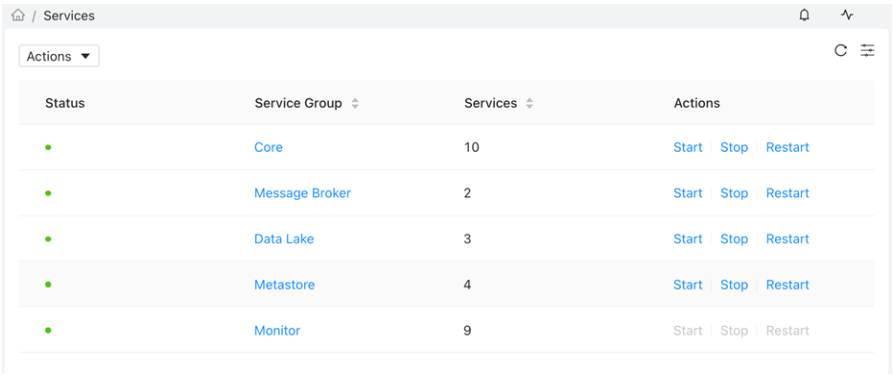
1. In the Actions column, click *Assign Role*.
   The *Assign Role dialog* loads.
2. Select the role you want to assign to the host.

   At this time, you can only assign the Data Node role.

3. Click *Assign* to confirm your selection.
   FortiAnalyzer-BigData begins the role assignment process.

Service management

The Services page has a table with information about all the services running on your system. This table provides an overview of all your services and enables you to monitor and manage all the services running in the system.



The Services table contains the following columns:

Column header	Description
Status	There are five icons that represent the status of the host: The services are healthy. A command is currently running. There is a problem with the service. Services within the service group are experiencing issues. The service has stopped.
Service Group	Service Groups are a way to group and categorize individual services. Click on the Service Group to access the Service Configuration page and manage the services contained inside. By default, FortiAnalyzer-BigData has five pre-defined Service Groups (see Service groups on page 22).
Services	The number of services running in each group.
Actions	There are three actions you can perform on each Service Group or service. • **Start:** Start the service group or a specific service. • **Stop:** Stop the service group or a specific service. • **Restart:** Restart the service group or a specific service.

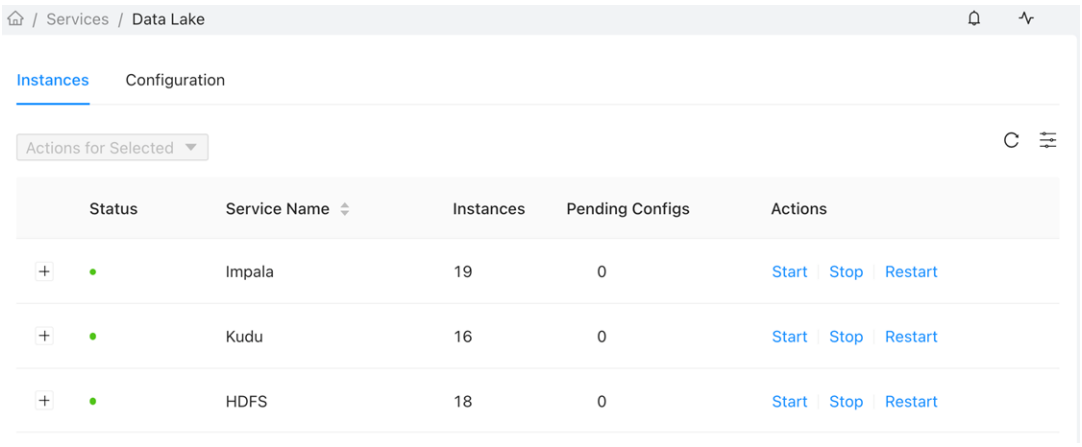
Service groups

Services are organized into Service groups, which can contain several services. Each service can further contain multiple instances running on a host. By default, FortiAnalyzer-BigData has five pre-defined Service groups that contain the following services:

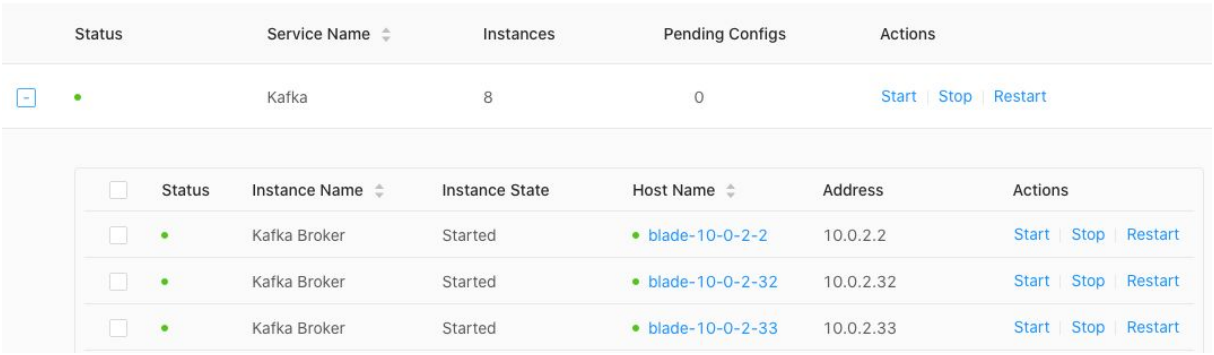
Service Group	Services within the Service group
Core	• Catalog • Query • Ingestion • Data Explorer • Pipeline • Controller Service • Controller Failover • Management Portal • Management Server • Management Task
Message Broker	• Kafka • Rabbitmq
Data Lake	• Impala • Kudu • HDFS
Metastore	• Zookeeper • Consul • Redis • Stolon
Monitor	• Monitor Portal • Metrics Server • Metrics Exporters • Log Server

Service details

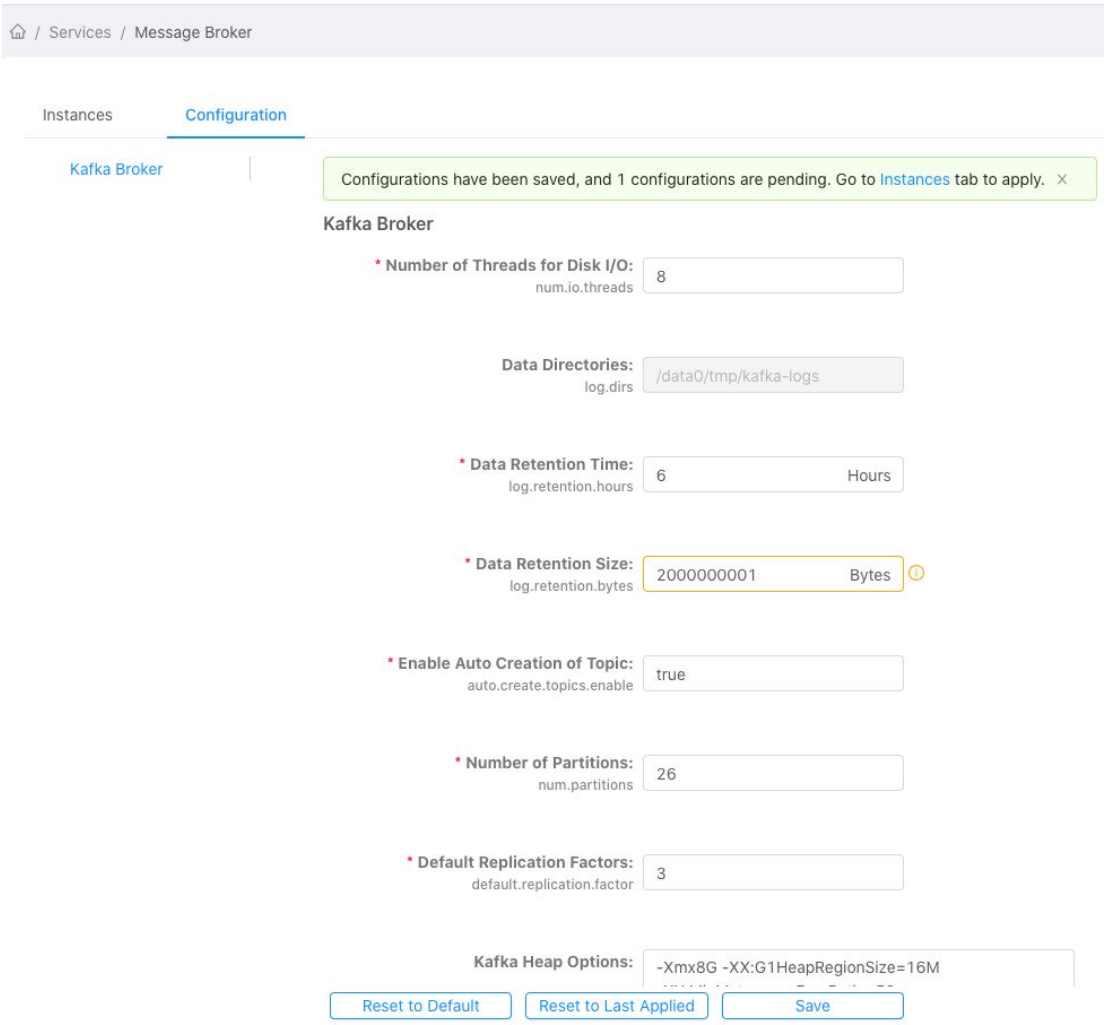
To access the Service Details page, click the name of the Service group.



The Service Details page contains all the services grouped under the Service group. You can expand each service to see the instances it contains, and manually start, stop, or restart those services.



Some services may contain configurations that you can modify via the Configuration tab.



To modify service configurations

The FortiAnalyzer-BigData default configurations are optimized for performance, availability, and scalability. Configure these settings with caution as improper configurations can have a negative impact on the entire system, and even lead to system failure or data loss. Approach these options with great care and when in doubt, err on the side of caution.

1. From the Service page, click the Service group name to access the Service Configuration page.
2. Click *Configuration* to switch to the Configuration tab.
3. Modify the fields as needed.
4. Once you are finished, click *Save*.
   Once you save the changes, you must apply the changes.

You can click *Reset to Default* to reset the changes to the default configurations, or click *Reset to Last Applied* to reset the configurations to the last changes you applied.

5. To apply the configurations, click *Instances* to return to the Instance tab.
   The number in the Pending Configs column changes to reflect the number of configurations that are pending.
6. In the Actions column, click *Apply Config* to apply the changes.

Monitor

From the Navigation bar, you can expand the Monitor section to access three pages:

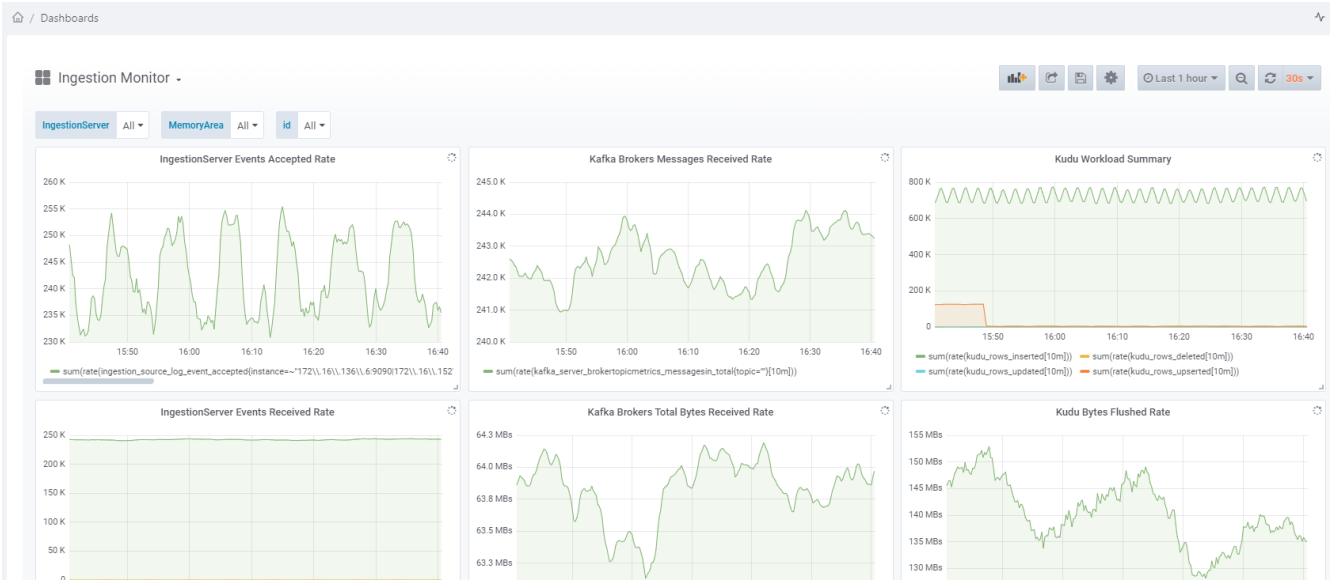
- Dashboards
- Logs and metrics
- Health

Dashboards

The Dashboards page displays both real-time monitoring and historical trends of your system metrics.

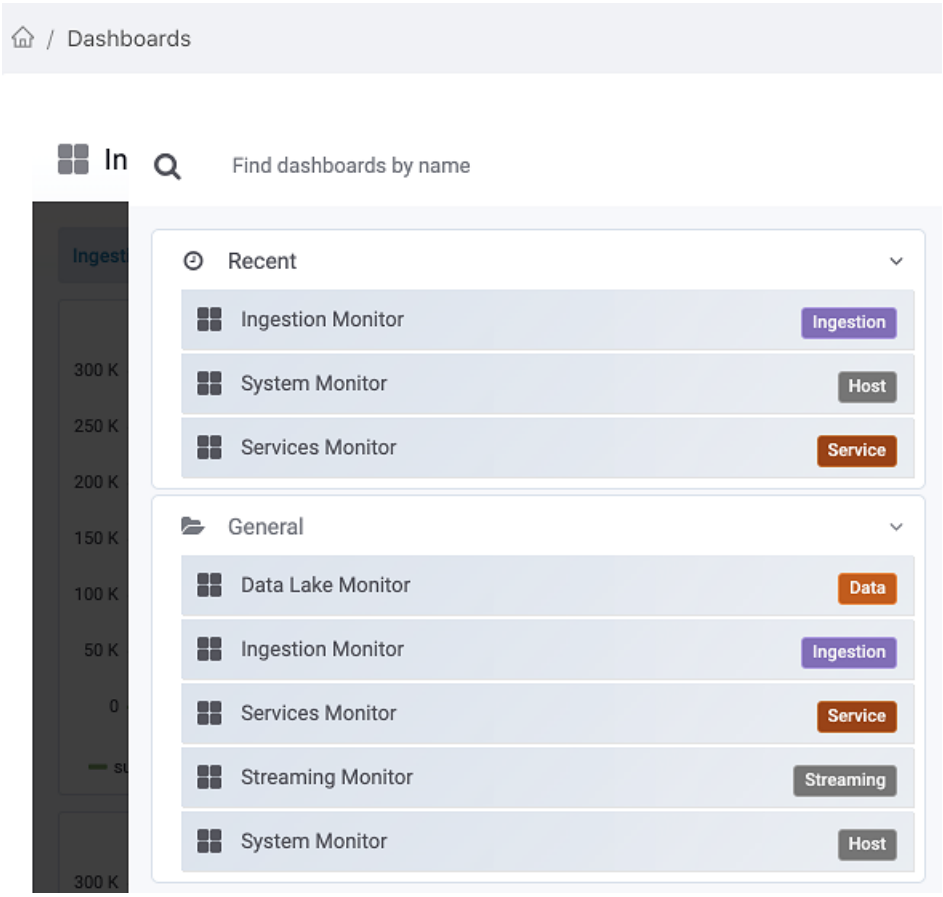
From the Dashboard, you can:

- Select specific data to focus on and filter your results to narrow down your view
- Customize the panels on your dashboard
- Use panels to see more information and set alerts



Filtering the Dashboard

You can filter the dashboard to focus on different areas of focus. By default, the Dashboard shows statistics relating to data ingestion. You view built-in dashboards by clicking the title of each page (for example, Ingestion Monitor) and selecting a topic from the drop-down list.



You can view the following built-in dashboards:

- Ingestion
- Data Lake
- Services
- Streaming
- System

In some views, you can filter your results to show information from a specific server, node, memory area, ID, and more. You can also narrow down results to a specific time period and set the refresh rate.

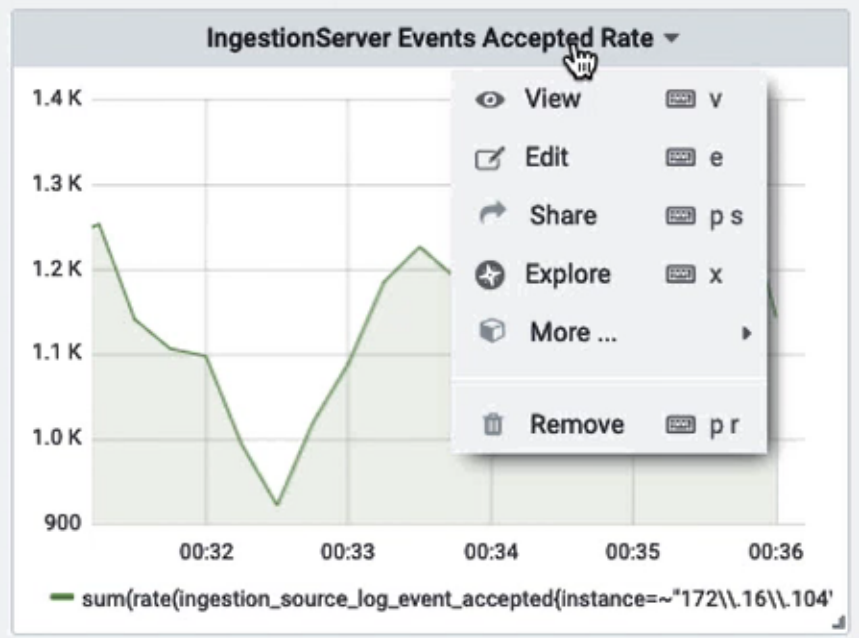
Customizing the Dashboard

You can customize the FortiAnalyzer-BigData dashboard by adding new panels, creating custom settings, and saving those settings. Once you've customized the dashboard, you can share the dashboard.

Dashboard actions	Description
Add panel	Add a panel to your dashboard. Once a blank panel appears on the dashboard, you can select the following actions: • Add Query: Choose what metrics to track, • Choose Visualization: Choose how you want to visualize the data. • Convert to row: Convert a group of panels into a collapsible row.
Share Dashboard	Share the dashboard with a link or by exporting a JSON file.
Save Dashboard	Save all the changes you've made to the dashboard.
Dashboard settings	
General	Configure general settings for the current dashboard. The FortiAnalyzer-BigData dashboard is built on Grafana. For more information about using dashboard features, refer to the official Grafana documentation.
Annotations	Add annotations to mark points on a graph.
Variables	Add variables to change the data being displayed in the dashboard.
Links	Add a link to your dashboard so you can go to other dashboards and websites directly.
Versions	See the revision version history for the dashboard.
JSON Model	See the JSON model that defines the dashboard.

Using panels

The Dashboard contains panels that display specific metrics. You can drag and drop each panel to rearrange your Dashboard view, or stretch the panel to see more details. Click the drop-down menu on each panel to get a list of available actions.

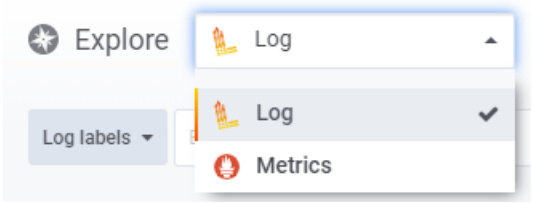


Panel menu actions		Description
View		Enlarge the panel to see a more detailed view of the graph.
Edit		You can customize the panel to show specific queries, change the way you visualize data, and set alerts rules to inform you when certain conditions are met.
Share		There are two ways to share your panels: • Create a direct link to the particular panel. • Create a snapshot of the panel with sensitive data stripped out.
Explore		View the historical logs and metrics for the panel.
More		
	Duplicate	Add a duplicate of the panel to your dashboard.
	Copy	Create a copy of the pane. You can paste the panel to the Dashboard from *Add panel*.
	Panel JSON	See the JSON model that defines the panel.
	Export CSV	Export a CSV file with panel data.
	Toggle Legend	Click to display or conceal the panel legend.
Remove		Remove the panel from the Dashboard.

Logs and metrics

The Logs & Metrics page contains all the logs and metrics that FortiAnalyzer-BigData produces.

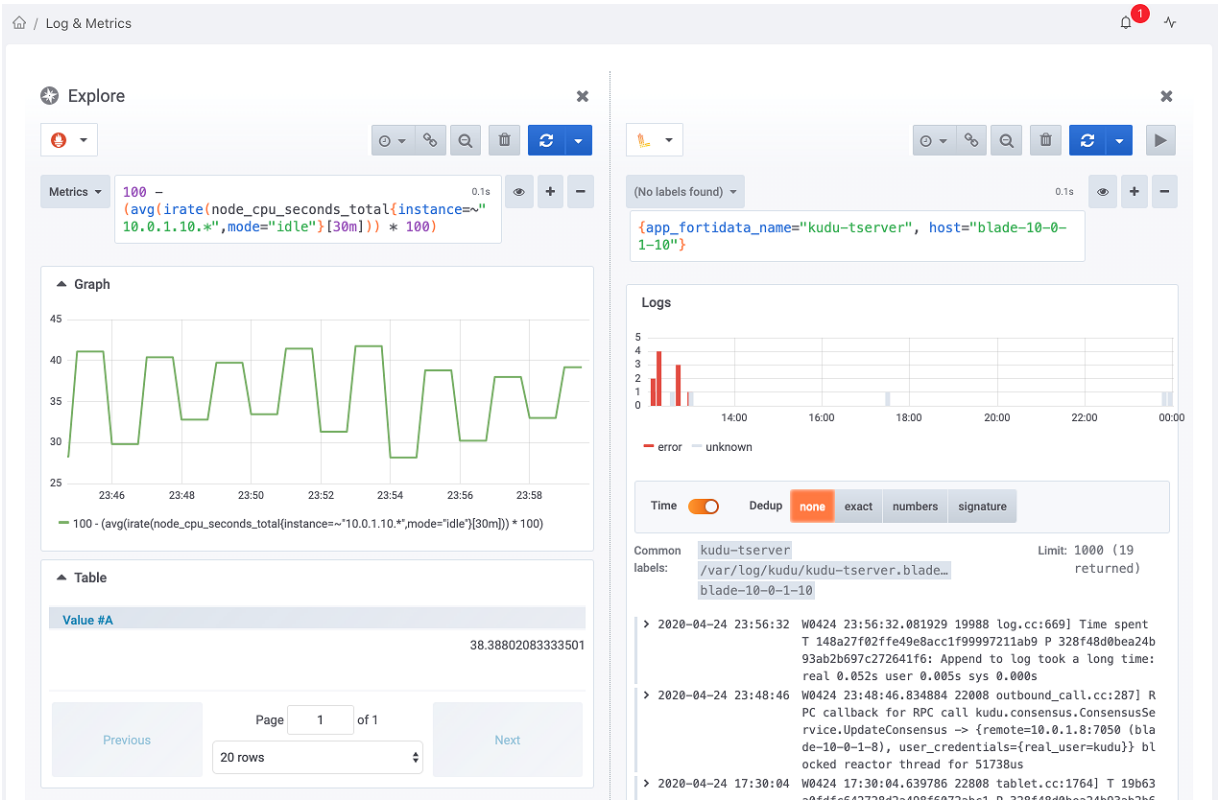
You can use the Explore search tool to switch between the Logs or Metrics view. The default selection is Logs.



- Logs are immutable records of discrete events that happened over time in the system.
- Metrics are a set of numbers that give information about a particular process or activity.

After you select a view, you can search for the particular log or metric that you want to see. You can add filters to show results from a certain time range.

The Logs and Metrics page has a Split screen feature which enables you to compared two different Logs or Metrics at the same time. Click *Split* to create a side-by-side comparison view.



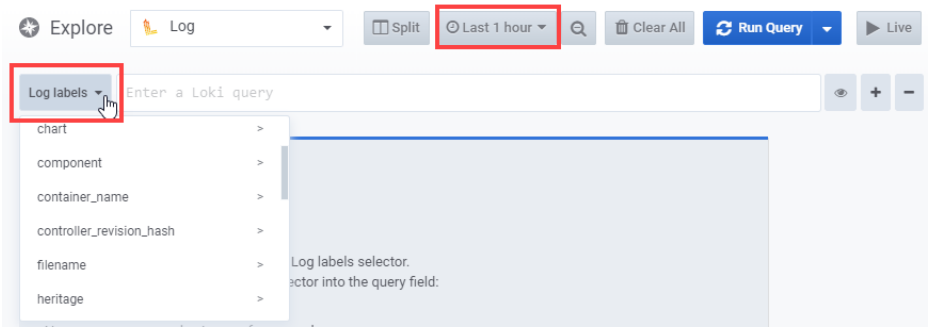
Explore logs

A log query has two main components:

- a log stream selector; and
- a search expression.

Choosing a log stream

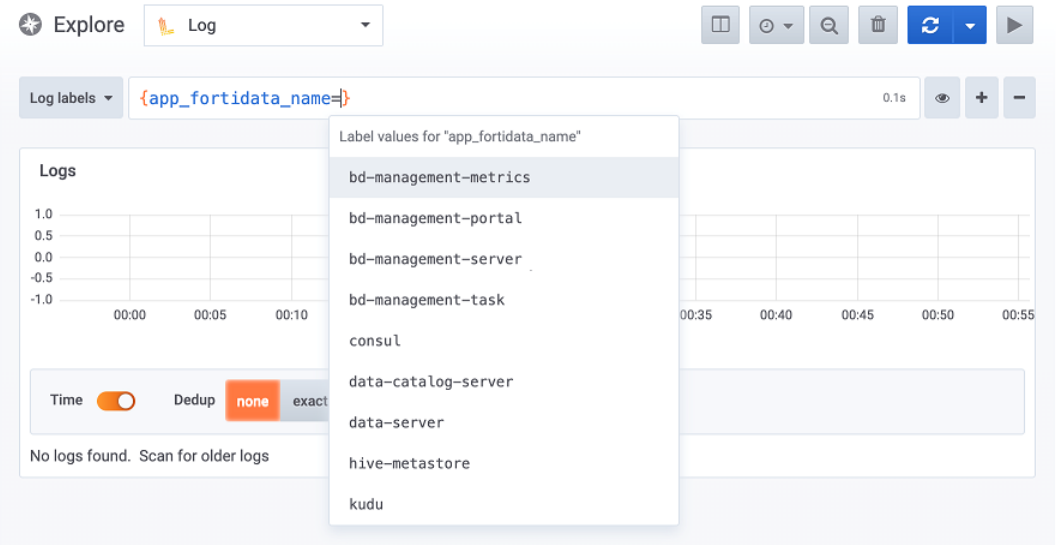
Choose a log stream by clicking the *Log labels* button next to the search bar, and select from the available log streams in your time range (the default time range is Last 1 hour).



If there are no logs in the selected time range, the log label of the log will not show up in the label list.

Entering a search expression

You can start a search query by using the search field's autocomplete feature. Enter a curly bracket { in the search field to see a suggested list of labels. You can browse through the suggested labels with your cursor or arrow keys and press the Tab key to select a label. Press the Enter key to execute the query.



The log stream selector is wrapped inside curly braces {} with the key and value of selecting labels. You can select multiple labels by using commas, for example:

```
{app_fortidata_name="ingestion-server", host="blade-10-0-1-10"}
```

This example selects the ingestion-server log on host blade-10-0-1-10.

After you choose a selector, you can follow up by entering a search expression to filter the results further. Search expressions can be in a text or regex expression, for example:

```
{app_fortidata_name="data-server"} |= "ERROR"
{app_fortidata_name="ingestion-server"} |~ "Starting.*engine"
{host="blade-10-0-1-10"} != "INFO"
```

You can chain the operators in order to search the log lines and satisfy all filters. For example:

```
{app_fortidata_name="ingestion-server"} |= "ERROR" != "timeout"
```

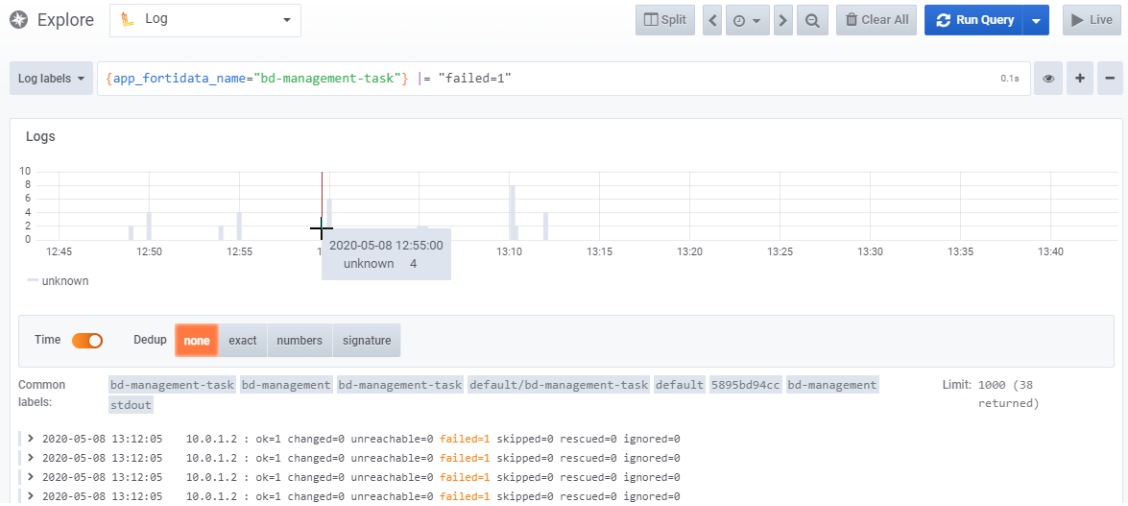
Supported operators:

- |= line contains a string.
- != line does not contain a string.
- |~ line matches regular expression.
- !~ line does not match regular expression.

For more details, refer to the Loki query language (LogQL) documentation.

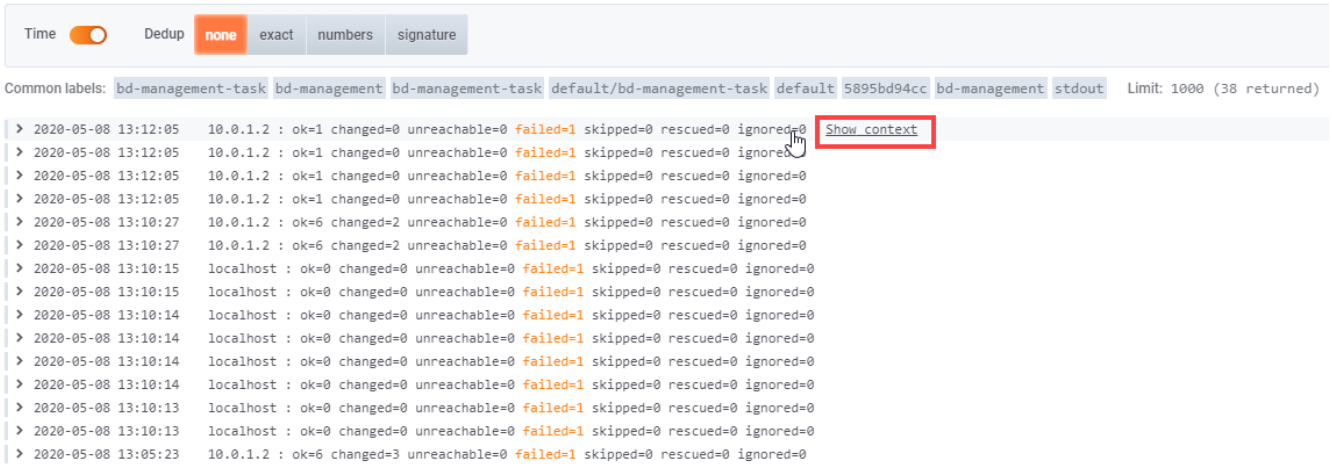
Log query results

After you run a query, search result are presented as either a list of log rows and/or a bar graph. For results with a bar graph, the time is placed on the x-axis while log count is on the y-axis. You can click and drag on the bar chart to narrow down the time range.



You can also click the *Live* button to enter Live Tailing mode and see logs changes in real-time.

If you use a search expression, you can see the context for each filtered result by hovering your mouse over a result and clicking the *Show Context* link by each result.

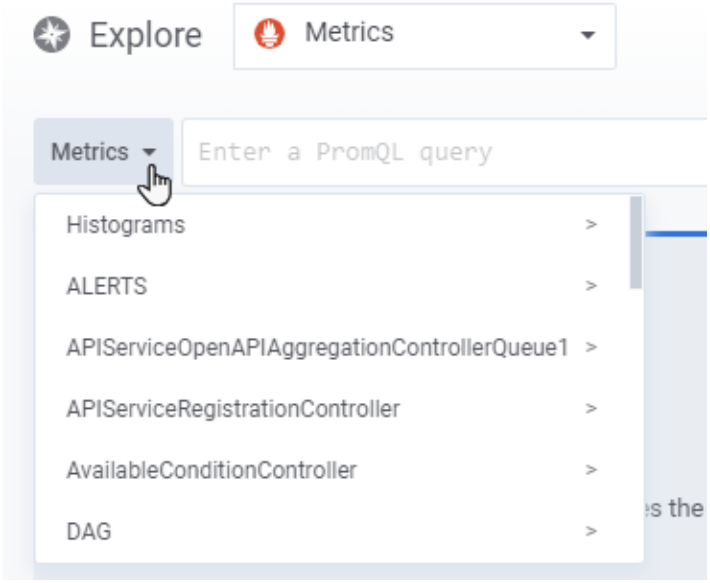


When you click *Show Context*, a new window loads enabling you to see the context of that particular result.

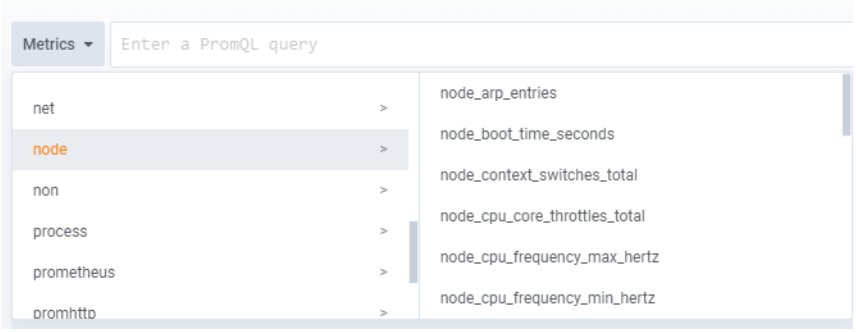
Explore metrics

Access the Explore Metrics view by changing the Explore field selection to *Metrics*.

To search for a metrics, click the *Metrics* dropdown to open a hierarchical menu with available metrics.

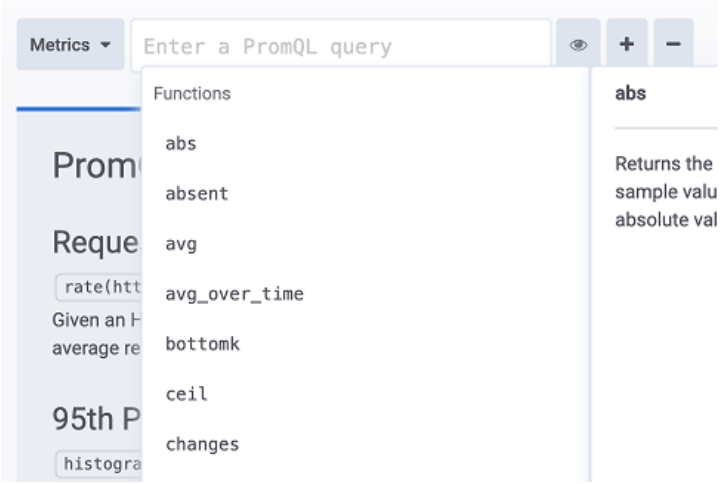


Metrics are grouped by prefixes, for example, all Node metrics are grouped under the "node" prefix.



After you select a metrics key, the data is represented with a graph and table. The raw data is listed in the table with label keys as columns and the label values and metric values as rows.

You can also start a query by pressing the `Ctrl` key in search box to display suggestions for metric names and functions. Press the `Enter` key to execute.

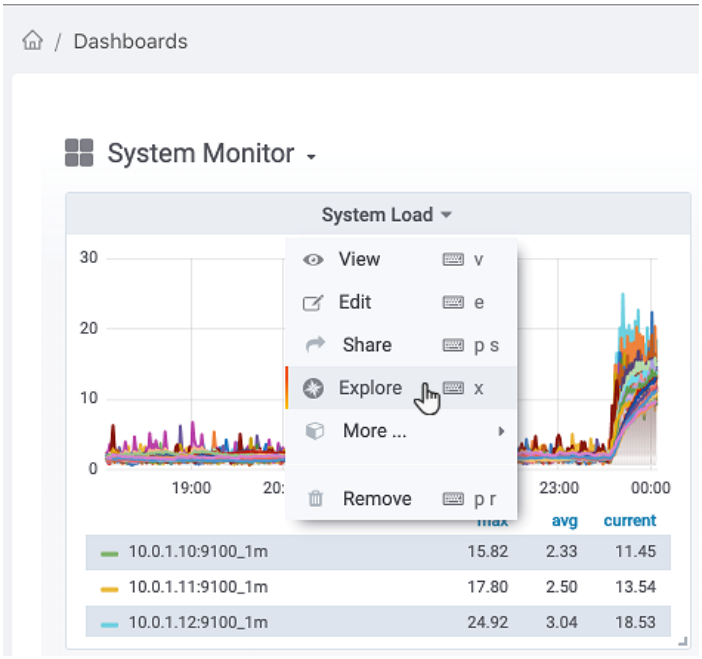


For more details, refer to the Prometheus Query Language documentation.

Accessing a specific metrics from the Dashboard

You can also access a specific metric by drilling down from a dashboard panel.

Find the specific panel you want to see metrics data for, click the panel title and select *Explore*.

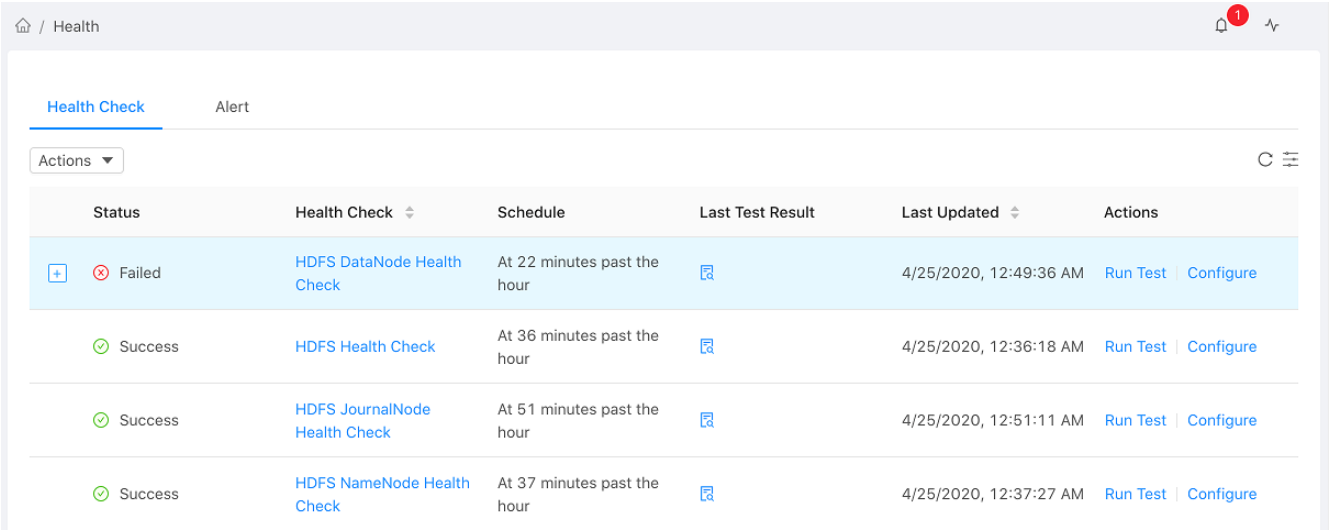


Health

In the Health page, you can set alerts for system health checks, and configure how you want to receive your alerts.

Health Check

The Health Check tab displays a table containing all predefined health checks in the system.



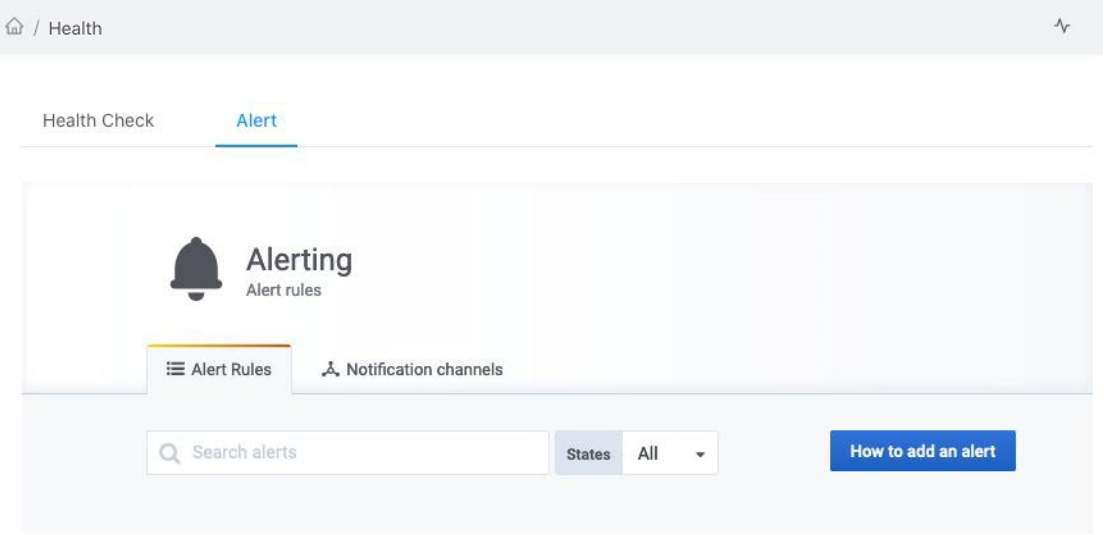
The Health Check table contains the following columns:

Column header	Description
Status	Indicates if the health check was a success or failure. If a health check fails, you can click *Expand* in the item row to see the error message.
Health Test	Shows what health check was run. You can click the name to see the history for that health check. FortiAnalyzer-BigData only saves the last 500 records for each health check.
Schedule	Shows how often the health check is run.
Last Test Result	View the full health test result by clicking *Test Result*.
Last Updated	The last time the health test was run.
Actions	You can perform two actions on the health test:

Column header	Description
	• *Run Test:* Manually start the health test. • *Configure:* Change how often the test is run by configuring the scheduling settings.

Alert

The Alert tab enables you to search through your existing alerts and set rules on how you receive alerts. You can also configure how you want to receive push notifications through various notification channels such as email, Slack, PagerDuty, WebHook, and more.



Notification channel alerts

You can add new ways of receiving alerts by adding a channel and specifying the channel type.

To create a notification channel with email

The following example shows how to set up the SMTP server and create an email notification channel.

1. Go to *Services* > *Monitor* > *Configuration*.
2. Enable *SMTP*.
3. In the *SMTP Host* field, enter the SMTP server address and SMTP port.
   The format is `<SMTP server address>:<SMTP port number>`. For example, `smtp.gmail.com:587`.
4. In the *SMTP TLS Policy* field, select *TLS policy*.
5. (Optional) Enable *SMTP authentication* if authentication is required.
6. In the *SMTP Auth User* and *SMTP Auth Password* fields, enter the username and password for authentication.
7. Click *Save*.

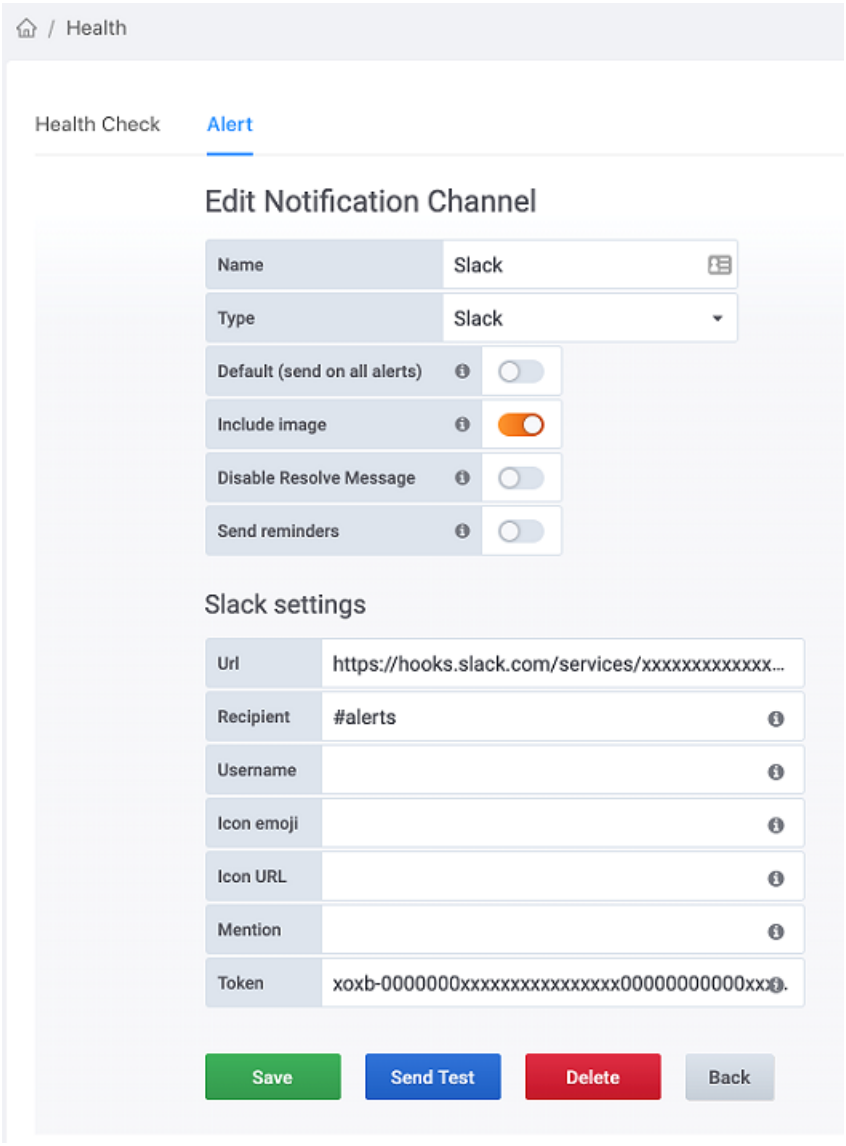
8. Go to the *Instances* tab and click *Apply Config*. The configuration changes take effect and triggers the `Enable Smtp` command.
   Wait for the command to finish running.
9. Go to *Monitor > Health > Alert > Notification channels* and click *New channel*.
10. In the *Name* field, enter a name for the channel.
11. In the *Type* field, select *Email*.
12. In the *Addresses* field, enter the destination email addresses for notifications. Separate multiple email addresses with a semi-colon (;).
13. Click *Test* and check if you can receive the test alert email.
14. Click *Save* once you have verified the email channel alert works.

To create a notification channel with Slack Incoming Webhook

The following example shows how to create a notification channel with Slack Incoming Webhook and set up an alert.

1. Go to *Monitor > Health > Alert > Notification channels* and click *Add channel*.
2. In the Name field, enter a name for the channel.
3. In the Type field, select *Slack*.
4. You can choose how you want to configure your alert.
   In this example, enable the *Include image* toggle so a snapshot of your Slack chart can be sent with the alert.
5. In the URL field, enter your Slack Incoming Webbook URL.
   For instructions on how to create a Slack Incoming Hook, refer to the Slack documentation.
6. In the Token field, enter the in the Slack “Bot User OAuth Access Token” in order to allow the generated image to be uploaded via Slack’s file.upload API method.
7. In Slack, invite the bot to the channel you want to send notifications to and add the Slack channel name to the Recipient field.
8. Click *Send Test* and check if you can see the test message in your Slack channel with the Webhook hooked.

9. Once you have verified that the channel alert works, click *Save*.



Custom alert rules

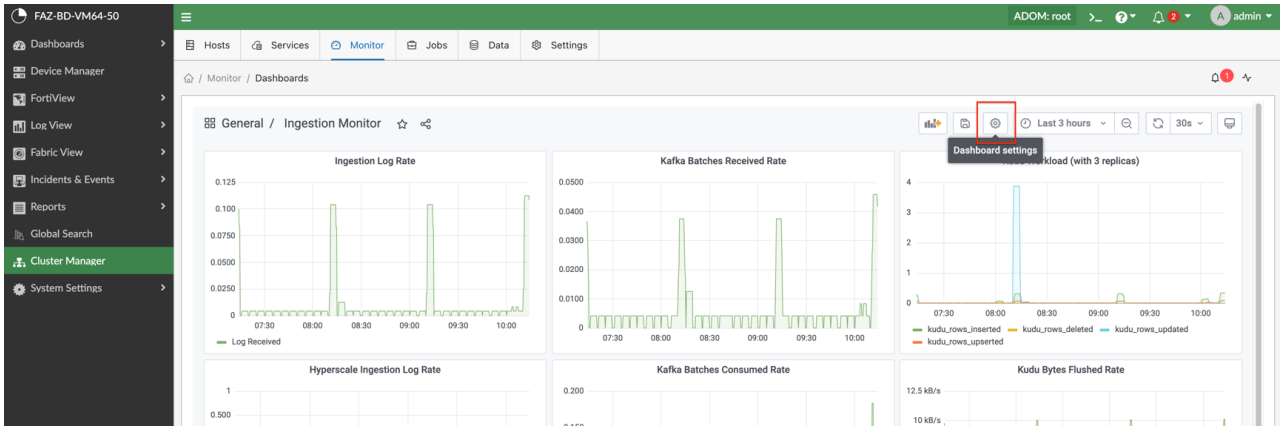
You can create custom alert rules from Dashboard panels and have it sent to a specified notification channel.

To create a custom alert for a notification channel:

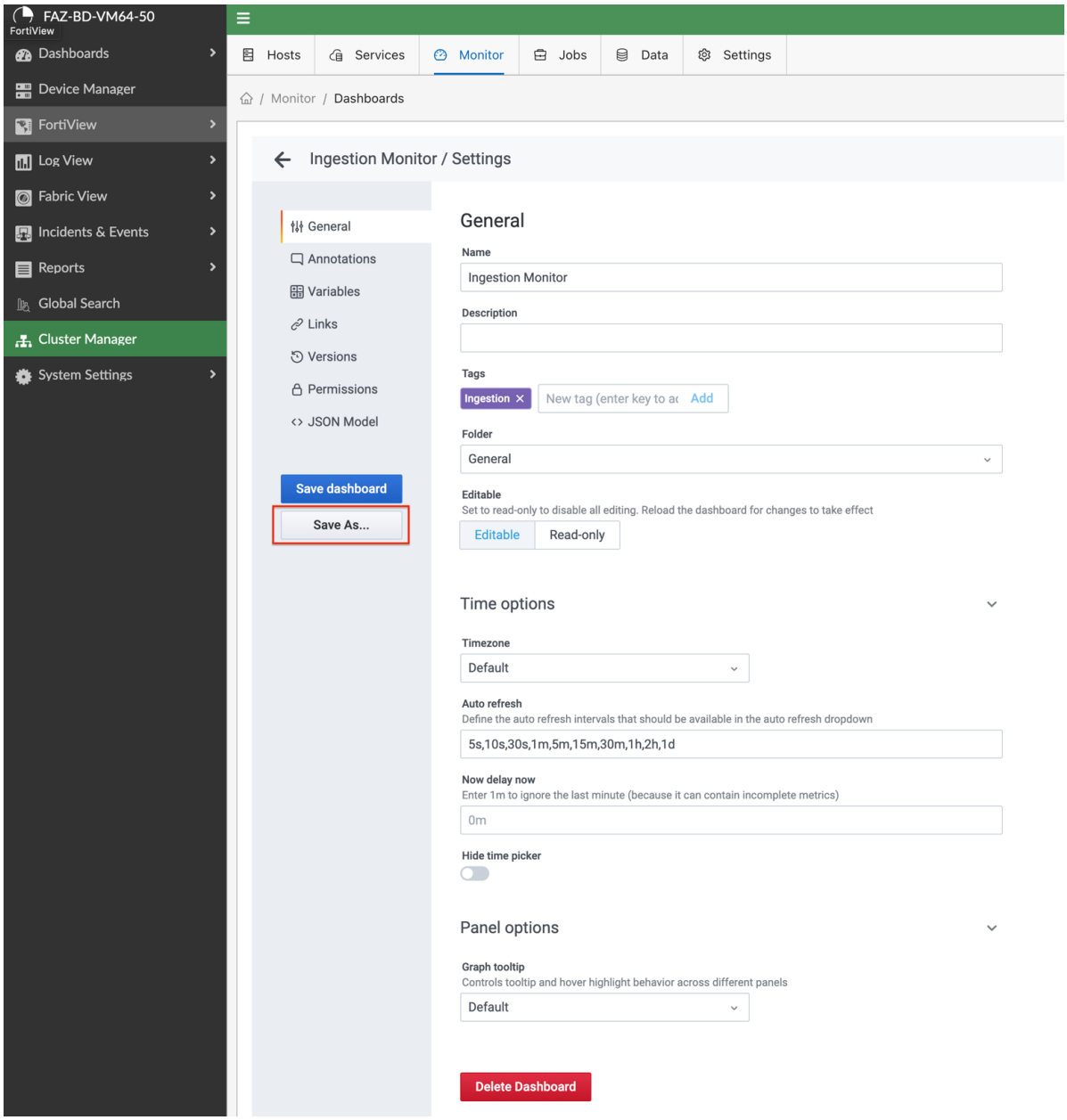
The following example shows how to create custom alert rule that can be sent directly to the example Slack notification channel.

1. Go to *Monitor* > *Dashboards* and select a panel for which you want to create an alert.
2. Click *Dashboard Settings*.

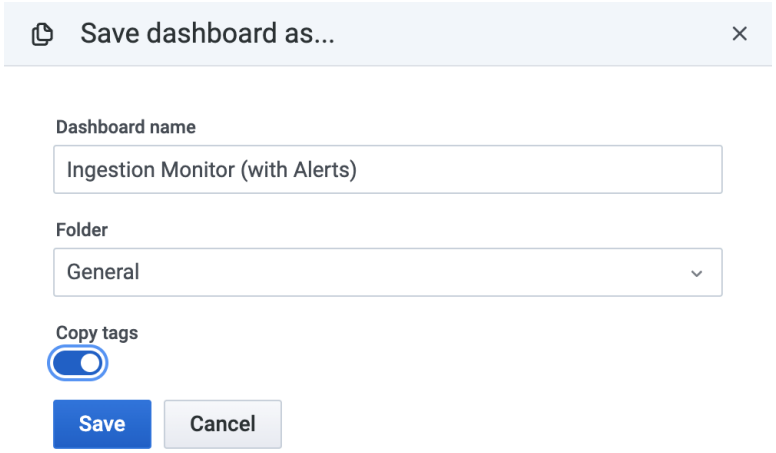
Fortinet recommends creating alerts on custom dashboards. If alerts are set up on the default dashboard, they may be lost when the default dashboard is updated during FortiAnalyzer-BigData firmware upgrades.



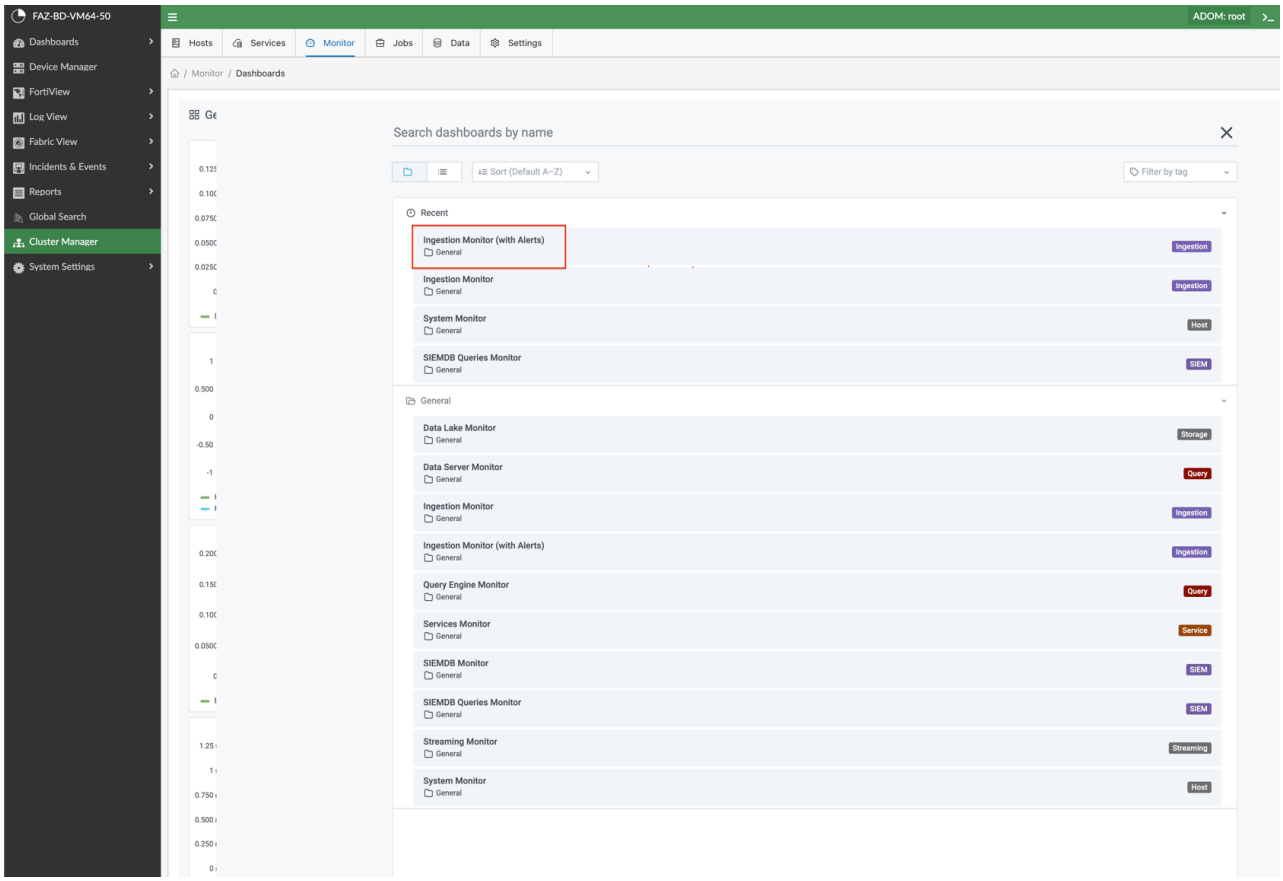
3. Click *Save As*.

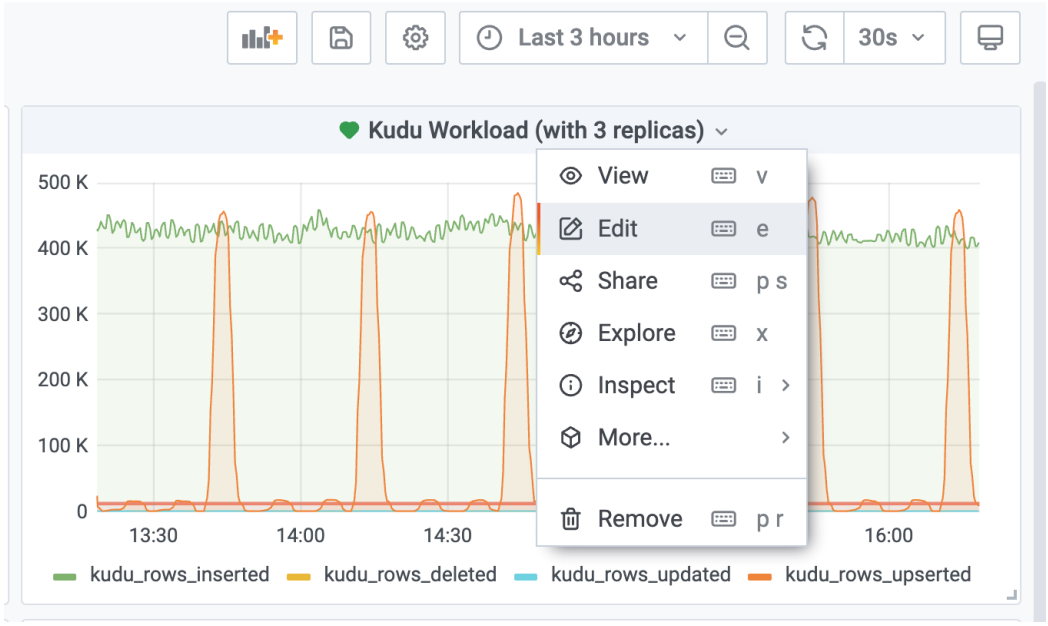


4. Enter a *Dashboard name* and click *Save*.



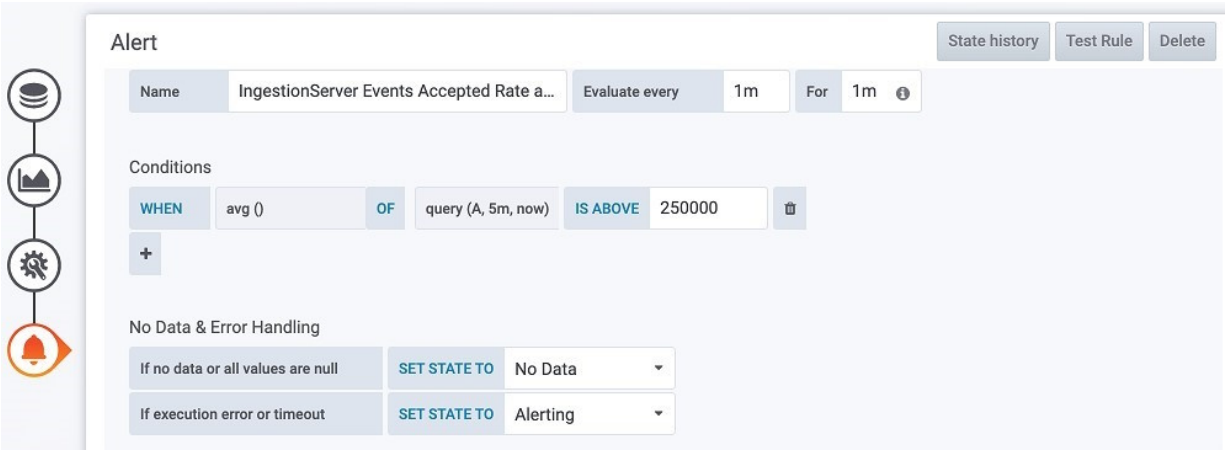
5. Navigate to the created Dashboard, click a panel title, and click *Edit*.



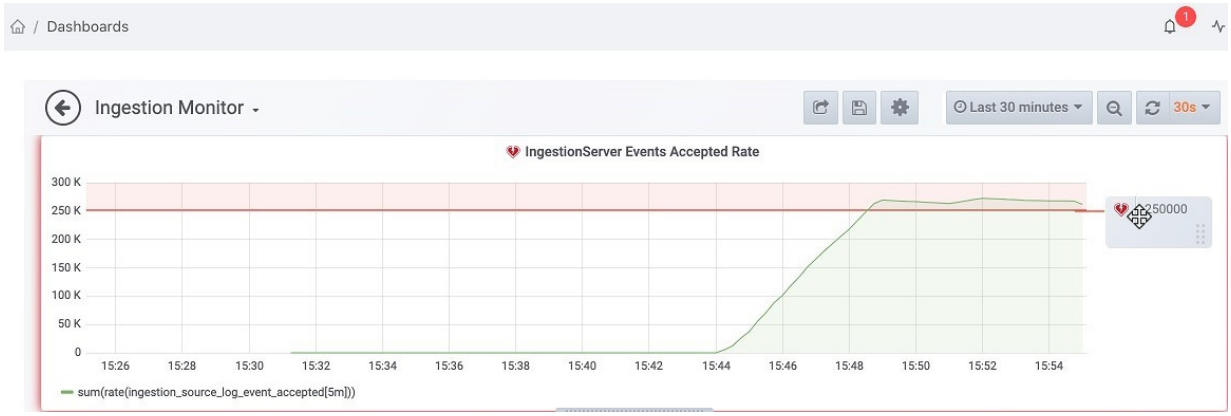


The panel's detailed view displays.

6. Click Alert (bell icon) to access the *Alert* view.
7. Click *Create Alert* to specify conditions that trigger the alert.
8. You can create conditions through two different methods:
   - By making queries in the *Conditions* section.

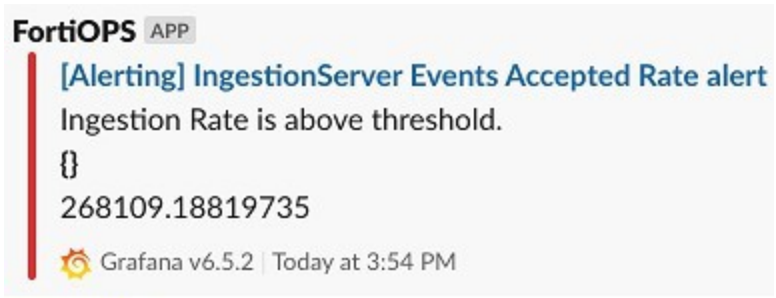


   - By dragging the threshold bar in the graph to indicate an allowable threshold level.



9. After you have defined your condition, select the *Notification Channel* and click *Test Rule* to test the alert rule.
10. Click *Save* to save your settings.

    If your conditions are configured correctly, you should receive an alert with snapshot resembling the following:



Hyperscale firewall logging support

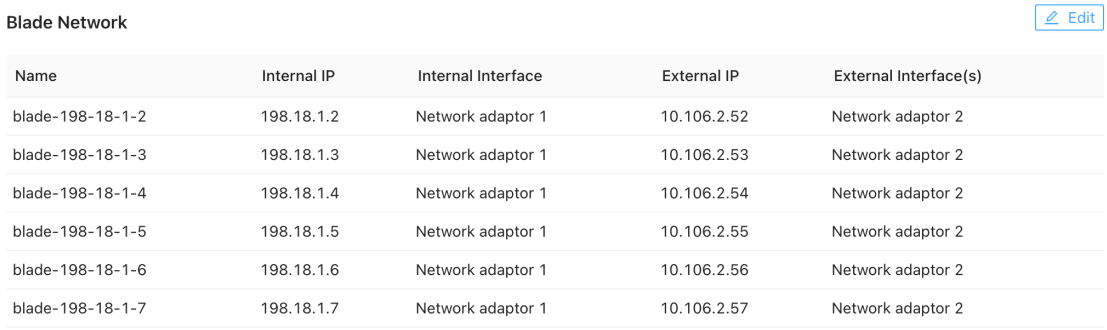
You can configure FortiAnalyzer-BigData as a log server for a Fortinet Hyperscale firewall that supports hardware logging with Hyperscale SPU log offload feature. FortiAnalyzer-BigData can collect, store, and query log messages sent as NetFlow v10, which is compatible with IP Flow Information Export (IPFIX) format, or Syslog over UDP from a Hyperscale firewall. For more information, see Hyperscale Firewall Hardware logging in the Fortinet Doc Library.

Set up Security Manager hosts external IP addresses

When receiving log messages from Hyperscale FortiGate, each Security Manager host of FortiAnalyzer-BigData can be exposed as a distributed log collector to distribute the log traffic load. A set of external IP addresses for the hosts that your FortiGate can reach are required to receive the log message traffic.

To set up external IP addresses for Security Manage hosts:

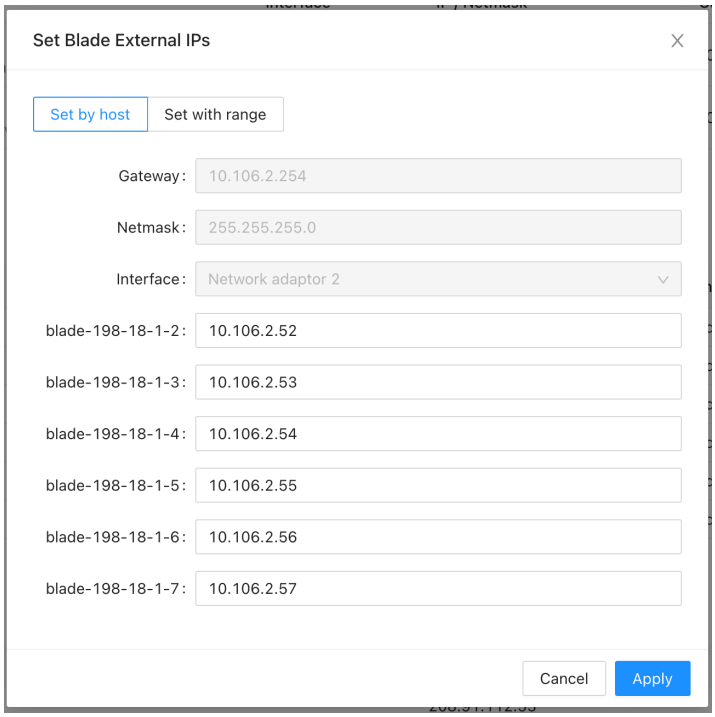
1. Go to *Cluster Manager* > *Settings* > *Network* > *Blade Network* and click *Edit*.



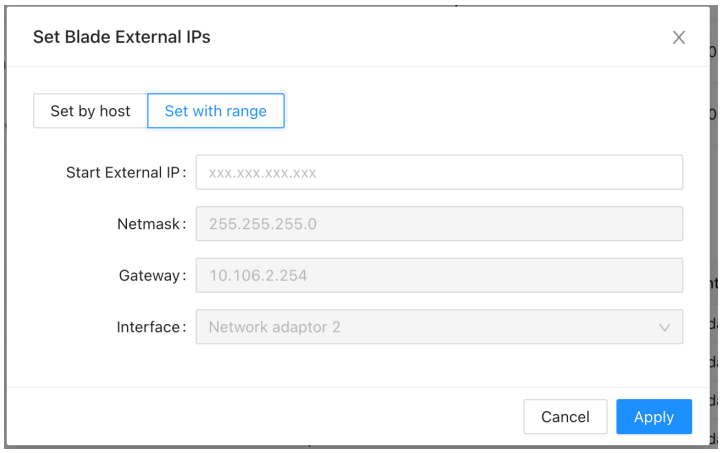
Name	Internal IP	Internal Interface	External IP	External Interface(s)
blade-198-18-1-2	198.18.1.2	Network adaptor 1	10.106.2.52	Network adaptor 2
blade-198-18-1-3	198.18.1.3	Network adaptor 1	10.106.2.53	Network adaptor 2
blade-198-18-1-4	198.18.1.4	Network adaptor 1	10.106.2.54	Network adaptor 2
blade-198-18-1-5	198.18.1.5	Network adaptor 1	10.106.2.55	Network adaptor 2
blade-198-18-1-6	198.18.1.6	Network adaptor 1	10.106.2.56	Network adaptor 2
blade-198-18-1-7	198.18.1.7	Network adaptor 1	10.106.2.57	Network adaptor 2

2. Set the *Default Gateway* and *Netmask* to your internal network.

3. Enter an IP address for each host.



4. If you have a range of continuous IP addresses, you can click *Set with range* and specify a *Start External IP* to automatically increment and set the IP addresses to all hosts.

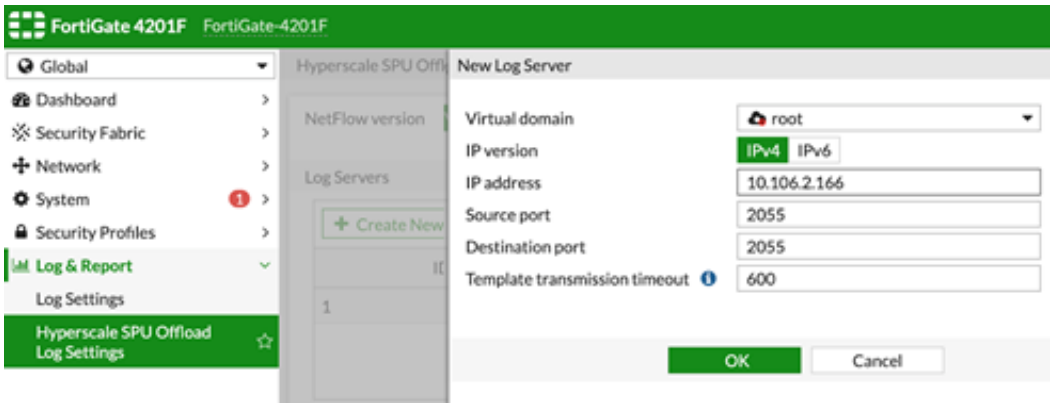


Configure FortiAnalyzer-BigData as log server on hyperscale FortiGate

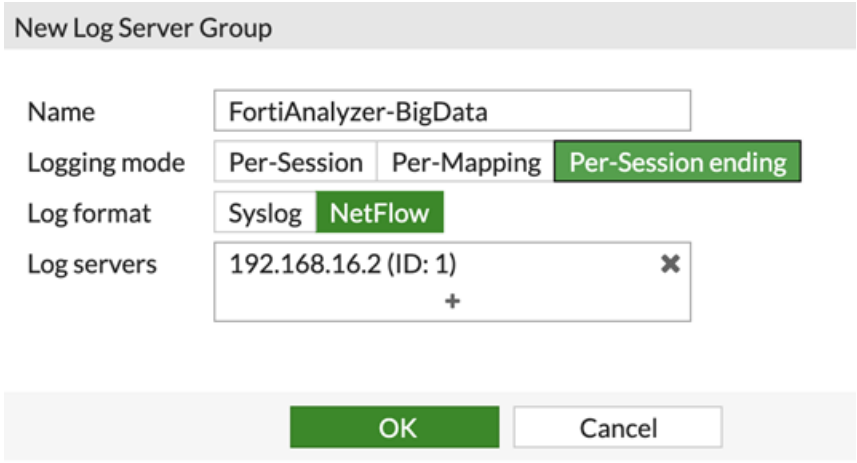
After external IP addresses for Security Manager hosts are set, you can configure a FortiGate with Hyperscale firewall features to send NetFlow v10 (IPFIX) or Syslog log messages over UDP to FortiAnalyzer-BigData. For more information, see Hyperscale Firewall Hardware logging in the Fortinet Doc Library.

To configure FortiAnalyzer-BigData as NetFlow log server on Hyberscale FortiGate:

1. Go to *Log & Report* > *Hyperscale SPU Offload Log Settings*.
2. Select *NetFlow version V10*.
3. In *Log Servers*, click *Create New* to add each external IP address of FortiAnalyzer-BigData Security Manager Host.
4. In the *Source port* and *Destination port*, enter 2055.



5. In *Log Servers Groups*, click *Create New* to create a log group.
6. For *Logging mode*, select *Per-Session ending*.
7. For *Log format*, select *NetFlow*.
8. For *Log servers*, add all the log servers created in the previous step.
9. Click *OK*.
   The FortiGate is configured to send NetFlow log messages to FortiAnalyzer-BigData.



To configure FortiAnalyzer-BigData as Syslog log server on a hyperscale FortiGate:

1. Go to *Log & Report* > *Hyperscale SPU Offload Log Settings*.
2. In *Log Servers*, click *Create New* to add each external IP address of FortiAnalyzer-BigData Security Manager Host.
3. In the *Source* port and *Destination* port, enter 514.
4. In *Log Servers Groups*, click *Create New* to create a log group.
5. Set *Logging mode* to *Per-Session ending*.

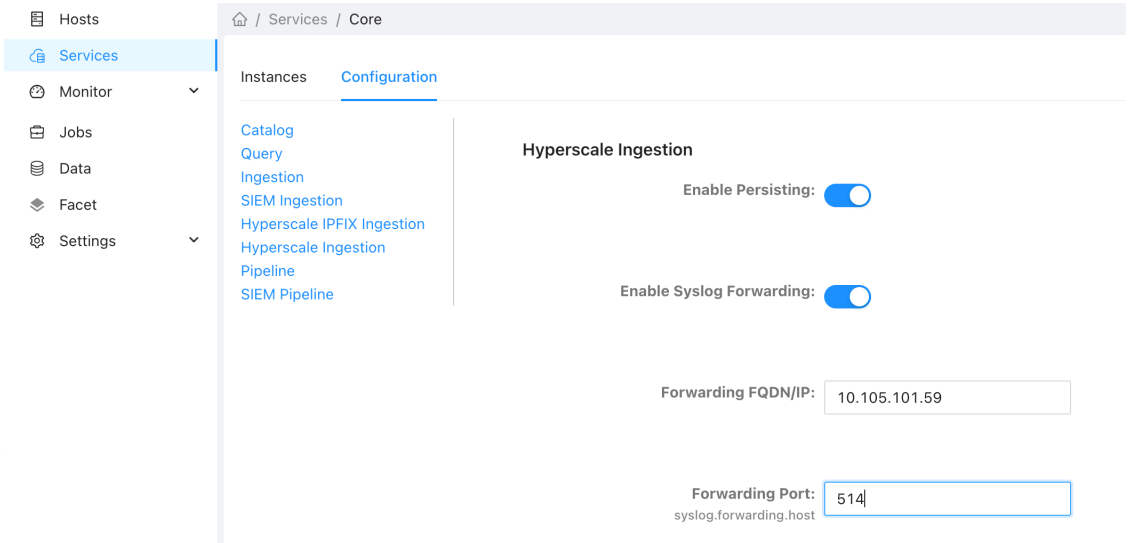
6. *Set Log format* to *Syslog*.
7. For *Log servers*, add all the log servers created in the previous step.
8. Click *OK*. The FortiGate is configured to send Syslog log messages to FortiAnalyzer-BigData.

Configure FortiAnalyzer-BigData Hyperscale Ingestion

By default, the Hyperscale ingestion is disabled in the Security Event Manager. You can also configure FortiAnalyzer-BigData to forward Hyperscale Syslog messages to an external Syslog UDP server:

To configure Hyperscale Ingestion:

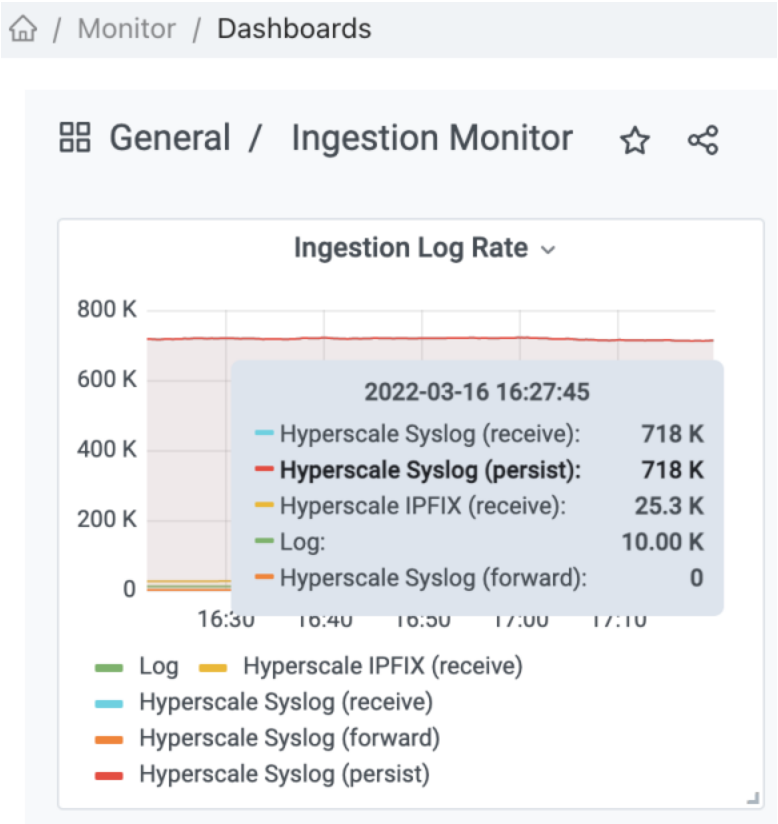
1. Go to *Cluster Manager* > *Services* > *Core*.
2. Click the *Configuration* tab and go to the *Hyperscale Ingestion* section.
3. Toggle *Enable Persisting* to enable or disable persisting the logs into the Security Event Manager. This is disabled by default.
4. Toggle *Enable Syslog Forwarding* to enable or disable forwarding to an external Syslog UDP server. This is disabled by default.
5. When *Enable Syslog Forwarding* is on, configure the destination Syslog UDP server's IP and port.
6. Click *Save* and follow the prompts to apply the configuration.



Device Manager and log rate

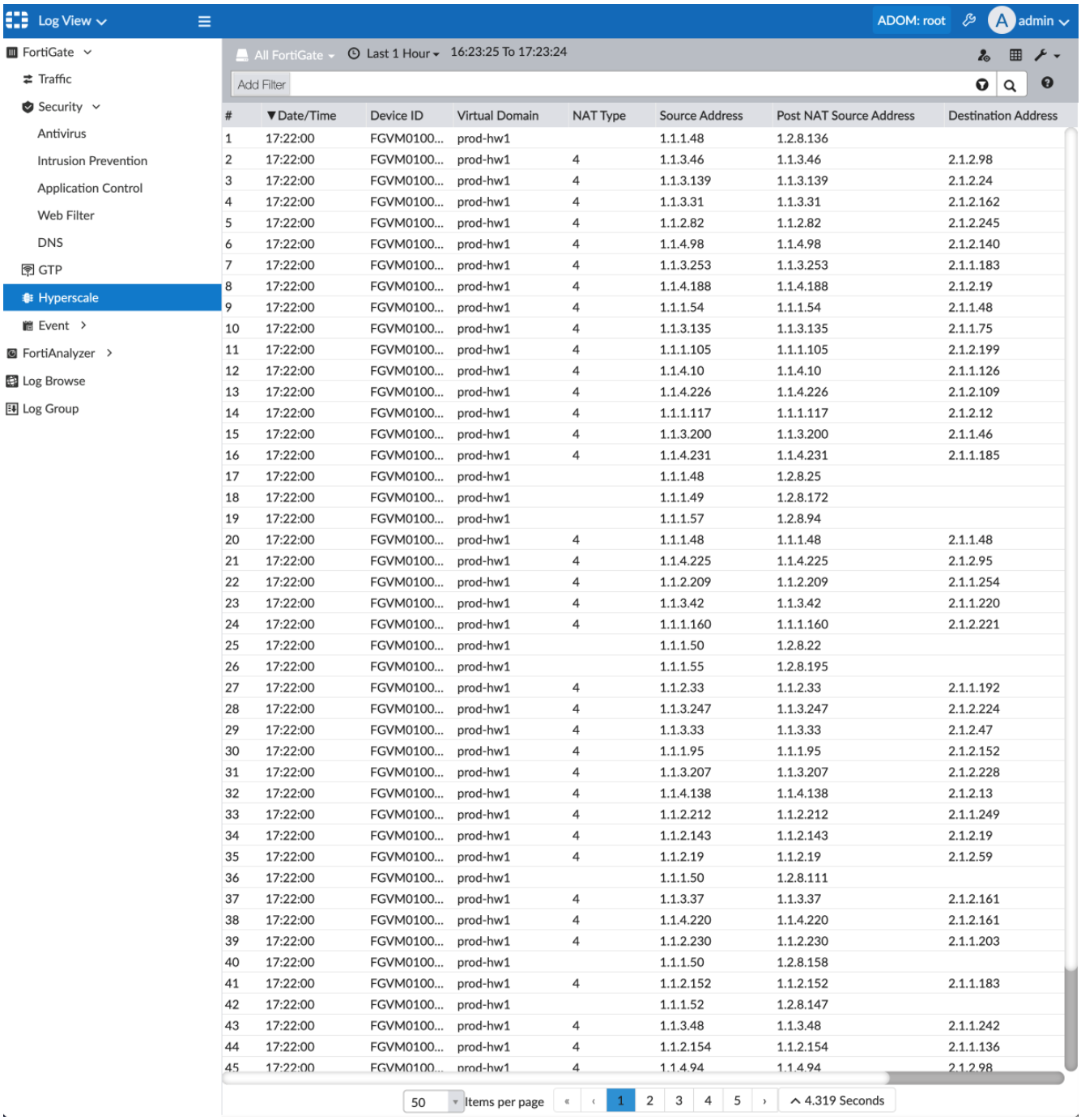
When FortiAnalyzer-BigData starts to receive hyperscale log messages, the device appears in Device Manager along with information such as log status, VDOM, log rate, and so on. Click the number to display a graph of historical average log rates of the device.

To view the overall log rate of normal logs and hyperscale logs in different log format, go to *Cluster Manager > Monitor > Dashboards* to view the *Ingestion Log Accepted Rate*.



Search Hyperscale log in Log View

If you have Hyperscale logs collected, you can go to *FortiGate > Hyperscale* to view the logs in *Log View*. You can apply filters, click to view log details, and use other features as you search other logs.



#	Date/Time	Device ID	Virtual Domain	NAT Type	Source Address	Post NAT Source Address	Destination Address
1	17:22:00	FGVM0100...	prod-hw1		1.1.1.48	1.2.8.136	
2	17:22:00	FGVM0100...	prod-hw1	4	1.1.3.46	1.1.3.46	2.1.2.98
3	17:22:00	FGVM0100...	prod-hw1	4	1.1.3.139	1.1.3.139	2.1.2.24
4	17:22:00	FGVM0100...	prod-hw1	4	1.1.3.31	1.1.3.31	2.1.2.162
5	17:22:00	FGVM0100...	prod-hw1	4	1.1.2.82	1.1.2.82	2.1.2.245
6	17:22:00	FGVM0100...	prod-hw1	4	1.1.4.98	1.1.4.98	2.1.2.140
7	17:22:00	FGVM0100...	prod-hw1	4	1.1.3.253	1.1.3.253	2.1.1.183
8	17:22:00	FGVM0100...	prod-hw1	4	1.1.4.188	1.1.4.188	2.1.2.19
9	17:22:00	FGVM0100...	prod-hw1	4	1.1.1.54	1.1.1.54	2.1.1.48
10	17:22:00	FGVM0100...	prod-hw1	4	1.1.3.135	1.1.3.135	2.1.1.75
11	17:22:00	FGVM0100...	prod-hw1	4	1.1.1.105	1.1.1.105	2.1.2.199
12	17:22:00	FGVM0100...	prod-hw1	4	1.1.4.10	1.1.4.10	2.1.1.126
13	17:22:00	FGVM0100...	prod-hw1	4	1.1.4.226	1.1.4.226	2.1.2.109
14	17:22:00	FGVM0100...	prod-hw1	4	1.1.1.117	1.1.1.117	2.1.2.12
15	17:22:00	FGVM0100...	prod-hw1	4	1.1.3.200	1.1.3.200	2.1.1.46
16	17:22:00	FGVM0100...	prod-hw1	4	1.1.4.231	1.1.4.231	2.1.1.185
17	17:22:00	FGVM0100...	prod-hw1		1.1.1.48	1.2.8.25	
18	17:22:00	FGVM0100...	prod-hw1		1.1.1.49	1.2.8.172	
19	17:22:00	FGVM0100...	prod-hw1		1.1.1.57	1.2.8.94	
20	17:22:00	FGVM0100...	prod-hw1	4	1.1.1.48	1.1.1.48	2.1.1.48
21	17:22:00	FGVM0100...	prod-hw1	4	1.1.4.225	1.1.4.225	2.1.2.95
22	17:22:00	FGVM0100...	prod-hw1	4	1.1.2.209	1.1.2.209	2.1.1.254
23	17:22:00	FGVM0100...	prod-hw1	4	1.1.3.42	1.1.3.42	2.1.1.220
24	17:22:00	FGVM0100...	prod-hw1	4	1.1.1.160	1.1.1.160	2.1.2.221
25	17:22:00	FGVM0100...	prod-hw1		1.1.1.50	1.2.8.22	
26	17:22:00	FGVM0100...	prod-hw1		1.1.1.55	1.2.8.195	
27	17:22:00	FGVM0100...	prod-hw1	4	1.1.2.33	1.1.2.33	2.1.1.192
28	17:22:00	FGVM0100...	prod-hw1	4	1.1.3.247	1.1.3.247	2.1.2.224
29	17:22:00	FGVM0100...	prod-hw1	4	1.1.3.33	1.1.3.33	2.1.2.47
30	17:22:00	FGVM0100...	prod-hw1	4	1.1.1.95	1.1.1.95	2.1.2.152
31	17:22:00	FGVM0100...	prod-hw1	4	1.1.3.207	1.1.3.207	2.1.2.228
32	17:22:00	FGVM0100...	prod-hw1	4	1.1.4.138	1.1.4.138	2.1.2.13
33	17:22:00	FGVM0100...	prod-hw1	4	1.1.2.212	1.1.2.212	2.1.1.249
34	17:22:00	FGVM0100...	prod-hw1	4	1.1.2.143	1.1.2.143	2.1.2.19
35	17:22:00	FGVM0100...	prod-hw1	4	1.1.2.19	1.1.2.19	2.1.2.59
36	17:22:00	FGVM0100...	prod-hw1		1.1.1.50	1.2.8.111	
37	17:22:00	FGVM0100...	prod-hw1	4	1.1.3.37	1.1.3.37	2.1.2.161
38	17:22:00	FGVM0100...	prod-hw1	4	1.1.4.220	1.1.4.220	2.1.2.161
39	17:22:00	FGVM0100...	prod-hw1	4	1.1.2.230	1.1.2.230	2.1.1.203
40	17:22:00	FGVM0100...	prod-hw1		1.1.1.50	1.2.8.158	
41	17:22:00	FGVM0100...	prod-hw1	4	1.1.2.152	1.1.2.152	2.1.1.183
42	17:22:00	FGVM0100...	prod-hw1		1.1.1.52	1.2.8.147	
43	17:22:00	FGVM0100...	prod-hw1	4	1.1.3.48	1.1.3.48	2.1.1.242
44	17:22:00	FGVM0100...	prod-hw1	4	1.1.2.154	1.1.2.154	2.1.1.136
45	17:22:00	FGVM0100...	prod-hw1	4	1.1.4.94	1.1.4.94	2.1.2.98

Global search

Global Search lets you explore log messages collected by FortiAnalyzer-BigData across all ADOMs. When searching with a Federation, you can search across multiple clusters.

Use *Global Search* to identify trends in the data with the *Histogram* and detailed log messages at the same time. You can quickly explore log messages by selecting the type and labels and pivoting directly from the fields in the log details with just a few clicks. Perform advanced queries with rich *LogQL* (log query language). Cross-cluster search federation allows you to run searches against one or more remote FortiAnalyzer-BigData clusters and compare the results in a single view.

This section contains the following topics:

Starting a global search

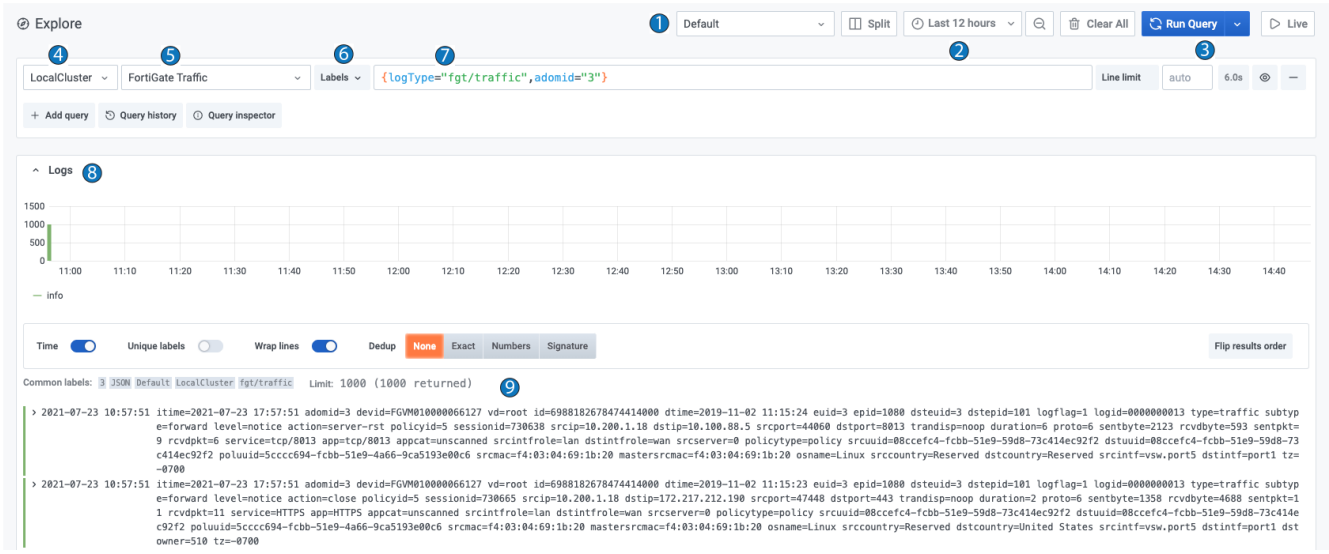
To perform a simple global search, use the default values for the search federation, cluster and log time, then select a log type.

To perform a simple search:

1. Select a search federation. *Default*" is the default.
2. Select a cluster. *LocalCluster* is the default.
3. Select the log time. *Last 1 hour* is the default.
4. Select the log type. For example, *FortiGate Traffic*.
5. (Optional) Select the log labels filter.
6. Click *Run Query* to start a search.

Global Search settings

The following image and the corresponding to table provide information about each of the Global Search settings.



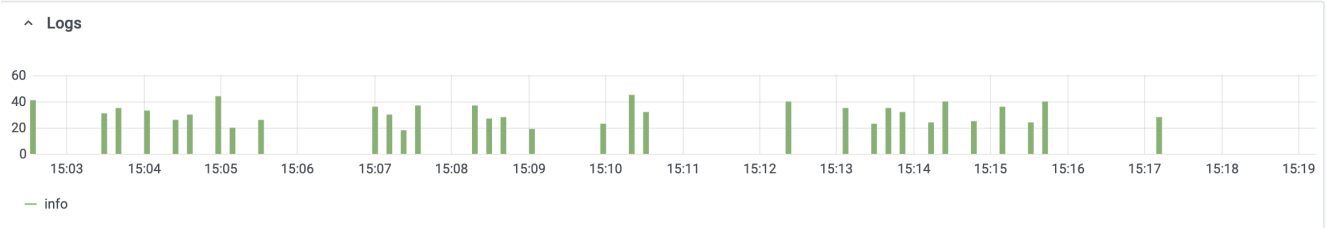
Search setting		Description
1	**Search Federation dropdown**	Click the dropdown menu to select a federation. The default is *Default*.
2	**Time Range selection**	Click the dropdown menu to select a time range. The default is *Last 1 hour*.
3	**Run Query**	Click *Run Query* to start the search.
4	**Server**	Click the dropdown to select a server. The default is *Local Cluster*.
5	**Log Type**	Click the dropdown to select a log type.
6	**Log Label**	Click the dropdown to select a log label.
7	**Log Query Input**	Use this field to enter the log query.
8	**Histogram**	Displays the log time-range.
9	**Log details**	Displays the log details.

Log types (Global Search)

Global search includes a wide array of log types to help you ananlyize your log data and identify trends. Use the log type tools to narrow your search, isolate data, or compare two log searches at the same time.

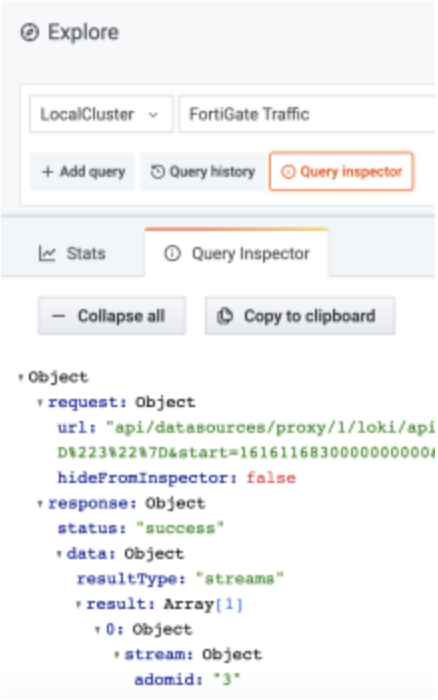
Histogram

The log *Histogram* displays the number of logs collected within the time range selected in the *Global Search* settings. You can use your mouse to select a custom time range and zoom in on the log display



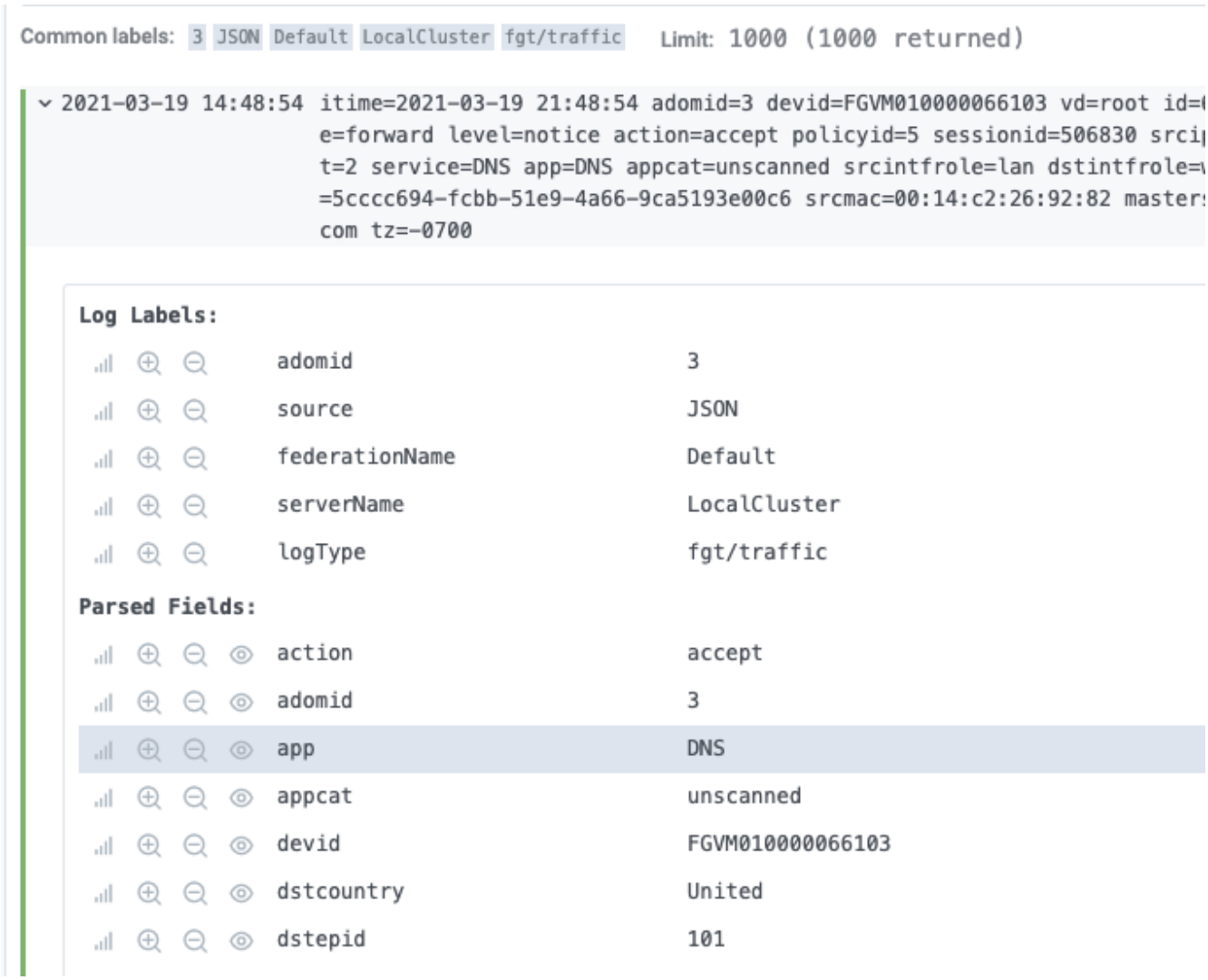
Event Inspector

Click the *Query inspector* button to open the *Query Inspector* panel, and then run the query. The Query Inspector panel shows the plain log search result object. The *Stats* tab shows the query information such as processing time, request time, etc.



Faceted Search (+, -, focus)

Click a log line to view the *Log Details* panel to display the *Log Labels* and *Parsed Fields*.

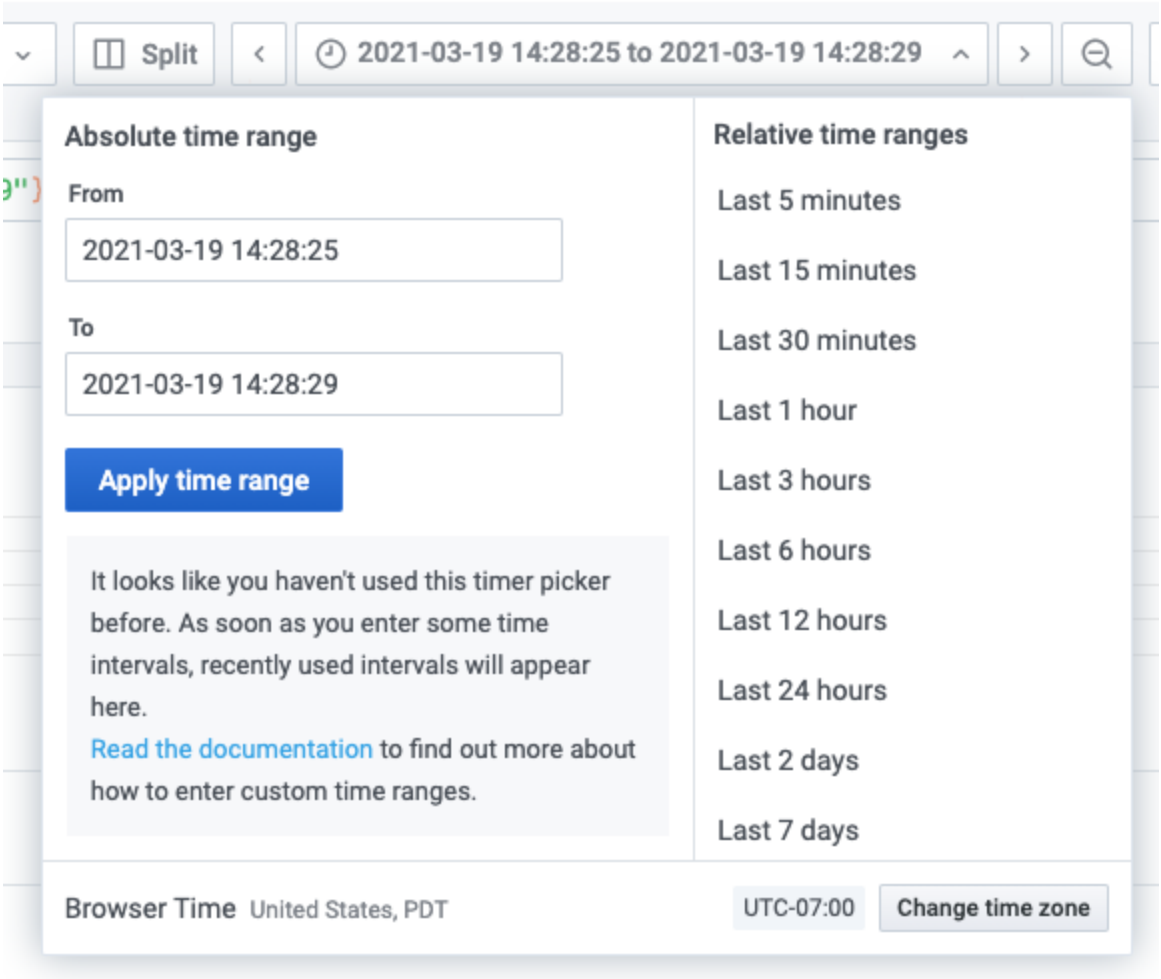


The following table describes the function of each icon in the Faceted Search:

Icon	Description
	Shows the value statistics of the label or fields.
	Adds the label or field as a condition in query language. For example, `app=DNS`.
	Excludes the label or field in the query language. Fore example, `app!=DNS`.
	Displays only this label or field in the log item. For example, `app=DNS`.

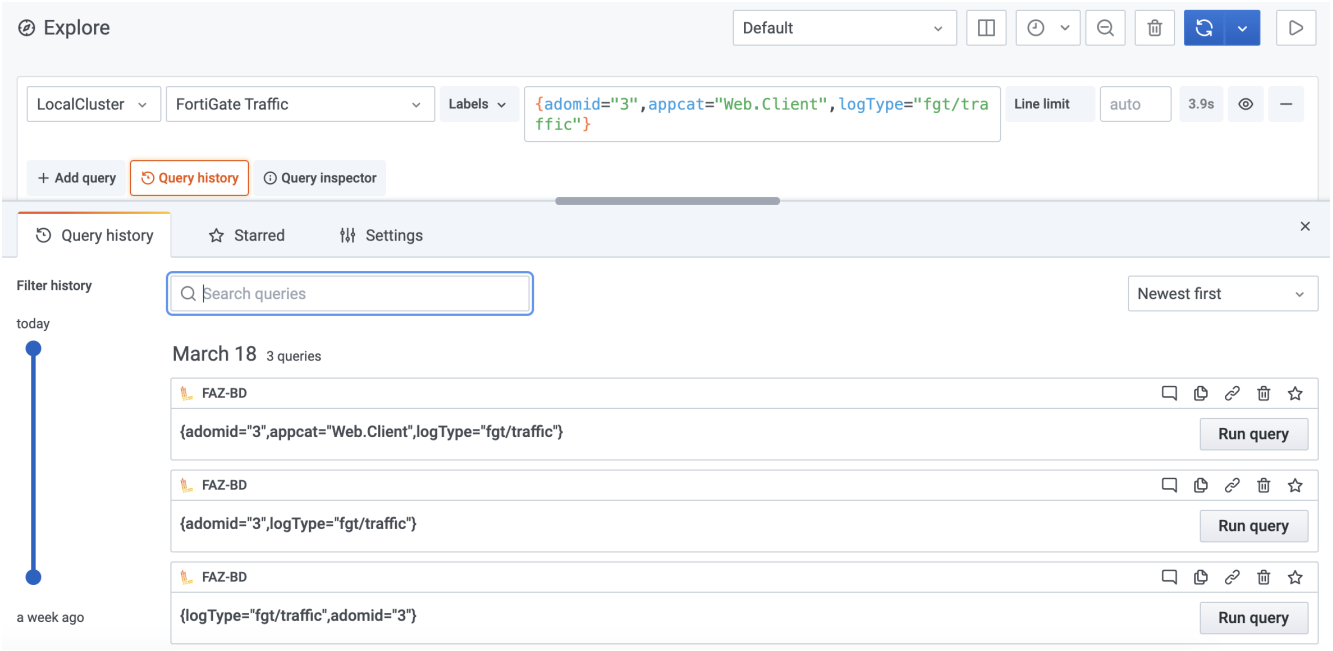
Time Window

Ue the time window to select a time range for your log search. Relative time ranges are provided (*Last 5 minutes* to *Last 7 days*). You can also use the *From* and *To* fields to specify a custom time range. Click the *Back* and *Forward* buttons to move back and forth in the Time Window.



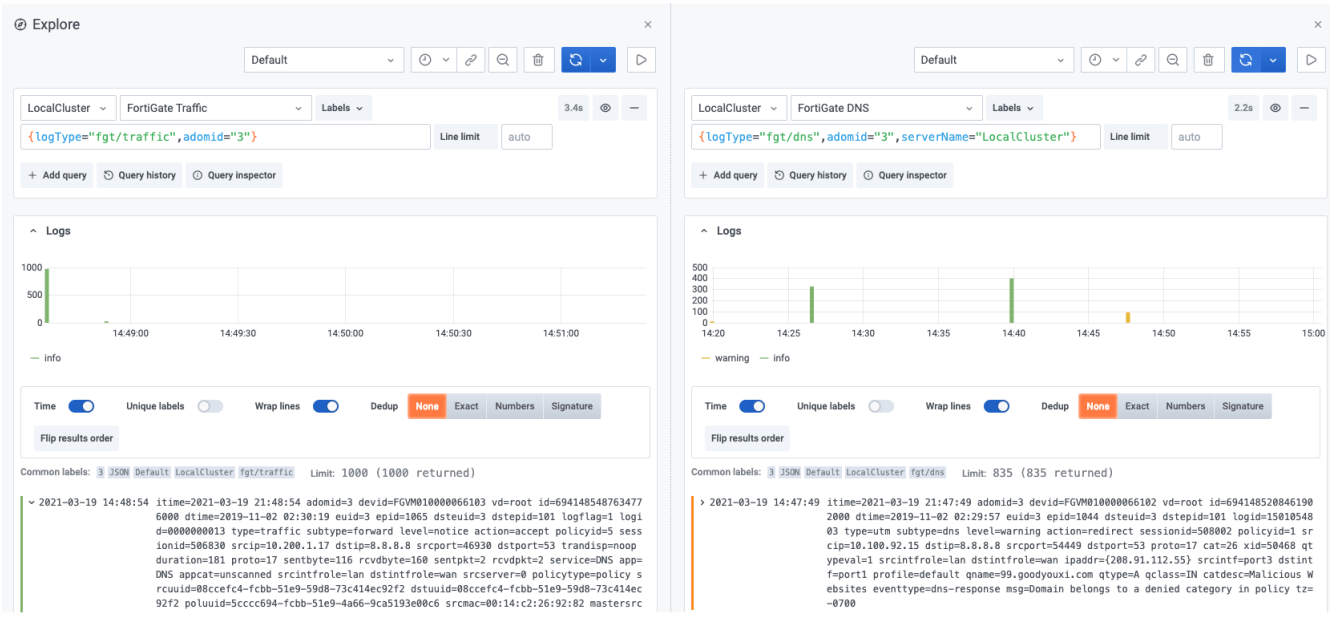
Search History

Click *Query history* to show the log search history. After the query is run, you have the option to comment, favorite, clone, or delete the query.



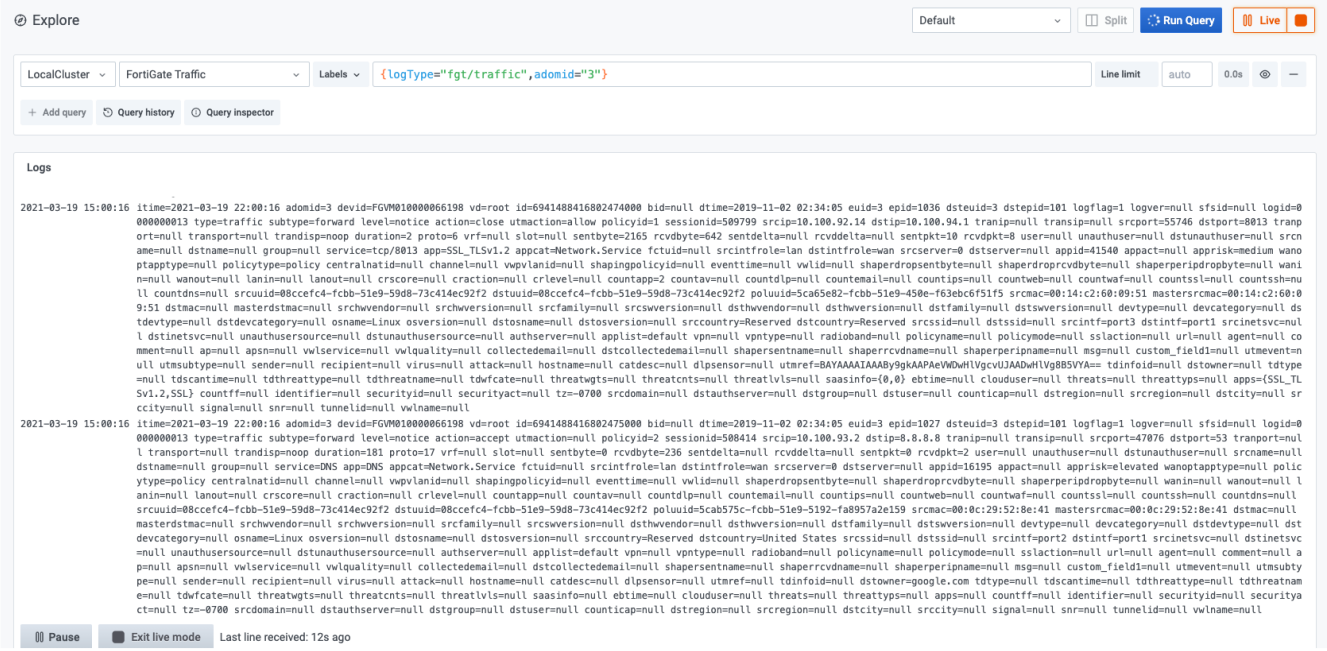
Split View

Click the *Split* button to enable *Split View* mode. Split View displays two log search panes so you can search different content and view the results at the same time.



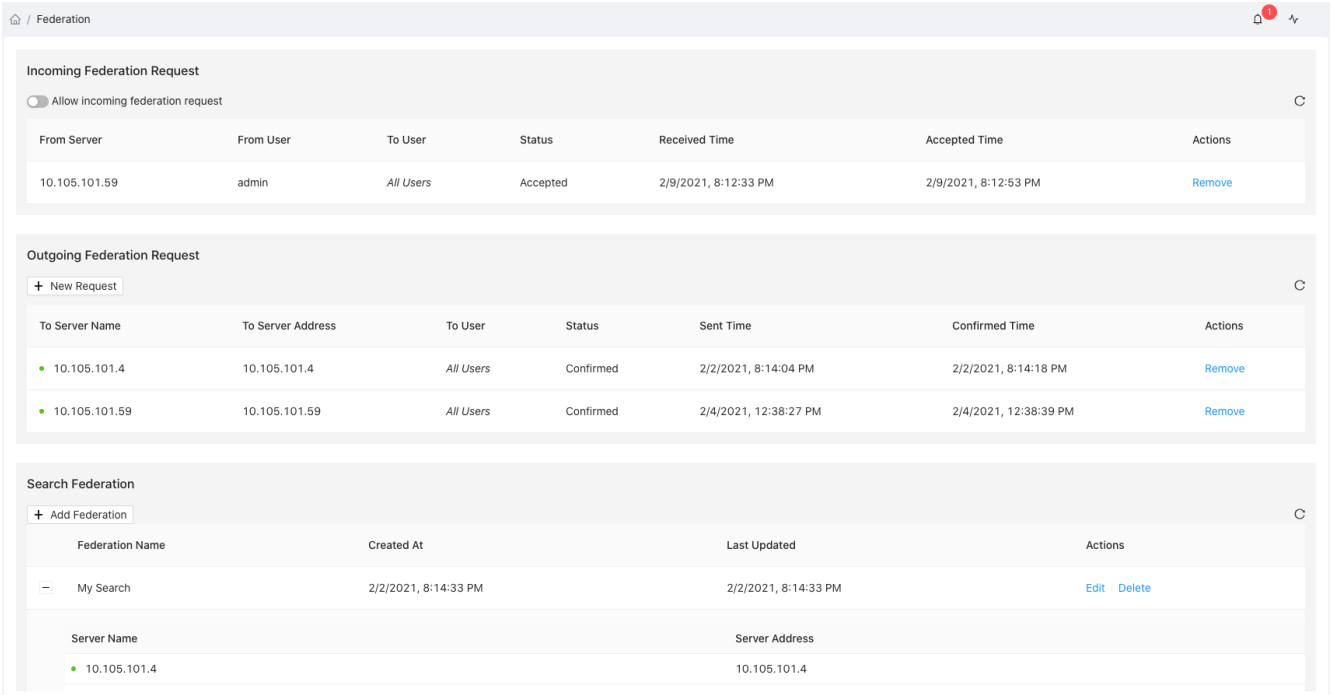
Live Streaming Search

Click the *Live* button at the top-right corner of your search to enable *Live Log* search. Live Log search displays search results in real-time. Click *Pause* to pause the real-time results, or click *Exit live mode* to return to normal mode.



Cross-Cluster Search Federation

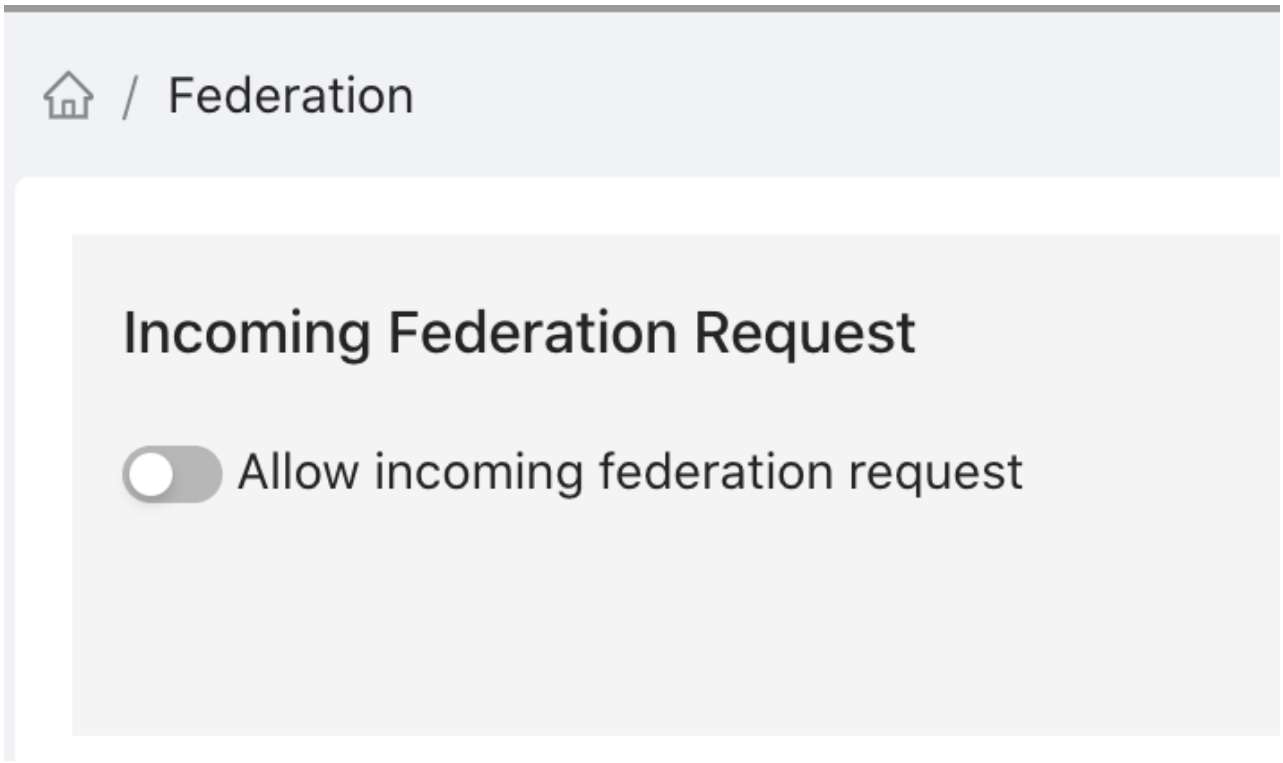
Cross-Cluster search allows you to run searches against one or more remote FortiAnalyzer-BigData clusters. To perform a cross-cluster search, you must have a Search Federation configured. Click the *Federation* menu to open the Federation management UI.



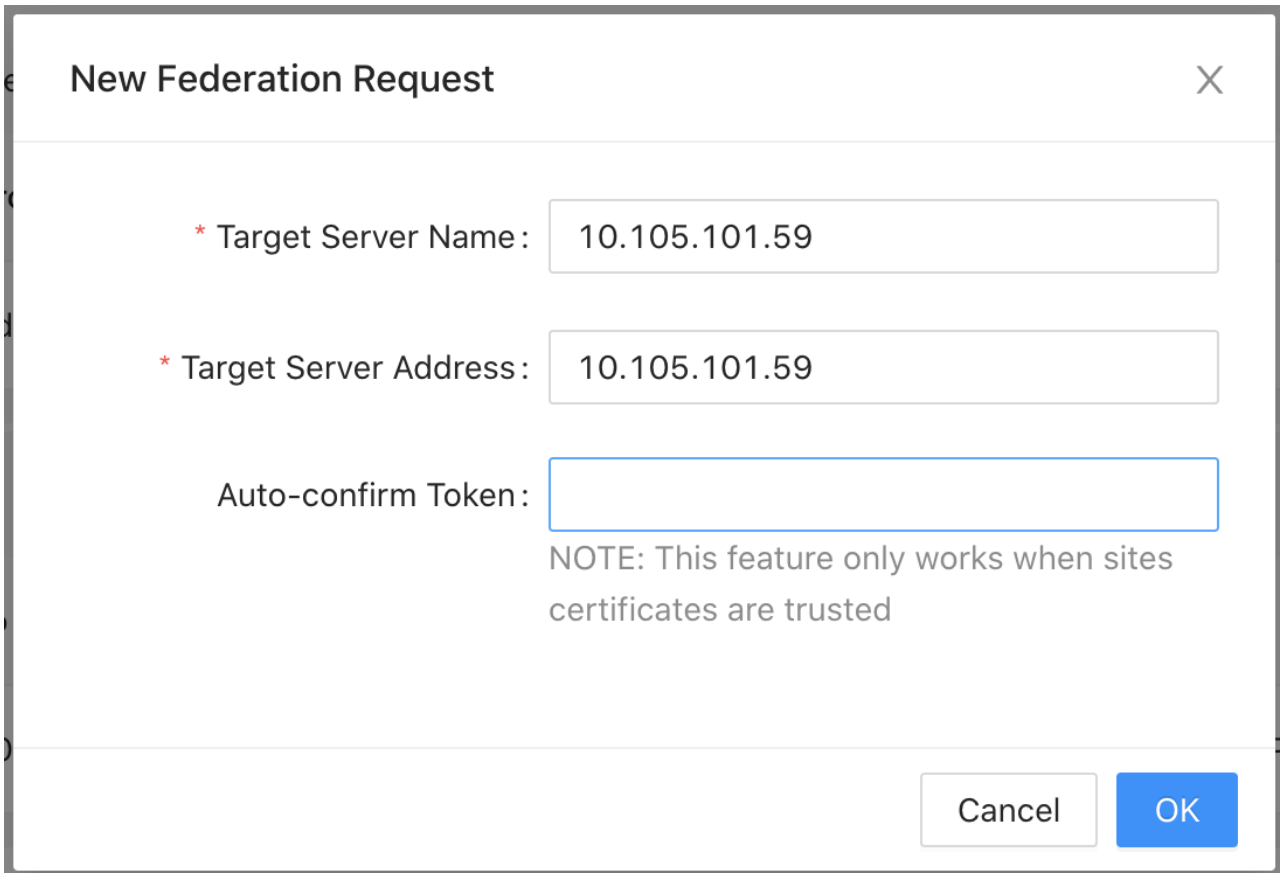
Create a new Search Federation (Example)

In the following example, a user on a local cluster (10.106.2.166) wants to create a *Search Federation* using a remote cluster (10.105.101.59).

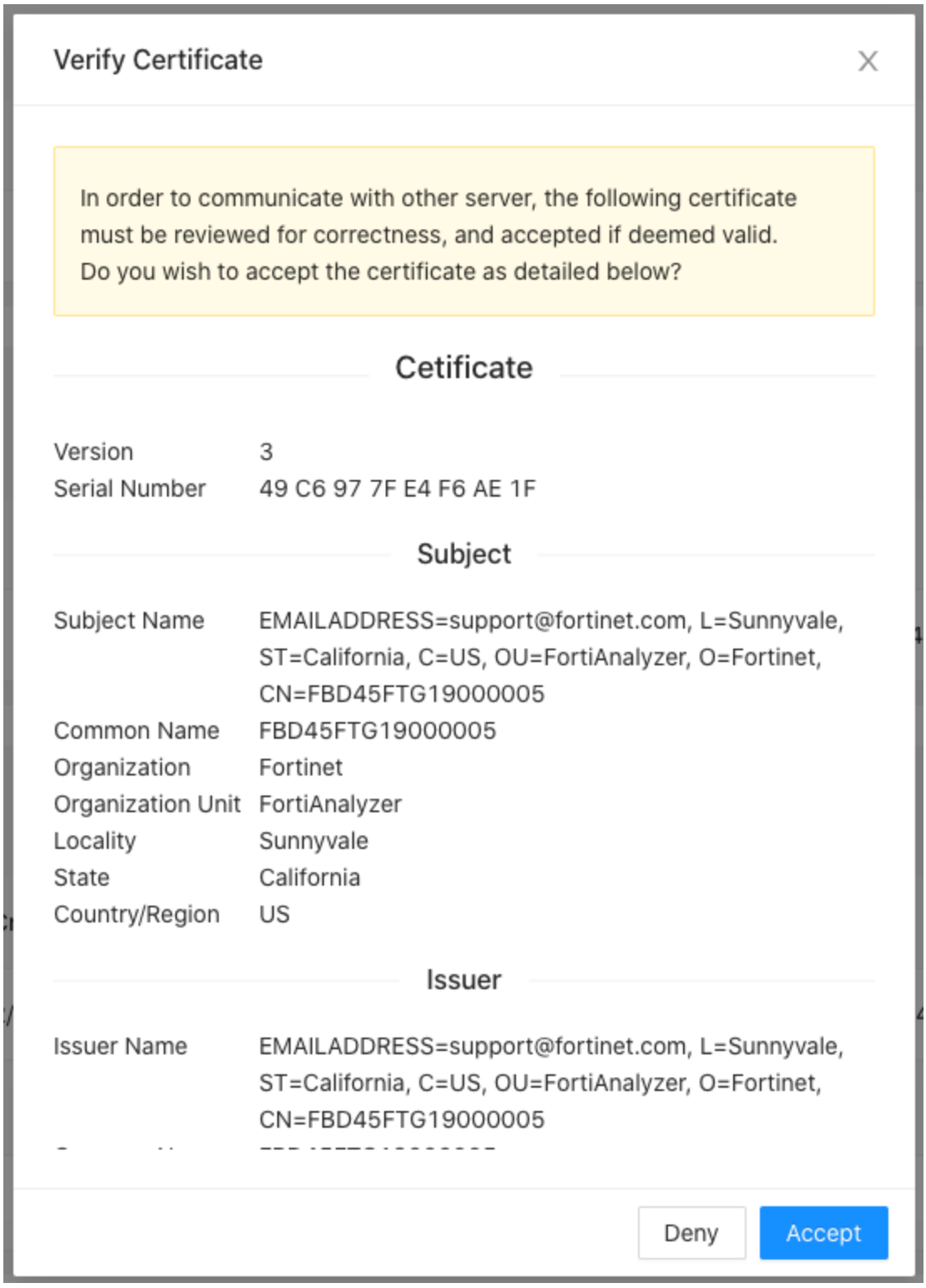
1. On the remote cluster (10.105.101.59), click the *Allow incoming federation request* button to allow the incoming federation request.



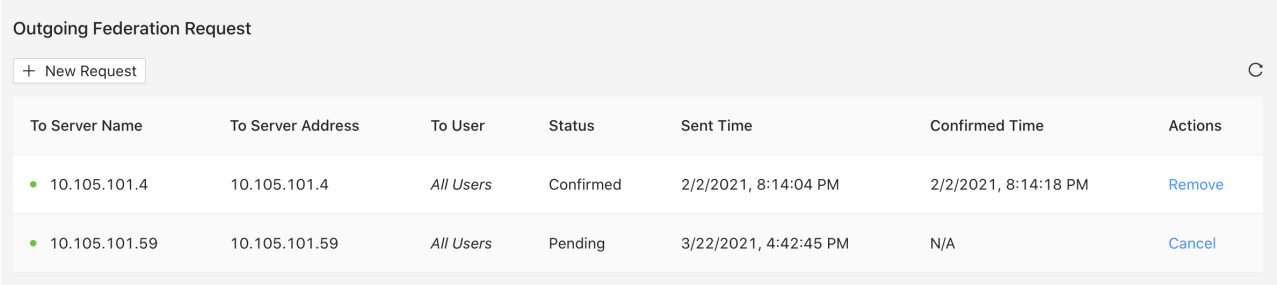
2. On the local cluster (10.106.2.166), click the *New Request* button under *Outgoing Federation Request* section and configure the request.



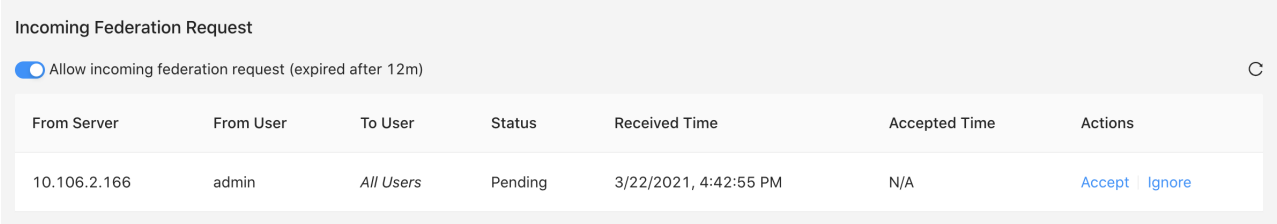
If the remote cluster is using a self-signed certificate, you may see the following dialog for certificate verification. Click *Accept* to send the request.



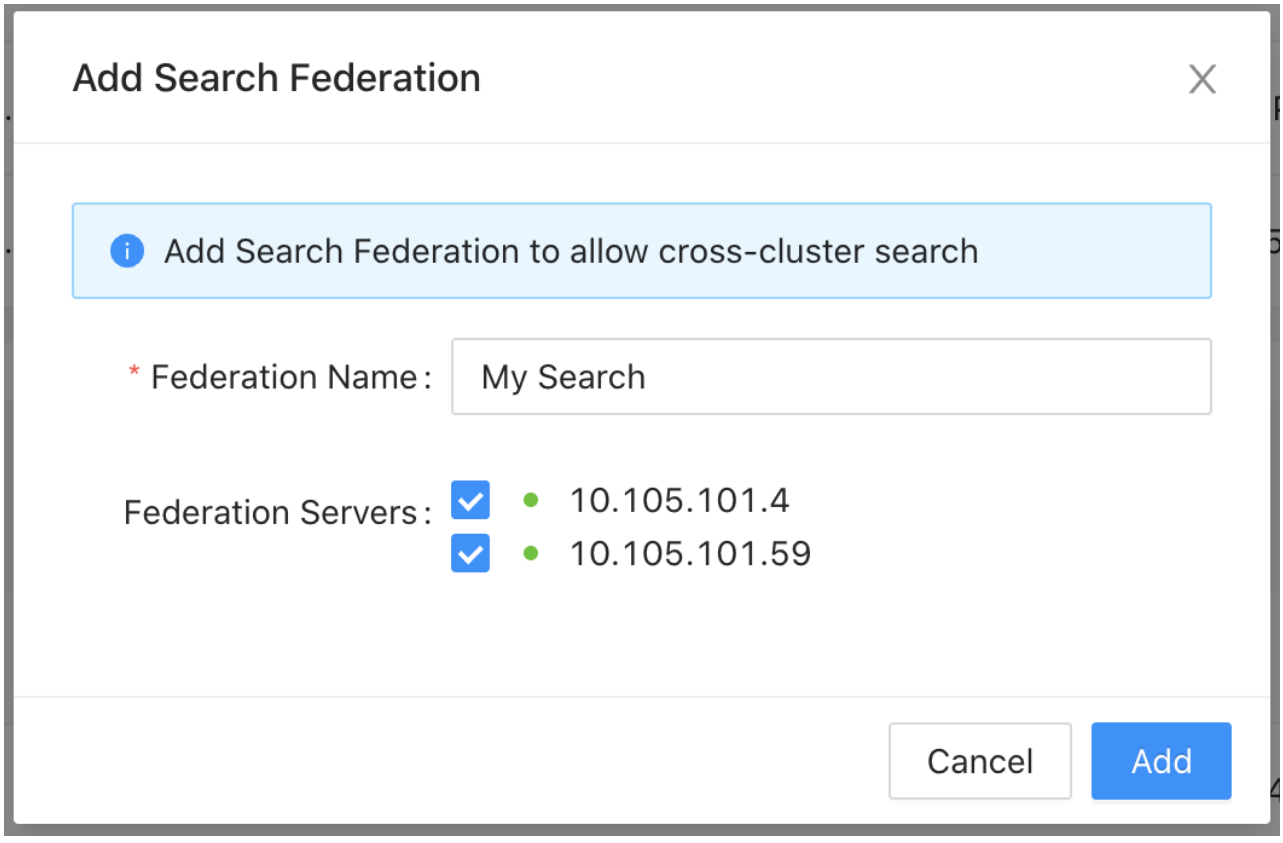
After the request is sent, the you will see a *Pending* item created in the table. You can cancel this item any time.

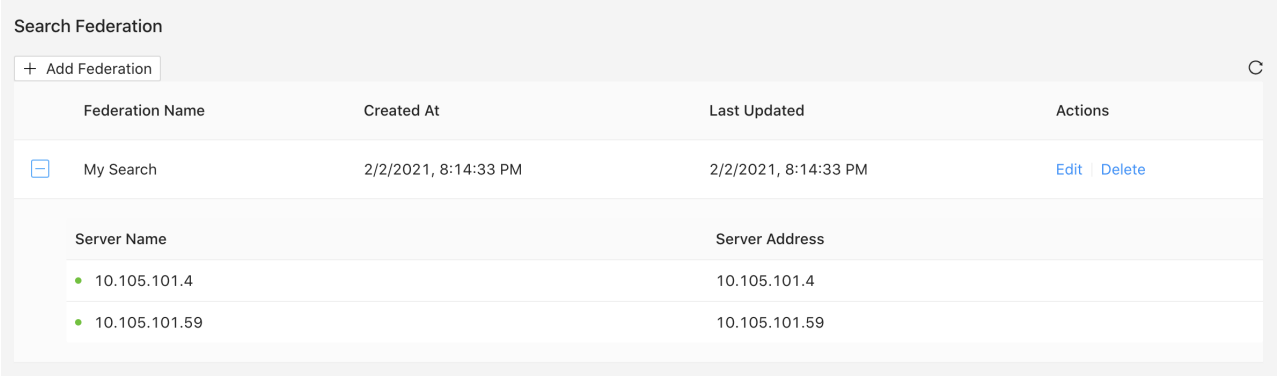


3. Go back to *Federation Management* in the remote cluster (10.105.101.59), and click *Accept* to accept this federation request, or click *Ignore* to ignore the request.



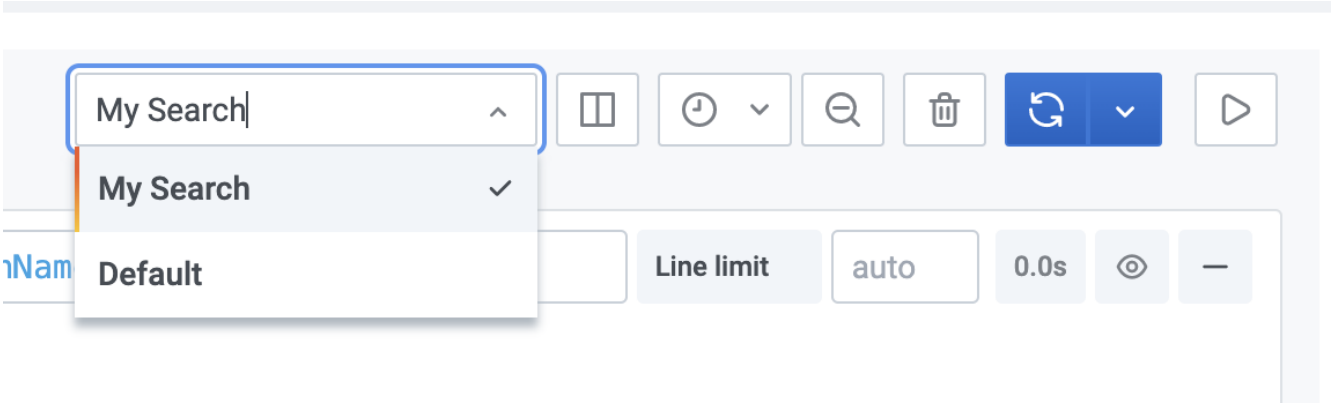
4. On the local cluster (10.106.2.166), click the *Add Federation* button of the *Search Federation* section, and select the *Federation Servers*.



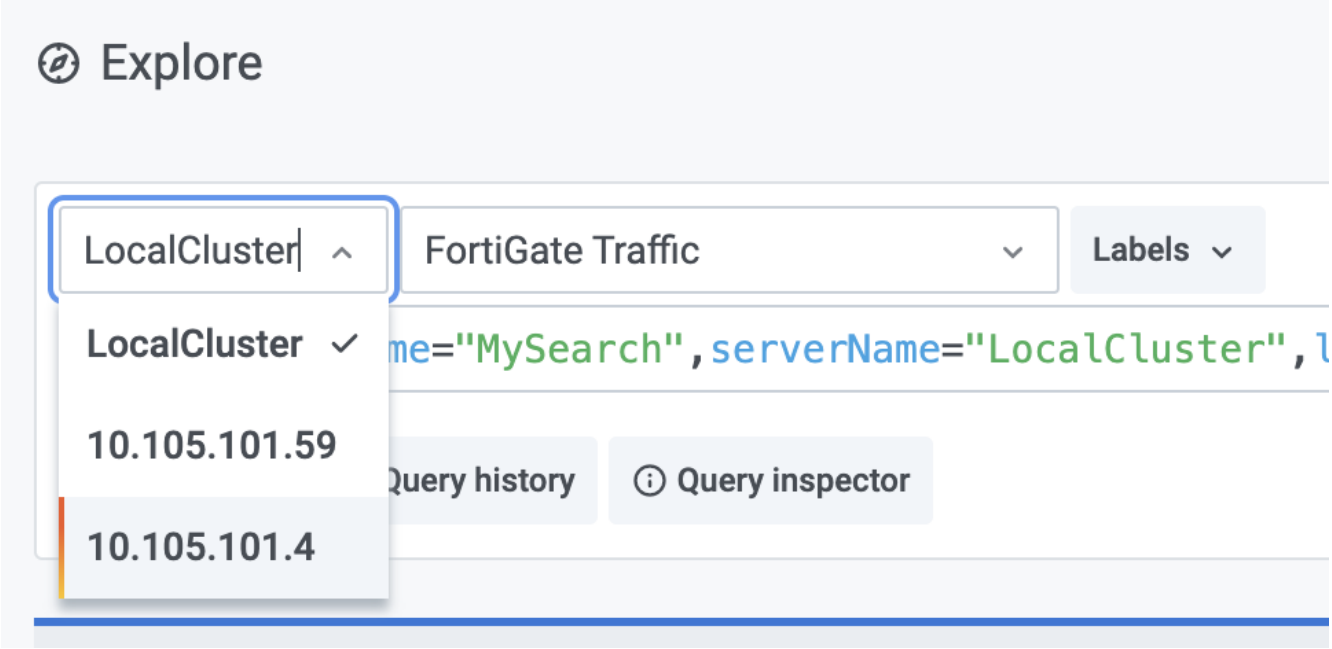


Search with Federation

To search with a different cluster, select a *Search Federation* that contains multiple servers (for example, *My Search*), and then select the cluster name (10.105.101.59) from the *Cluster* dropdown.



And then select the cluster name (e.g. 10.105.101.59) in the *Cluster* dropdown.



You can also add another query for a remote cluster by clicking the *Add query* button. The search returns the results from both servers.

Log Query Language (LogQL)

To create custom queries, use *LogQL* in the log query input box of the *Global Search*. LogQL can be considered a distributed *grep* that aggregates log sources. LogQL uses labels and operators for filtering.

A basic log query consists of two parts:

- Log stream selector
- Log pipeline

Log Stream Selector

The log stream selector determines which log streams should be included in your query results. The stream selector is comprised of one or more key-value pairs, where each key is a log label and each value is that label's value. The log stream selector is written by wrapping the key-value pairs in a pair of curly braces:

```
{logType="fgt/traffic", adomid="3"}
```

In the example above, all log streams that have a label of `logType`, whose value is `fgt/traffic` and a label of "`adomid`" whose value is `3` will be included in the query results. This will match any log stream whose labels contains at least `3` for their `adomid` label. If there are multiple streams that contain that label, logs from all of the matching streams will appear in the results.

The = operator after the label name is a label matching operator. The following label matching operators are supported:

- **=**: Equals exactly
- **!=**: Not equal

Log Pipeline

Optionally, the log stream selector can be followed by a log pipeline. A log pipeline is a set of stage expressions chained together and applied to the selected log streams.

A log pipeline can be appended to a log stream selector to further process and filter log streams. This usually consists of one or multiple expressions, each expression is executed in sequence for each log line. If an expression filters out a log line, the pipeline will stop at this point and start processing the next line. An expression is a SQL-where-clause-like condition.

```
{logType="fgt/traffic", appcat="Collaboration"} | osname ILIKE 'windows%' AND dstinetsvc IREGEXP
      '^.*gmail.*' AND sentbyte > 10000000
```

In the example above , the condition will filter out the FortiGate traffic Collaboration app category log messages when the OS name contains "`windows`" in the beginning and destination internet service matches `Gmail` and sent bytes is greater than `1000000`10MB).

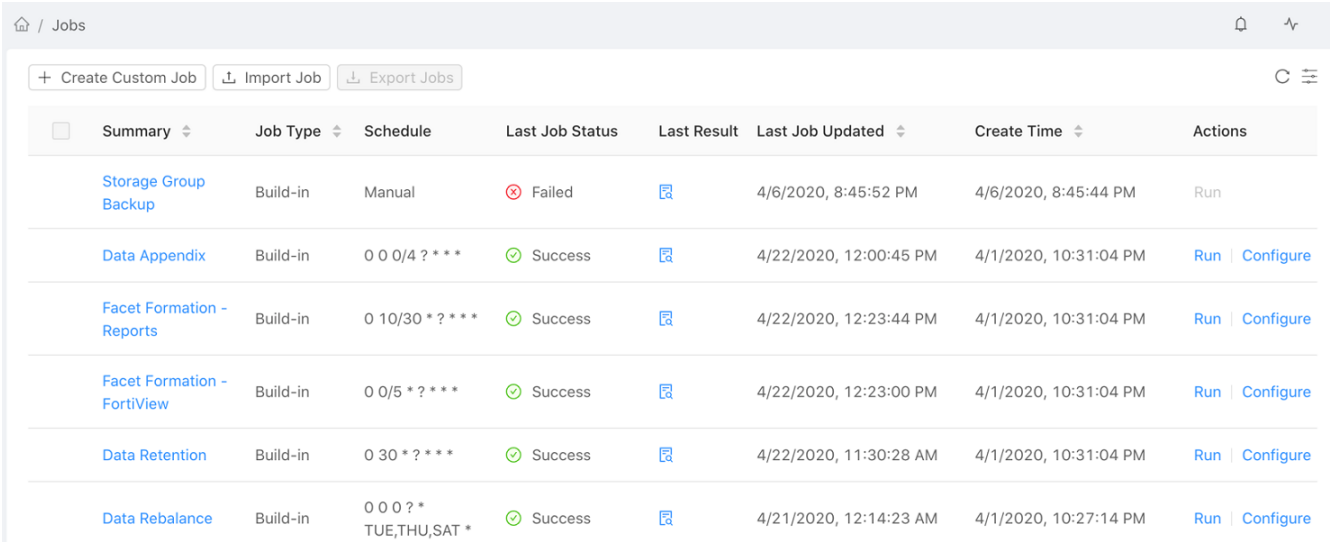
The following operators are supported in the Log Pipeline expression:

Operator	Description
=, **!=**, **<**, **<=**, **>**, **>=**	Comparison operators.
AND, **OR**, **NOT**	Logical operators.
BETWEEN ... **AND** ...	Compares to both a lower (**>=**) and upper (**<=**) bound.
IN	Compares an argument value to a set of values and returns **TRUE** if the argument matches any value in the set. **NOT IN** reverses the comparison.
LIKE	Comparison operator for **STRING**, with basic wildcard capability using **_** to match a single character and **%** to match multiple characters.
ILIKE	Case insensitive **LIKE**.
REGEXP	Tests whether an argument value matches a regular expression. Uses the **POSIX** regular expression syntax where **^** and **$** match the beginning and end of the string: • **.** represents any single character,

Operator	Description
	• ***** represents a sequence of zero or more items, • **+** represents a sequence of one or more items, • **?** produces a non-greedy match, and so on.
IREGEXP	Case insensitive **REGEX**.

Job management and automation

The Jobs page contains a table that displays all jobs in the system, including built-in jobs and custom jobs.



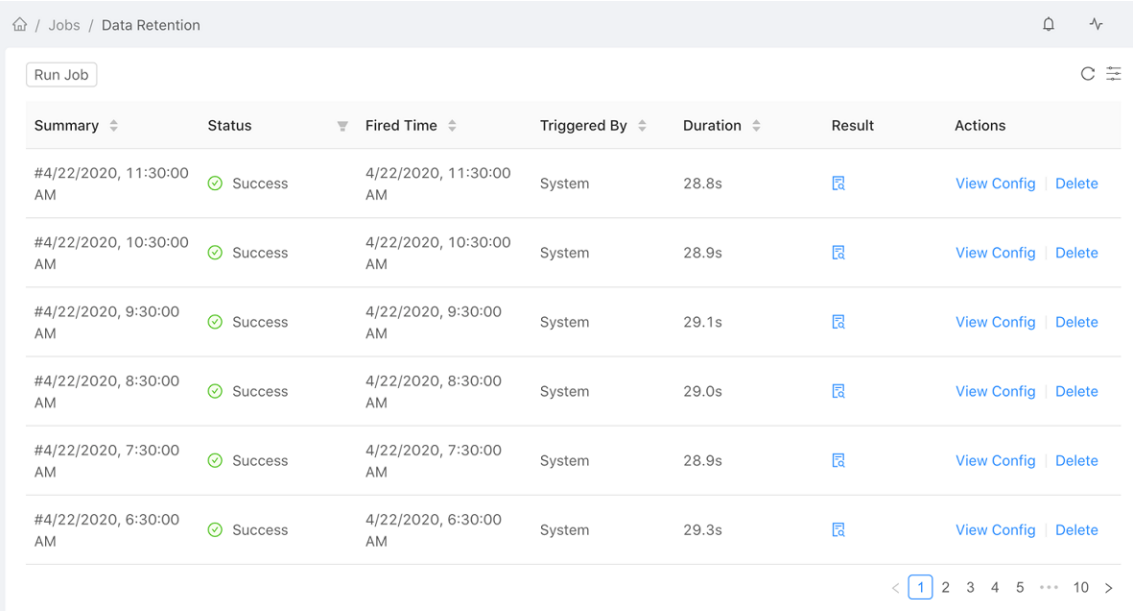
The Jobs table contains the following columns:

Column header	Description
Summary	The name or short description of a job. You can click the summary to view its execution history (see Job history on page 68).
Job Type	There are two types of jobs: • **Built-in:** Pre-configured system jobs. • **Custom:** Job created by an administrator.
Schedule	Shows how often the job is run.
Last Job Status	Indicates the status of the job: • **Success:** The job execution successful. • **Failed:** The job execution failed. • **Running:** The job is currently executing. • **Queued:** The job has been put into an execution queue and will be executed shortly. • **Timeout:** The job execution has timed out. • **Aborted:** The job execution has been interrupted. This status usually occurs when the user manually aborts. • **Skipped:** The job has been skipped. This status usually occurs when a previously executed job is still running and its job configuration does not allow concurrent jobs.
Last Job Result	View the last job execution result by clicking **Job Result** .

Column header	Description
Last Job Updated	When the job was last run.
Create Time	When the job was first created.
Actions	You can perform two actions on the health test: • **Run:** Manually launch a job execution. • **Configure:** Change a job's configurations. • **Delete:** Delete a job and the job's history.

Job history

To access the Job History page and see the job execution records, click its Job Summary link.



You can view records of the job's execution result, job configurations, or even delete the record.

FortiAnalyzer-BigData only saves the last 500 records for job execution results

Built-in automation jobs

FortiAnalyzer-BigData has the following default built-in jobs:

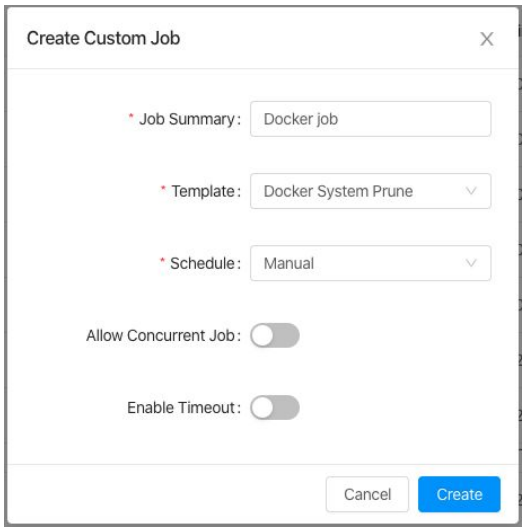
Built-in jobs	Description
Data Retention	Created automatically when storage pools are created. This job is used to apply data retention policies for the Storage Pool which marks the old data for deletion and makes space for future data.
Data Rebalance	Created automatically when storage pools are created. This job is used to rebalance Kudu data partitions to evenly distribute them across the hosts.
Data Appendix	Created automatically when storage pools are created. This job generates the list of available sub-types of FortiGate Event logs for LogView.
Facet Formation - Report	Created automatically when storage pools are created. This job generates the pre-aggregated facets to speed up Report queries.
Facet Formation - FortiView	Created automatically when storage pools are created. This job generates the pre-aggregated facets to speed up FortiView queries.
Storage Pools Restore	This job will be created automatically when you launch the storage pool restore function from the Data page. For more details, see Data restore on page 83.

Custom automation jobs

You can create or import custom jobs by using built-in or custom templates rendered as an Ansible playbook.

To create a custom automation job:

1. In the top-left corner of the Jobs page, click *Create Custom Job*.
   The Create Custom Job dialog box loads.



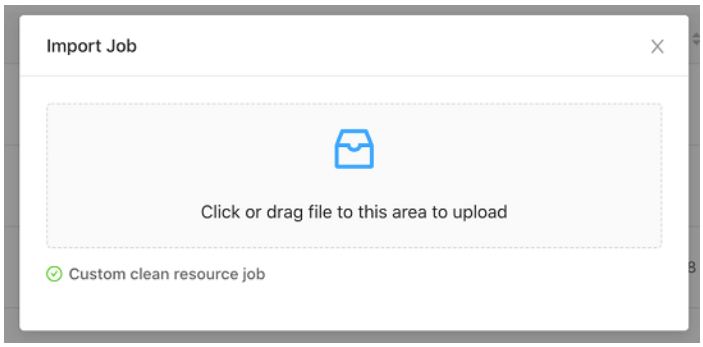
2. Complete the following fields:

Field name	Description
Job Summary	Enter the job description.
Template	Select a job template. For templates that have additional fields to fill out, see Custom job templates on page 71.
Schedule	Select a scheduling timer: • **Manual:** The job will not be executed until you manually launch it. • **Daily:** The job is scheduled to run on a daily basis. Select a run time and enable the **Enable Job** toggle so the schedule takes effect. To pause the job schedule, disable the toggle. • **Advanced:** Supports standard cron expressions. You can use predefined cron expressions to schedule a run every 30 minutes, every hour, every 12 hours, and more. Switch the **Enable Job** toggle to enable so the schedule takes effect. To pause the job scheduling, disable the toggle.
Allow Concurrent Job	Enable to allow multiple jobs to run at the same time.
Enable Timeout	Enable to define job timeout.

3. When you finished configuring your job, click *Create*.

To import custom jobs:

1. In the top-left corner of the Jobs page, click *Import Job*.
The Import Job dialog box loads.



2. Drag or select the file you want to import into the dialog box.

To export multiple custom jobs:

1. From the Jobs page, select the jobs you want to export.
2. In the top-left corner of the Jobs page, click *Export Job*.
   The Confirm Export Job dialog box loads.
3. Click *Confirm* to export your jobs.

Custom job templates

When you select a template for your custom job, you might need to fill out additional fields depending on the template you select. The following templates require additional configuration before you can apply them.

Backup Table Validation

The Backup Table Validation template is used to verify the data integrity of the backup data at the selected location.

Select the storage pool and enter the Hadoop Distributed File System (HDFS) URL for the backup location.

Custom Template

Custom templates are used to create the content for custom jobs for when built-in jobs don't meet your specific needs. You can create custom templates to operate the host, collect information, take actions, and more.

Custom templates require you to use the Ansible playbook YAML format to define the content. For information about Ansible specifications, refer to the official Ansible documentation.

The following example template collects the disk usage of the BigData Controller and sends it to a Slack channel:

```
- name: Collect disk usage and send to slack
  hosts: controllerIp
  vars:
    - slack_url: "https://hooks.slack.com/services/xxxxxxx" # your slack app webhook url
  tasks:
- name: Collect disk usage
  command:"df -h"
  register: result
- name: Send to slack
  uri:
    url:"{{ slack_url }}"
    body:'{"text": "{{ result.stdout }}"}'
    body_format: json
    method: POST
```

The follow table shows all the Ansible inventory group names you can use as hosts values in your playbook and template. Those values are pre-populated in the Ansible inventory and are automatically applied with each execution.

• hdfs_datanode • hdfs_namenode • kudu_tserver • kudu hive_metastore • zookeeper • kafka_broker • impala_catalog • impala • impala_statestore • yarn_nodemanager • yarn_resource_manager • spark_history_server	These inventory groups can be used to select the host(s) that have the named services running. For example, using "**host**: kudu_tserver" in your playbook allows it to be executed on all hosts has kudu-tserver instance.
• hdfs_datanode_reachable • hdfs_namenode_ reachable • kudu_tserver_reachable • kudu_reachable • hive_metastore_reachable • zookeeper_reachable • kafka_broker_reachable • impala_catalog_reachable • impala_reachable • impala_statestore_ reachable • yarn_nodemanager_	These groups can be used to select one of the reachable hosts that belong to the named service. For example: kudu has instances spreading on 3 hosts, and "**hosts**:kudu_ reachable" will randomly return one that is reachable at the execution time.

reachable • yarn_resource_manager_ reachable • spark_history_server_ reachable	
• metastore • datanode • master	These groups can be used to select hosts the belong to the named role.
• metastore_reachable • datanode_reachable • master_reachable	These groups can be used to select a random host that is reachable at the execution time, from the ones with the named role.
• controllerIp	This group can be used to the BigData Controller host.

In addition to these groups, you can also use the host name shown in the Hosts page to directly select a particular host for the playbook execution.

Data Log Type Appendix

The Data Log Type Appendix is run to re-generate the list of available log types for LogView.

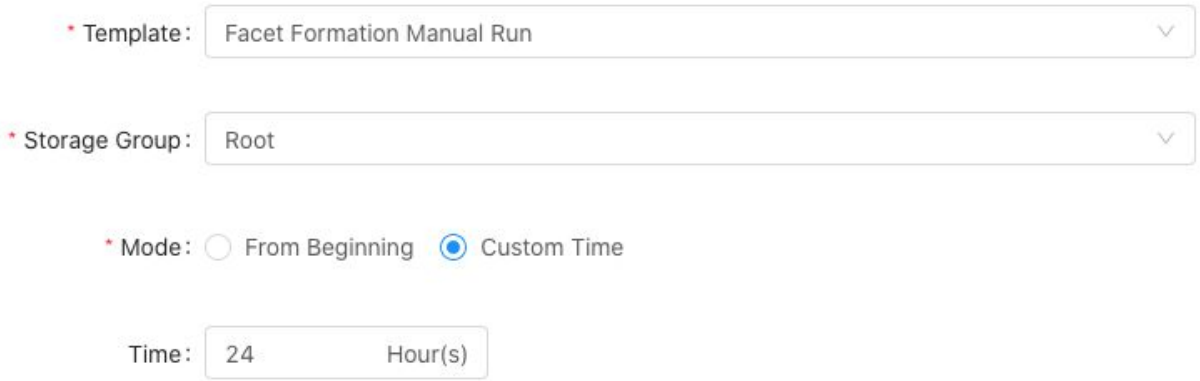
This is a resource intensive operation. Run this only if the available log types sidebar of LogView is not working properly.

Docker System Prune

The Docker System Prune template is run to remove all unused docker containers, networks, and images (both dangling and unreferenced) to clear disk space.

Facet Formation Manual Run

The Facet Formation Manual Run enables you to manually run a facet formation. Run this job only when the FortiView query performance is exceptionally slow.



First, select a storage pool, and then select the time to do facet formation. You can choose between starting the facet formation from the beginning, or from a specific time.

HDFS Safemode Leave

The HDFS Safemode Leave template enables you to leave the HDFS safe mode from an unexpected shutdown.

Hive Metastore Backup

The Hive Metastore Backup template creates a backup of the data in Hive Metastore and saves it to an HDFS location.

Hive Metastore Restore

The Hive Metastore Restore template restores the data in Hive Metastore from an HDFS location.

Kafka Deep Clean

The Kafka Deep Clean template deep cleans Kafka topics and reinstalls Kafka (see How to recover from an unhealthy service status on page 121).

Kafka Rebalance

The Kafka Rebalance template rebalances the data load across the hosts. This is useful for when a Kafka node is decommissioned or when a new Kafka node joins or leaves the cluster. It includes replica leadership rebalance and partition rebalance. For more information, see Scaling FortiAnalyzer-BigData on page 104.

NTP Sync

The NTP Sync template performs a manual NTP time sync on all the BigData hosts. Run this job when Kudu time synchronization is unsynced (see How to recover from an unhealthy service status on page 121).

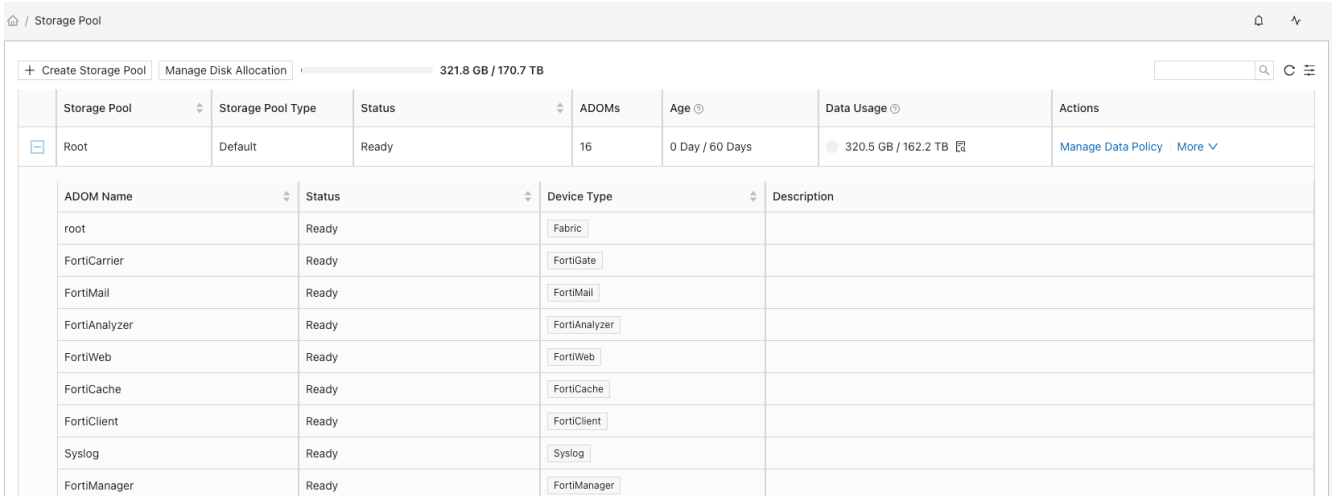
Purge Data Pipeline

This job resets the watermark and performs a clean restart of the pipeline.

Any unprocessed data will be lost (see How to recover from an unhealthy service status on page 121).

Data management

FortiAnalyzer-BigData uses Storage Pools to manage disk space. The *Data* page contains the Storage Pools table where you can monitor the group's status, manage storage polices and jobs, and backup or restore data. A default *Root* storage pool is included with FortiAnalyzer-BigData.



The Storage Pool table contains the following columns:

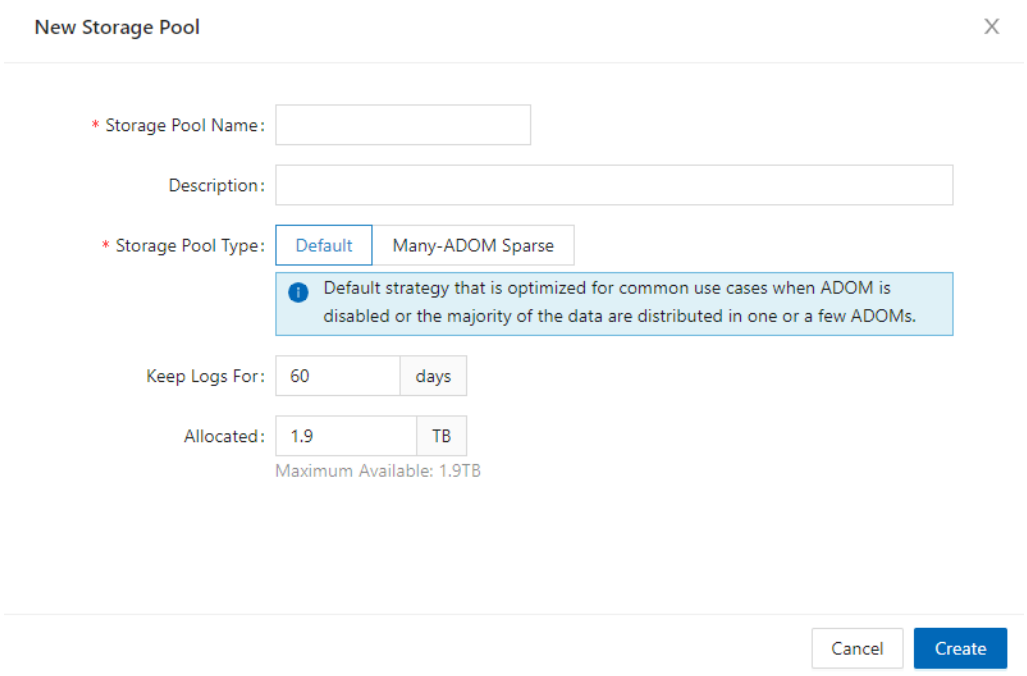
Column header	Description
Storage Pool	The name of storage pool. You can expand each storage pool to display all the ADOMs in that group.
Storage Pool Type	The type of storage pool, which indicates the storage strategy.
Status	Indicates the status of the storage pool. • **Ready**: The storage pool is ready for use. • **In Progress**: The storage pool is being created and is not yet ready for use. • **Failed**: The storage pool creation failed.
ADOMs	The number of ADOMs in that storage pool.
Age	The age of the storage pool and the number of days the logs will be stored.
Data Usage	The amount of data in use.
Actions	You can perform the following actions on a storage pool: • **Manage Storage Policy:** Determine how long and the maximum size you want to store the data, and when to do a data rollover. For more information, see Manage storage policy on page 77. • **Manage Job:** Manage jobs in that storage pool. • **Backup:** Create a backup of that storage pool. • **Manage Backups**: Show and delete the backup data. • **Restore:** Restore data.

Column header	Description
	• **Migrate ADOM**: Migrate ADOM from one storage pool to another. • **Delete Storage Pool**: Delete the storage pool. This action is only available if no ADOM exists in the storage pool.

To create a Storage Pool:

1. Click *Create Storage Pool*.
2. Configure the storage pool settings.

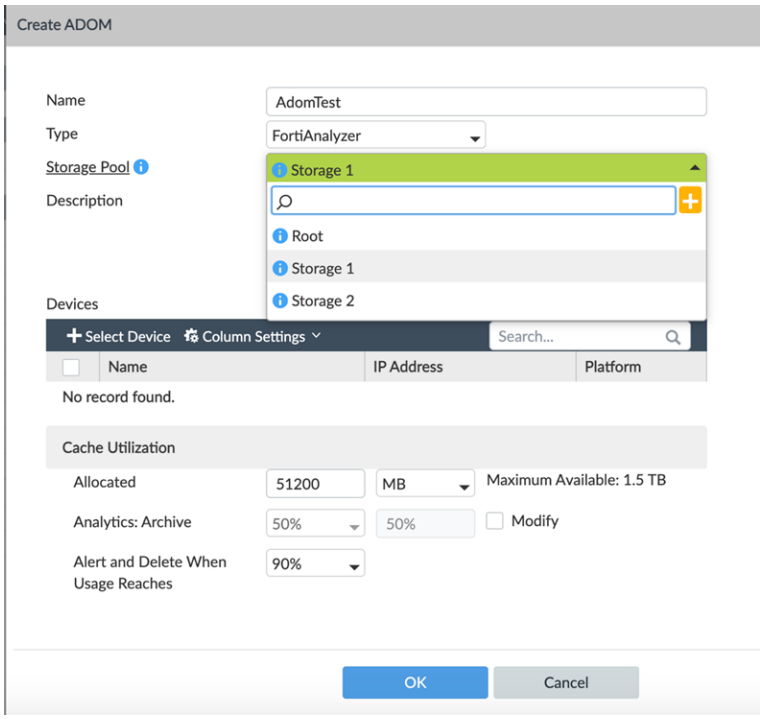
Option	Description
Storage Pool Name	Enter a name for the storage pool.
Description	Enter a description of the storage pool.
Storage Pool Type	Select the type of the storage pool. • **Default**: Default strategy that is optimized for common use cases when ADOM is disabled or the majority of the data are distributed in one or a few ADOMs. • **Many-ADOM Sparse**: Optimized for cases when ADOM is enabled and data are sparsely distributed across many ADOMs.
Keep Logs For	Enter the number days the logs are to be stored.
Allocated	Enter the amount of memory allocated for storing the logs.



3. Click *Create*.

To assign a Storage Pool to an ADOM:

1. Create a new ADOM.
2. From the *Storage Pool* dropdown, select a storage pool or click the Plus (**+**) sign to create a new pool.



Manage storage policy

You can manage the storage policy of each storage pool from the *Actions* column on the Data page.

To manage a data policy:

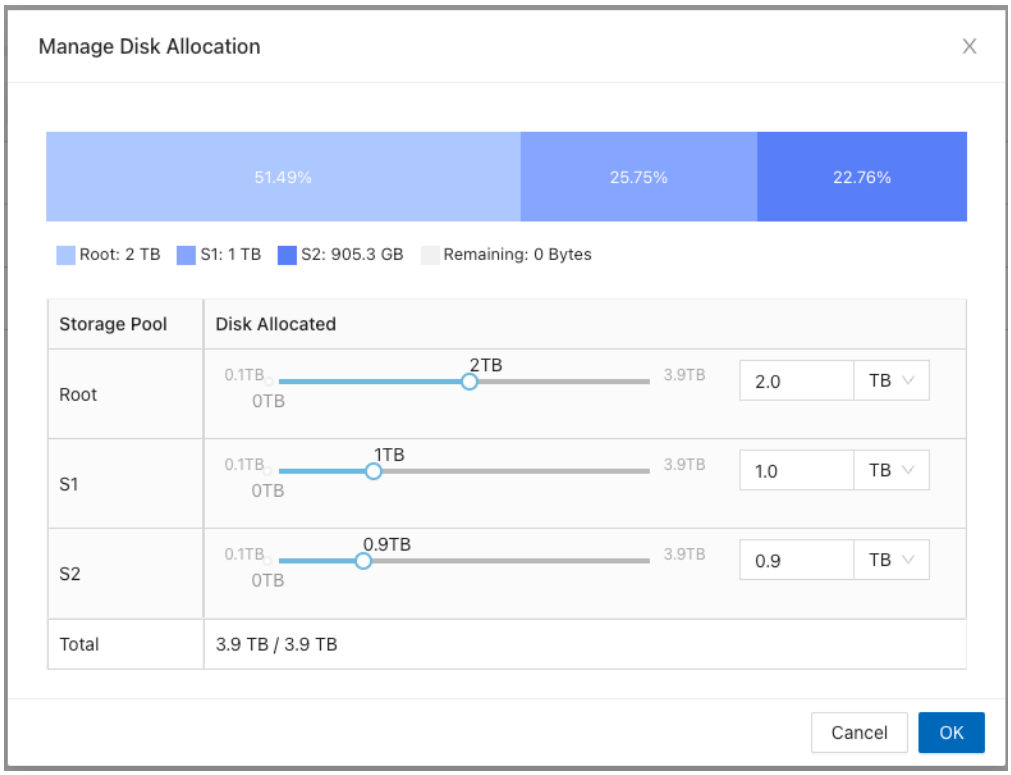
1. From the Data page, select a Storage Pool and click *Actions* > *Manage Data Policy*.
   The *Manage Data Policy* dialog opens:

2. In the *Keep Logs For* field, select the number of days you want to store the data in the system.
   FortiAnalyzer-BigData removes the data from the system after the selected number of days.

3. Click *OK*.

To manage disk allocation:

1. From the Data page, click *Manage Disk Allocation*.
   The *Manage Disk Allocation* dialog opens:



2. For each storage pool, move the slider in the *Disk Allocated* column to configure the maximum amount of data you want to store in the system.
   FortiAnalyzer-BigData removes the data from the system after the data size exceeds the selected number.
3. Click *OK*.

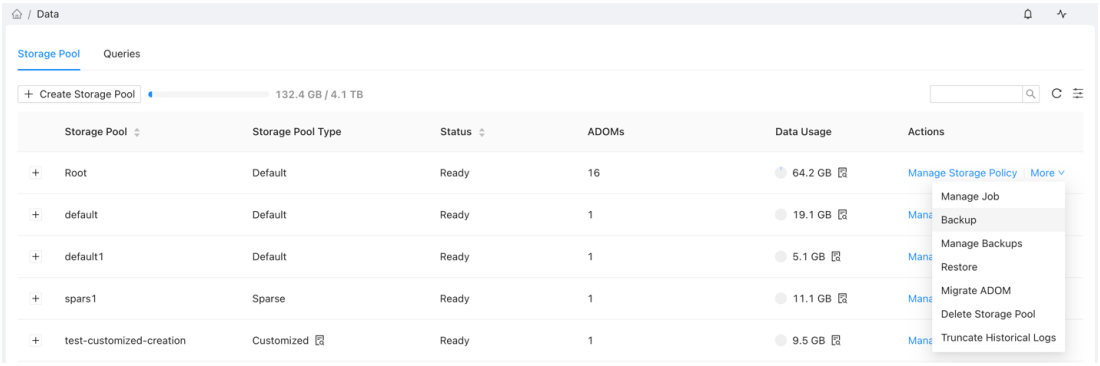
Data backup

The cluster-level high availability semantics guarantee that data stored in a Storage Pool can tolerate one blade lost at a time (data are replicated three times and distributed across the cluster hosts). We recommend backing up data to an external HDFS cluster for additional data-center-level redundancy.

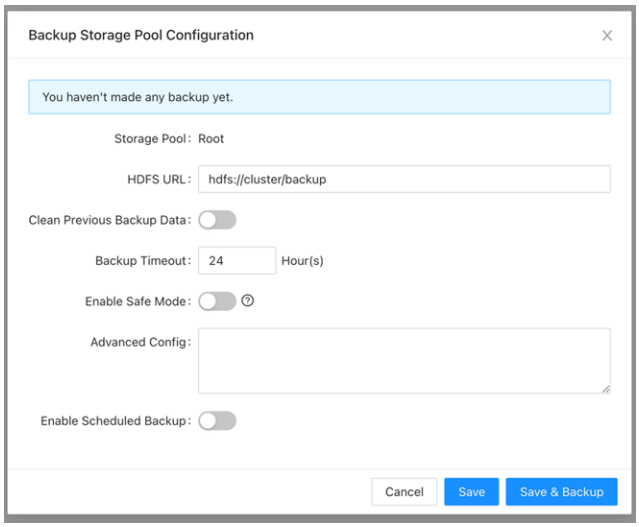
FortiAnalyzer-BigData supports disaster recovery and data portability. You can back up all the data within a Storage Pool to Hadoop Distributed File System (HDFS) in Parquet file format.

To back up data:

1. From the Data page, locate the storage pool you want to back up and select *Actions* > *Backup*.



The Backup Storage Pool Configuration dialog loads with the following fields:



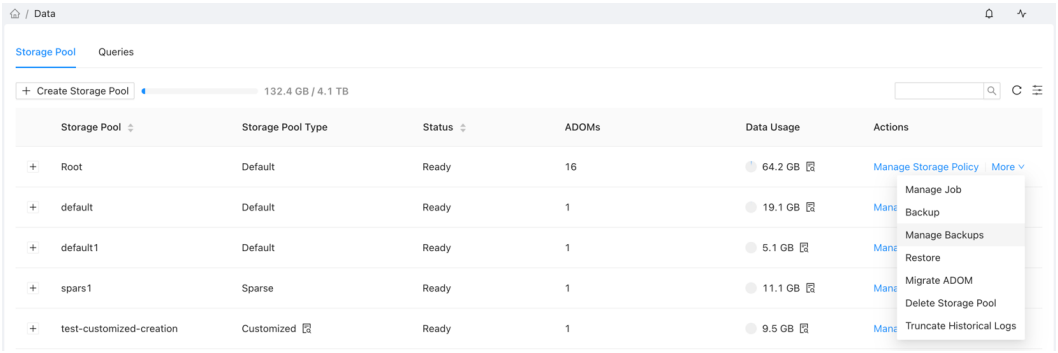
Field name	Description
HDFS Url	Defines the target directory of the HDFS cluster. By default, the field is set to the built-in HDFS in the Security Event Manager. We recommend backup to an external HDFS. If the URL is configured to an external HDFS cluster, all its hosts must be made accessible by the FortiAnalyzer-BigData hosts (see Backup and restore to external HDFS on page 97).
Clean Previous Backup Data	Enable to delete any previous backup data and start a new backup. Do not enable if you want to create an incremental backup.
Backup Timeout	Enter the number of hours before the backup job times out. After the timeout, the job will abort.

Field name	Description
Enable Safe Mode	By default, the normal backup job processes multiple tables in parallel and ignore any intermediate errors. Enable Safe Mode to back up the Storage Pool tables sequentially and to fail early if any error occurs. This mode may take longer to complete the back up, so only enable Safe Mode when the normal backup job fails.
Advanced Config	These configurations define the resources used for the job. Normal users should keep the default configurations.
Enable Scheduled Backup	Enable so the backup can be scheduled automatically.

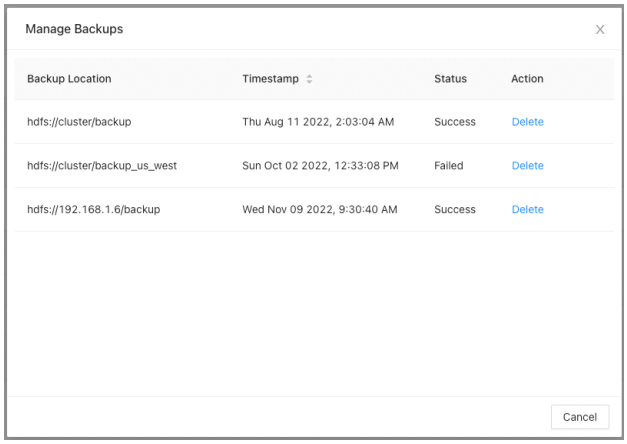
2. When you are finished, click *Save & Backup* to begin the backup process.
3. You can monitor the status of your backup by navigating to *Jobs > Storage Pool Backup*.

To delete backup data:

1. From the Data page, locate the storage pool and select *Actions > Manage Backups*.



2. The *Manage Backups* dialog displays the backup location, timestamp, and status. To delete the backup data, select *Action > Delete*.



Incremental backups

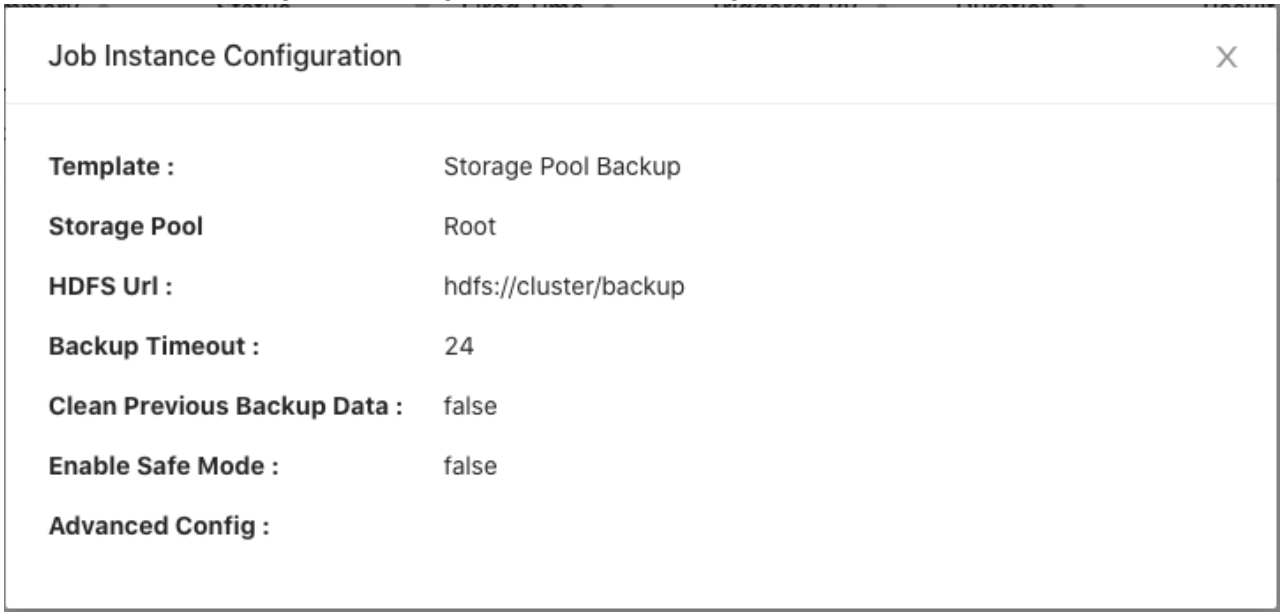
We recommend that you create incremental backups by consistently backing up new data to the same HDFS directory.

The first time a backup job is run, a full backup of the storage pool data will be saved to the HDFS directory. Subsequent runs will perform incremental backups which only contain the rows that have changed since the initial full backup. Thus, the subsequent backups will be faster and more efficient.

To create manual incremental backups:

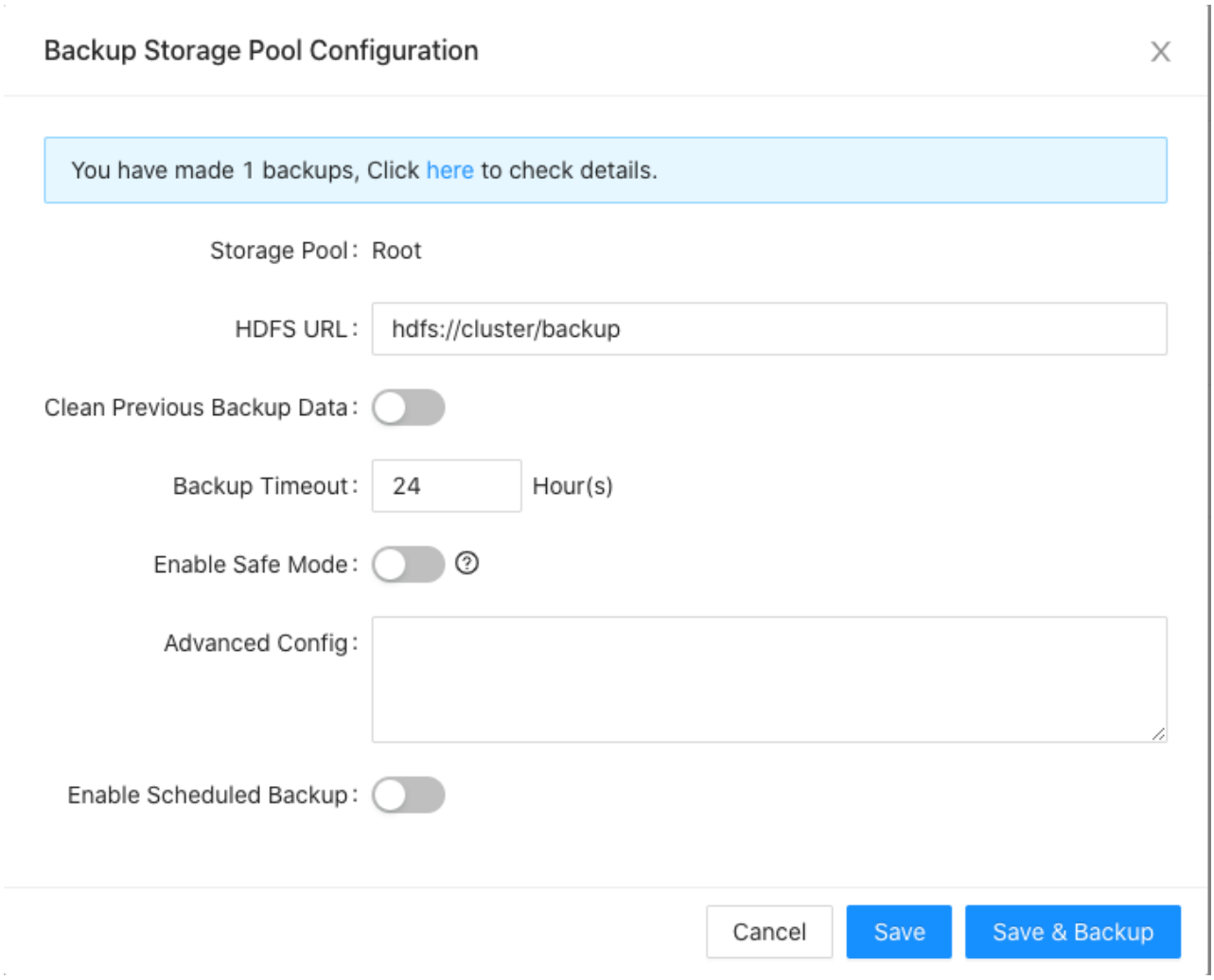
If you have already created a previous backup, you can manually create an incremental backup against it.

1. From the navigation bar, go *Jobs* and click *Storage Pool Backup* to view all the completed backups.
2. Select the backup which you want to create an incremental backup against and click *View Config*.
   The Job Instance Configuration dialog loads with the following fields:



3. In the *HDFS Url* field, copy the URL.
   For example: hdfs://cluster/backup/7o7T
4. Go to *Data* and select the same Storage Pool as the previous backup, and click *Actions* > *Backup*.
5. In the *HDFS URL* field, paste in the HDFS Url copied from step 3.

You can check the number of existing backups in the Backup Storage Pool Configuration dialog.



6. Ensure the *Clean Previous Backup Data* option is disabled so you do not clean any previous backup data, allowing this backup to be incremental.

   You can enable this option to make a full backup to the HDFS directory, however, a full backup job will be more time consuming than an incremental backup.

7. When you are finished, click *Save & Backup* to begin the backup process.

To create scheduled incremental backups:

You can also schedule incremental backup jobs by enabling the *Enable Scheduled Backup* option. This schedules incremental backup jobs to the HDFS you set. Fortinet strongly recommends scheduling maintenance jobs at off-peak hours.

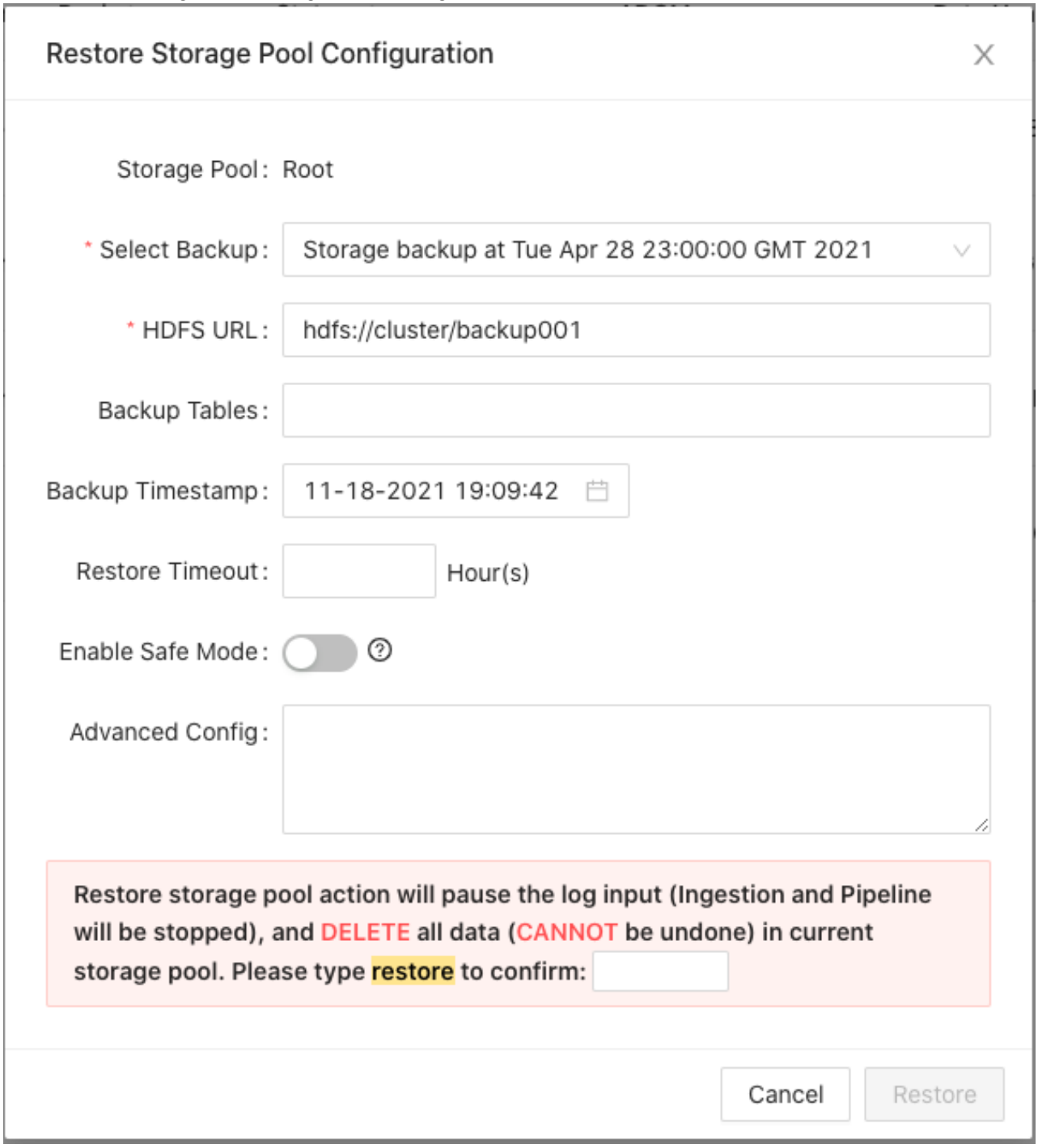
Data restore

Restoring data requires you to drop all tables in the storage pool. Be cautious when selecting your configurations.

To restore data from a backup

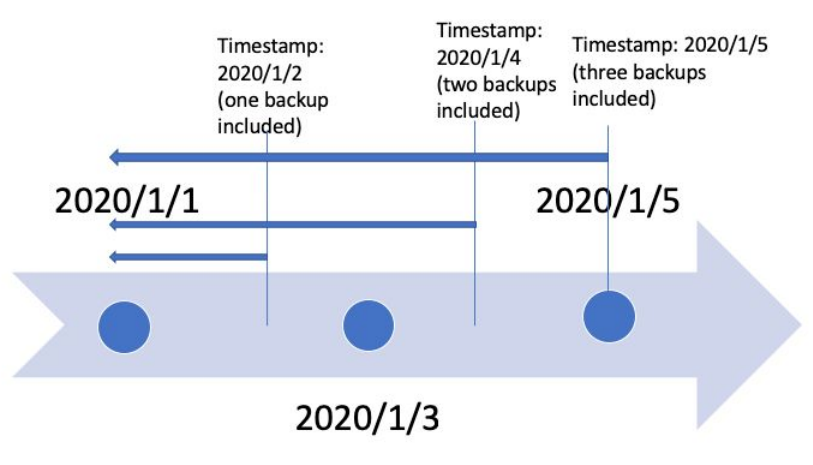
1. From the navigation bar, go to Data and select the Storage Pool you want to restore data for.

2. In the Storage Pool row, click *Actions* > *Restore*.
The Restore Storage Pool Configuration dialog loads.



3. Configure the following fields:

Field name	Description
Select Backup	Select the backup type you used. If the data is from an external system, select Custom.

Field name	Description
HDFS URL	Defines the location of the backup. If the URL is configured to an external HDFS cluster, all of its hosts must be accessible by of the hosts of the Security Event Manager.
Backup Timestamp	This config can be used to limit the data that you want to restore. It only applies for multi-backups (multiple incremental backups). The following figure shows how multi-backups are restored: 
Enable Safe Mode	By default, the normal backup job processes multiple tables in parallel and ignore any intermediate errors. Enable Safe Mode to back up the Storage Pool tables sequentially and to fail early if any error occurs. This mode may take longer to complete the back up, so only enable Safe Mode when the normal backup job fails.
Restore Timeout	Enter the number of hours before the restore job times out. After the hours elapse, the job will abort.
Advanced Config	These configurations define the resources used for the job. Normal users should keep the default configurations.

4. When you are finished, enter `restore` into the confirmation box to confirm.
5. Click *Restore* to begin the data restoration process.

Migrate an ADOM to another Storage Pool

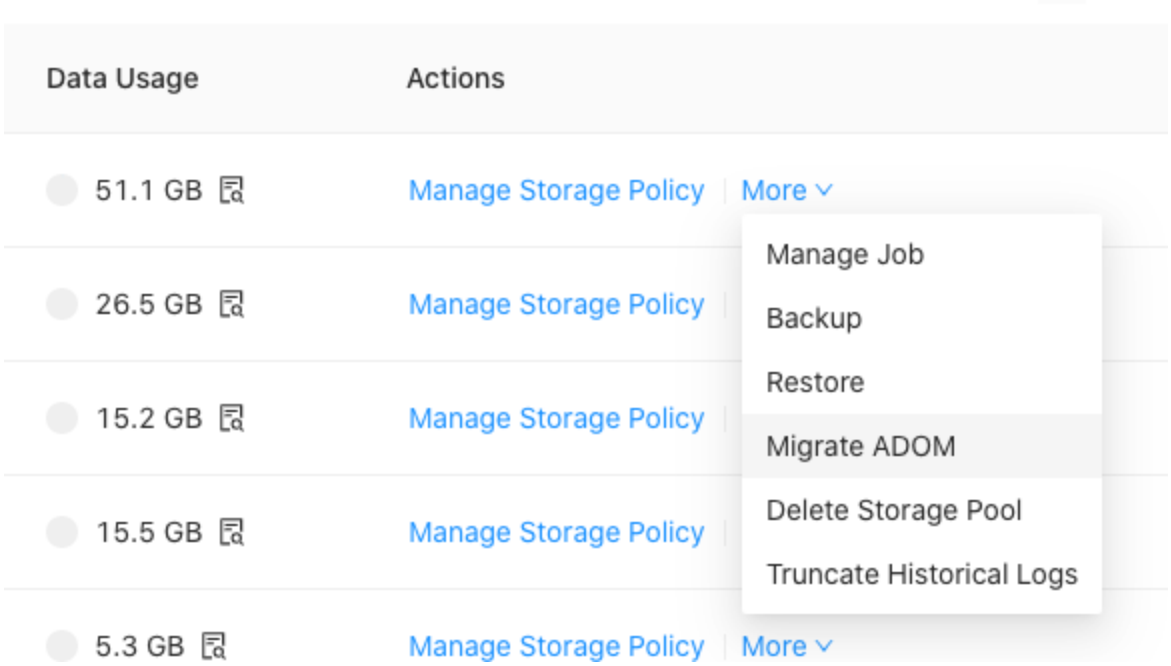
Grouping ADOMs with similar log rates and data retention requirements into a storage pool is recommended. For example, group small ADOMs (in terms of log rate and data volume) into one Storage Pool and larger ADOMs in another. When different sized ADOMs are grouped into one storage pool, the query performance on the smaller ADOMs will be affected by the larger ADOMS.

You may need to move an ADOM to another Storage Pool if its data characteristics change dramatically (e.g. increase in log rate) or data retention requirement changes.

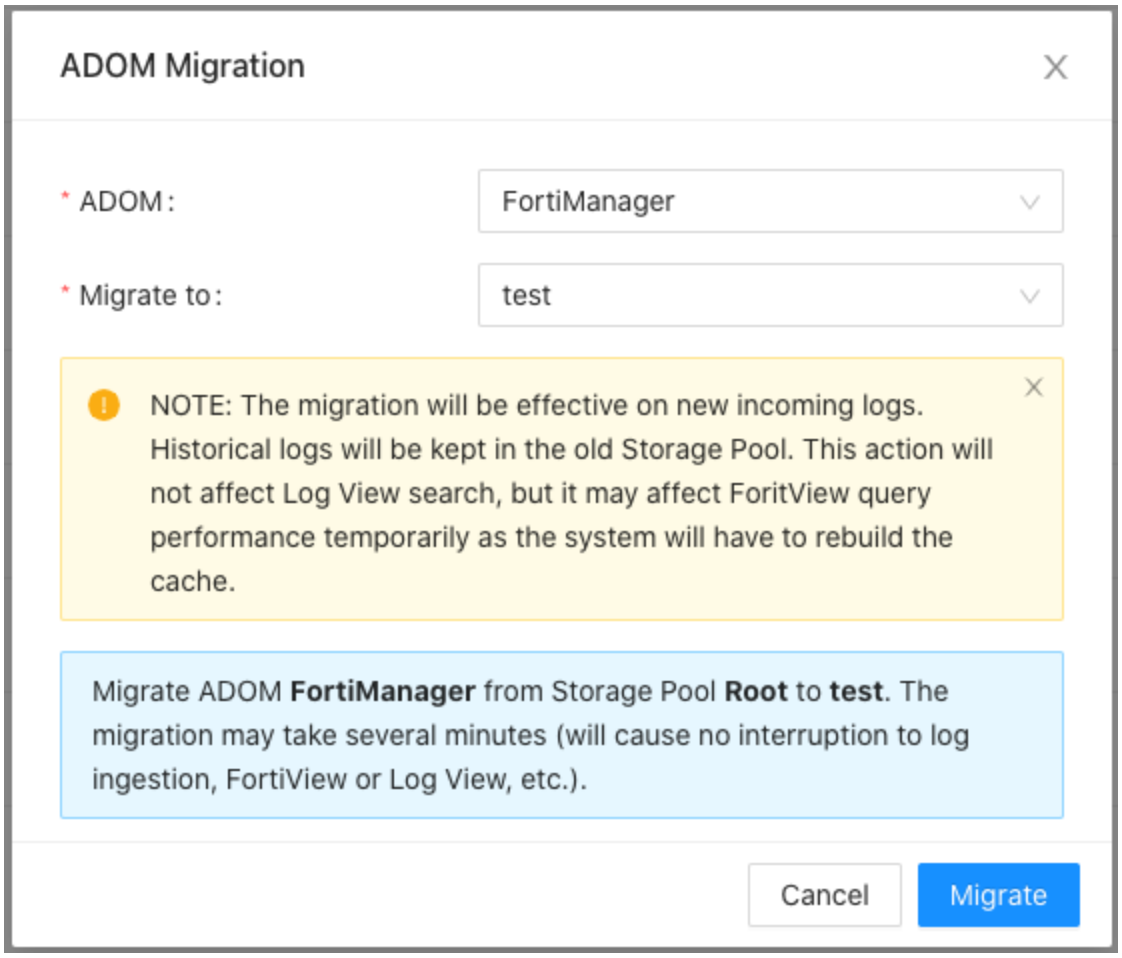
After migration, new incoming logs are sent to the new Storage Pool. Historical logs will be kept in the old Storage Pool and managed by the old data retention policy. Logs can be queried seamlessly even though the data resides in multiple Storage Pools.

To migrate an ADOM to another Storage Pool:

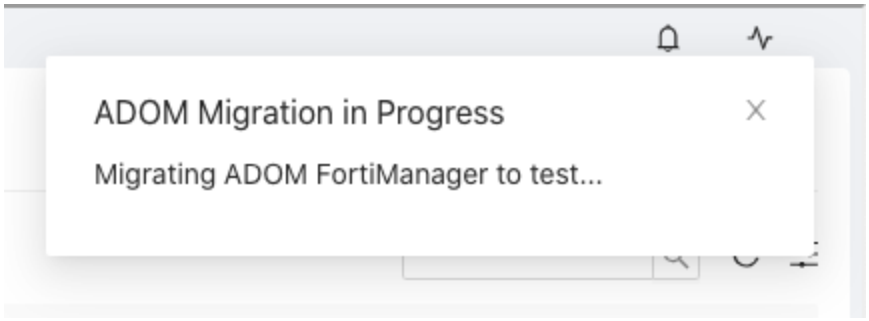
1. Go to System *Settings* > *Storage Pool*, and locate the Storage Pool that contains the ADOMs to migrate.
2. In the *Actions* column, click *More* > *Migrate ADOM*. The migration dialog opens.



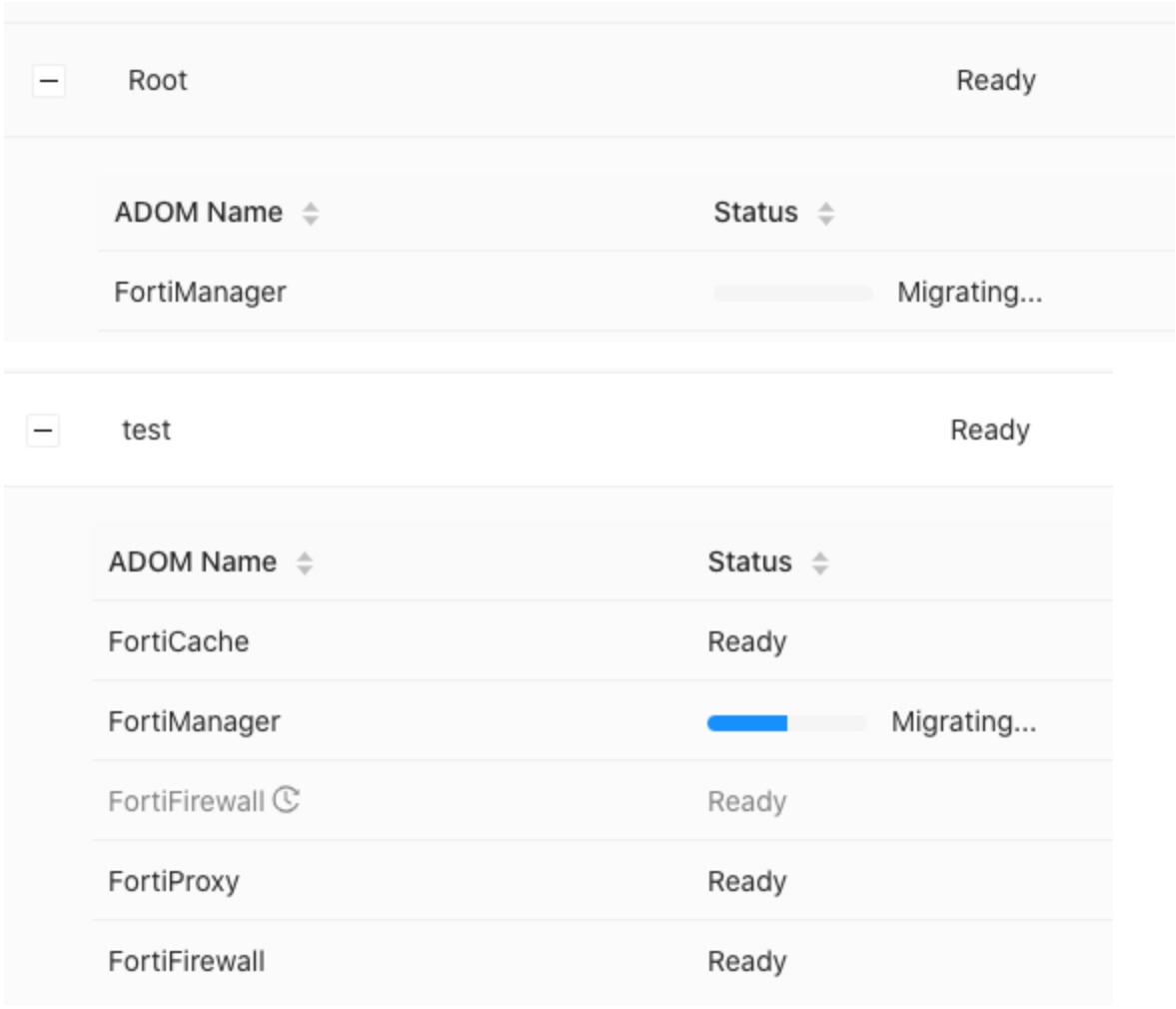
3. From the *ADOM* dropdown, select the ADOM you want to migrate, and from the *Migrate to* dropdown, select the target Storage Pool.



4. Click *Migrate*. The migration progress notification is displayed.

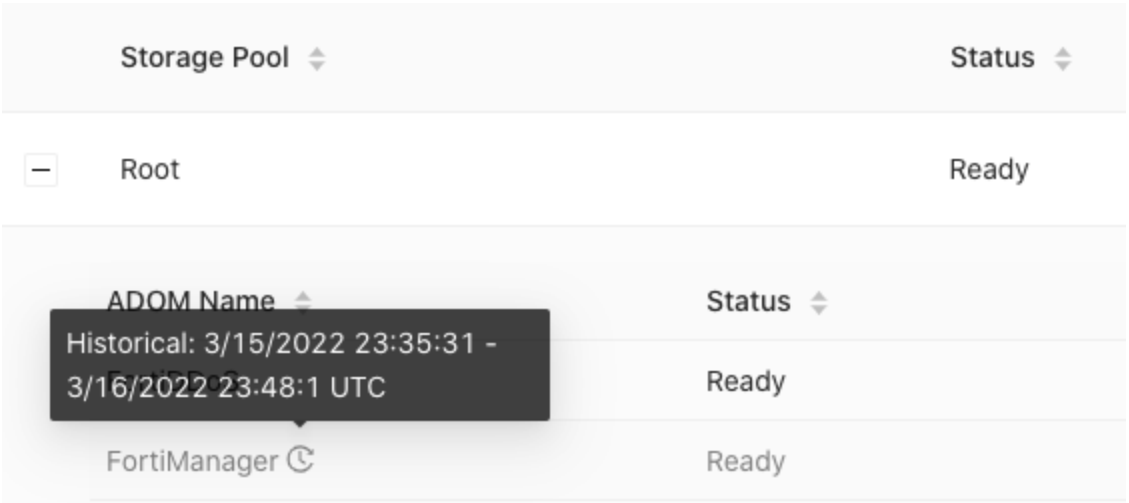


The s ADOM *Status* changes to *Migrating* in both Storage Pools.



When the migration is complete, two ADOM records are created in both Storage Pools. The pool with the clock icon indicates the ADOM with historical log data. The pool without the clock icon is the ADOM where the new incoming logs are sent.

To view the time range of historical logs, hover over the clock icon.

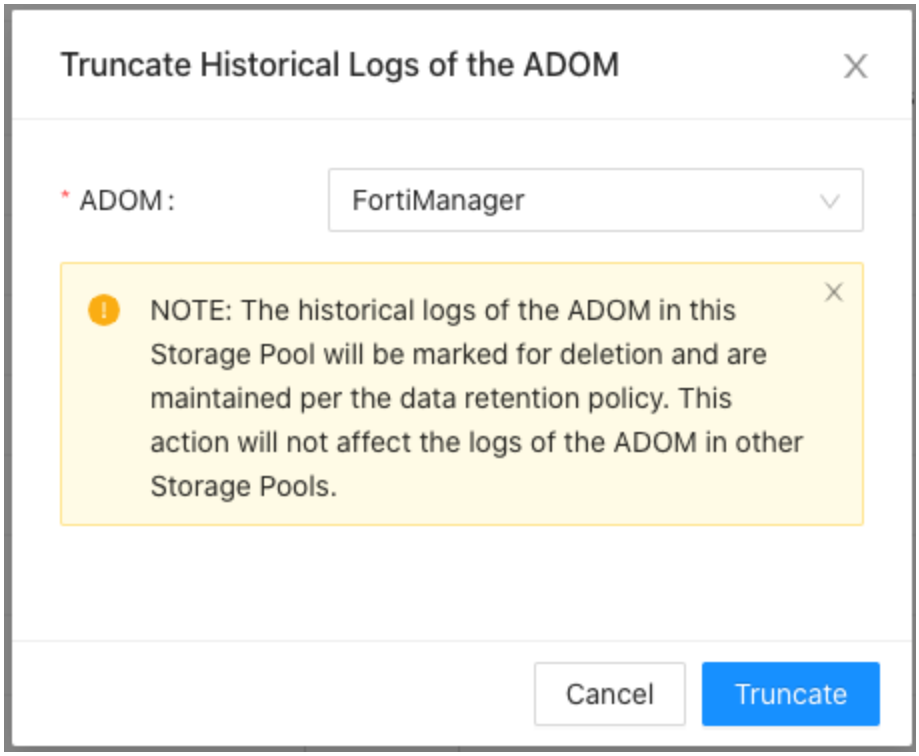


Truncate historical logs of the migrated ADOM

You can truncate the historical logs of an ADOM in a Storage Pool. Once truncated, the historical logs of the ADOM will be marked for deletion. After the logs are truncated the log data is not searchable, however the space is not cleared immediately. The log data will be retained by the data retention policy of the Storage Pool.

To truncate historical logs:

1. Go to *System Settings* > *Storage Pool*, and locate the Storage Pool that contains the historical ADOM to truncate.
2. In the *Actions* column, click *More* > *Truncate Historical Logs*. The migration dialog opens.
3. Click *Truncate*.



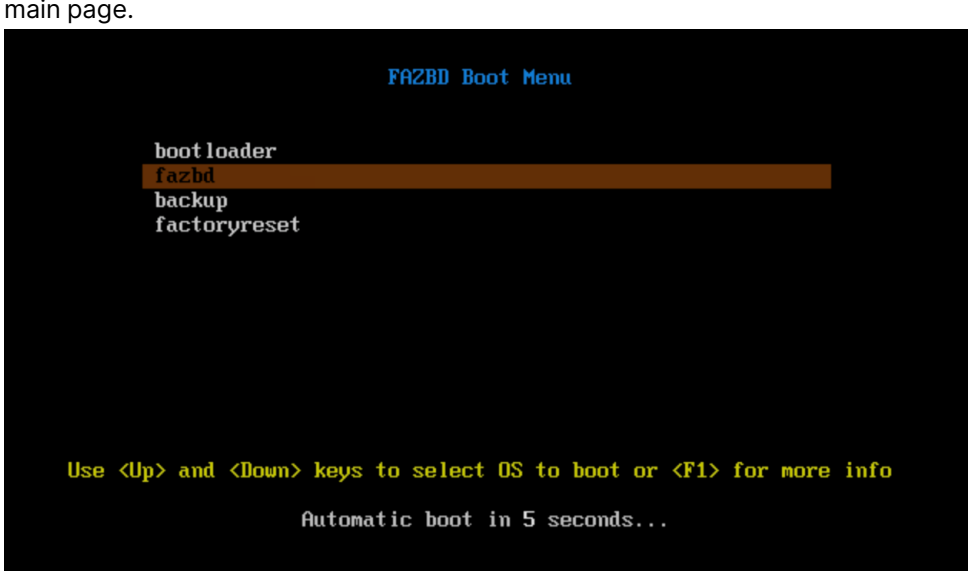
Bootloader

The FortiAnalyzer-BigData Bootloader is a system software that manages the FortiAnalyzer-BigData host's firmware. The Bootloader can be accessed during host reboot. The Bootloader can be accessed on all the hosts.

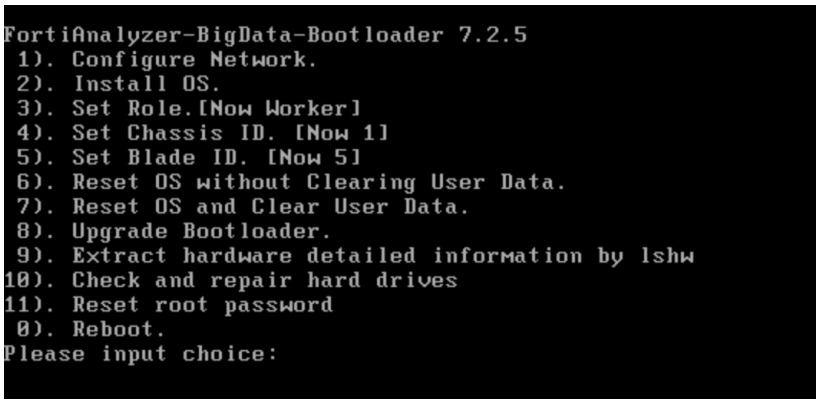
Improper selection of options in FortiAnalyzer-BigData Bootloader can have an adverse impact on the whole system, and even lead to system failure. Approach these options with great care and when in doubt, err on the side of caution.

To access the Bootloader for a FortiAnalyzer-BigData:

1. Connect to the CMM web management utility.
   See *Connect to the Chassis Management Module* in the FortiAnalyzer-BigData Getting Started Guide for your appliance: 4500F or 4500G.
2. Select one of the hosts to enter its bootloader.
   See *Remotely control blades via CMM* in the FortiAnalyzer-BigData Getting Started Guide for your appliance: 4500F or 4500G.
   For example: Go to *Blade System > Summary* and select Blade A2 to access the BMC (Blade Management Console).
3. Click the *BMC IPV4* link to enter the BMC for the host.
   The default login credentials are on the Fortinet Product Credentials card
4. Go to *Remote Control > Console Redirection or iKVM/HTML5*.
5. Click *Power Control > Set Power Reset*.
6. Wait for the following options to appear. Use the arrow keys to select `bootloader` to open the bootloader's main page.



Bootloader Main Page



From the main page of the bootloader, you can select the following options:

- 1. Configure Network
- 2. Install OS
- 3. Set Role
- 4. Set Chassis ID
- 5. Set Blade ID
- 6. Reset OS
- 7. Reset OS and Clear User Data
- 8. Upgrade Bootloader
- 9. Extract hardware detailed information by lshw
- 10. Check and repair hard drives
- 11. Reset root password
- 12. Reboot
- sh. shell

1. Configure Network

The Configure Network option enables users to configure their IP, network mask, and network gateway information for the bootloader on the host in order to communicate with external servers hosting bootloader or FortiAnalyzer-BigData firmware images. Users can choose to specify static or DHCP IP addresses when available.

This option only configures the network for the bootloader, not the OS of the FortiAnalyzer-BigData host.

Before users can use this option to configure the network, they need to have the network interface associated with the external network. By default, the external network interface defaults to `eth1`.

```
Please input choice: 1
Please Choose Port:
eth0
eth1
Your Choice [eth1]:
Please Input IP/MASK [dhcp]: 10.106.2.168/24
Please Input Gateway []: 10.106.2.254
Your current input:
Device: [eth1]
IP/MASK: [10.106.2.168/24]
Gateway: [10.106.2.254]
Corrent? [Y/N/C]: Y_
```

2. Install OS

The Install OS option enables users to install FortiAnalyzer-BigData OS images on the host. Upon selection, users are prompted to provide server and image information. After confirmation, the FortiAnalyzer-BigData OS is downloaded from the server and installed.

Generally, users should use the `fazbdctl upgrade fazbd` command in FortiAnalyzer-BigData OS to upgrade the system software instead of using the bootloader Install OS option.

```
Please input choice: 2
Please choose method:
1). FTP
0). Cancel
Your choice: 1
Please input server IP [10.106.2.123]:
Please input file path [FAZBD.out]:
Please input username [ftp]:
Please input password:
Your current input:
Server IP: [10.106.2.123]
File path: [FAZBD.out]
Username: [ftp]
Password: []
Continue? [y]es/[n]o/[c]ancel: y_
```

3. Set Role

The Set Role option enables users to select a role for each host. You can see the current role of the host by the option.

In a FortiAnalyzer-BigData Security Event Manager architecture, each host has a designated role in order to collaborate with other hosts. There are two roles from the bootloader perspective: controller and worker.

- Controller: Refers to the Security Event Manager Controller and acts as the master of the other hosts.
- Worker: Nodes that are managed by the controller.

In a given cluster, only one active controller is allowed.

```
Please input choice: 3
1). Controller.
2). Worker.
Please choose blade role: 1_
```

4. Set Chassis ID

The Set Chassis ID is used to identify the chassis in multi-chassis cluster use case. Chassis IDs may range from 1 to 254. By default, it is 1. When you connect an extension chassis to an existing chassis cluster, the chassis ID needs to be changed to a unique number in 1 to 254 range. You can see the current Chassis ID by option.

```
Please input choice: 4
Please input chassis ID [1-254]: 1_
```

5. Set Blade ID

A Blade ID is used to identify the blade slot within a chassis. The order of the blade slots starts from the left side of the FortiAnalyzer-BigData appliance, starting from 1 to 14.

By default, all Blade IDs are set to reflect its physical slot number and users should not change the Blade ID. For example, the controller is in blade slot #2 and has a Blade ID of 2.

If you need to add a replacement blade to the chassis, you must first set the Blade ID to reflect its slot number so the firmware running on the blade knows its physical slot and its role.

```
Please input choice: 5
Please input blade ID [1-254]: 2
```

6. Reset OS

The Reset OS option enables users to soft reset the FortiAnalyzer-BigData firmware of this BigData host. To soft reset the whole Security Event Manager, use `fazbdctl` CLI commands on the BigData Controller instead (see Soft reset FortiAnalyzer-BigData on page 107).

A soft reset only restores the firmware and will not touch the data volume.

If this action is performed on the BigData Controller, all the BigData member hosts will have to be rebooted during the progress in order to sync with the BigData Controller.

7. Reset OS and Clear User Data

The Reset OS and Clear User Data option enables users to hard reset the FortiAnalyzer-BigData firmware of this BigData host. To hard reset the whole Security Event Manager, use `fazbdctl` CLI commands on the BigData Controller instead (see Hard reset FortiAnalyzer-BigData on page 108).

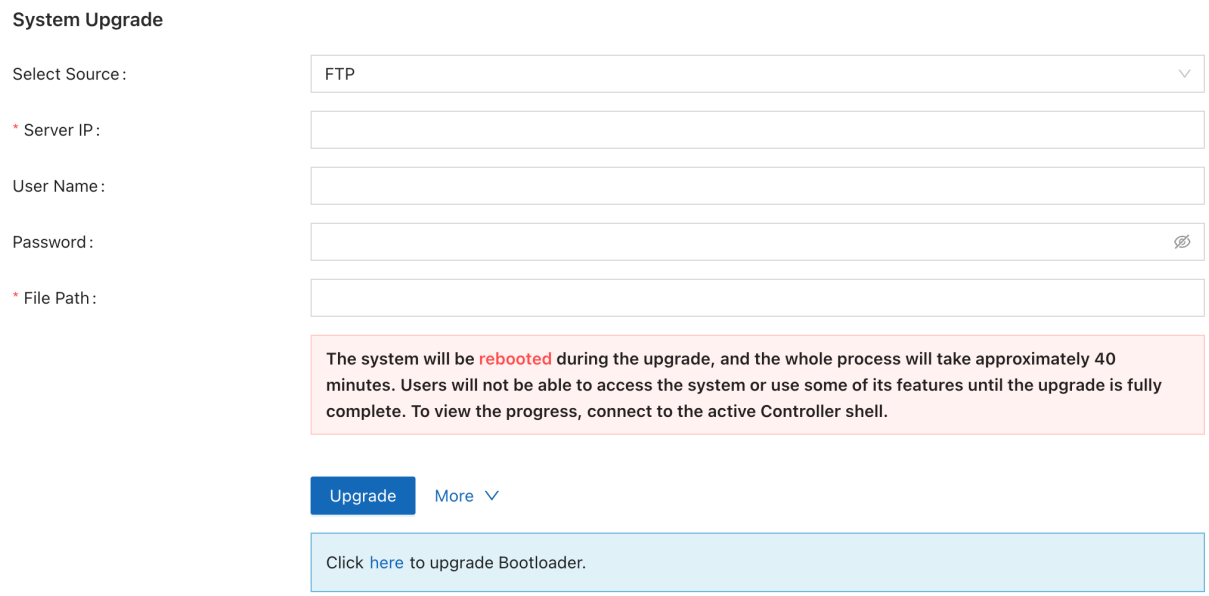
This will restore the firmware AND clear all the data volume.

8. Upgrade Bootloader

The Upgrade Bootloader option enables users to specify server and image information to perform upgrades to the existing bootloader. You can upgrade the bootloader from the Security Event Manager Controller CLI or the GUI.

To upgrade Bootload using the GUI:

1. In the banner, open the Account menu and click *Upgrade Firmware*.
2. Click *More > here*.

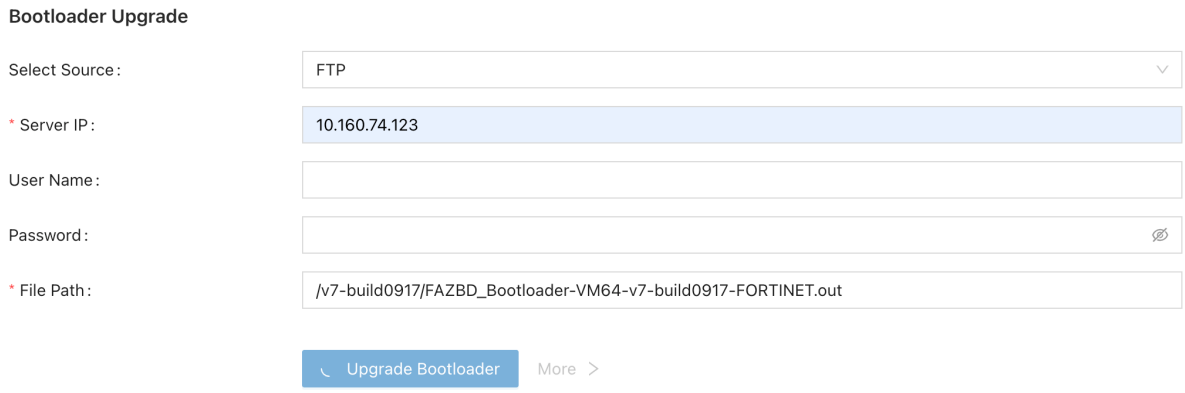


The *Bootloader Upgrade* dialog displays.

3. In the *Bootloader Upgrade* dialog, enter the following:

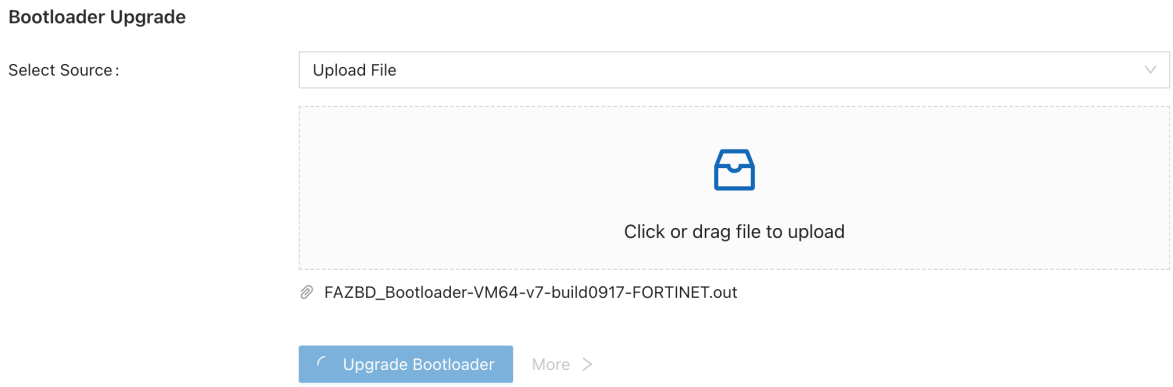
Select Source	Select *FTP*, *SFTP*, *HTTP*, *HTTPS*, or *Upload File*.
Server IP	Enter the source server's IP address.

User Name	Enter the user name. If not applicable, leave this field blank.
Password	Enter the password. If not applicable, leave this field blank.
File Path	Enter the file path for the new version of bootloader.

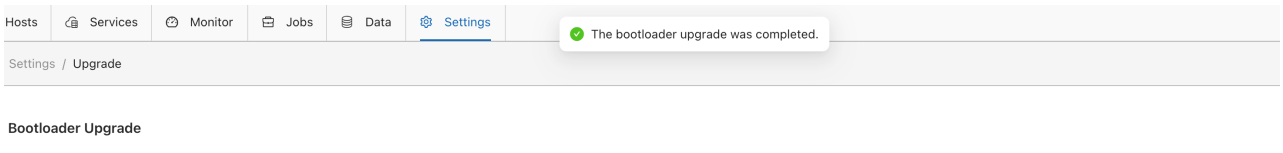


4. Click *Upgrade Bootloader*.
   The bootloader begins to upgrade. The upgrade takes approximately one to two minutes.

Do not leave this page while the upgrade is in progress.



When the upgrade is successful, the following message displays.



To upgrade Bootloader using the CLI:

Use the following command from the Security Event Manager Controller:

```
fazbdctl upgrade bootloader
```

This command allows you to upgrade the bootloader for all hosts at once.

1. Access the Security Event Manager Controller CLI by establishing an SSH connection to the Cluster Management IP. See Connect to the FortiAnalyzer-BigData CLI on page 12.
2. Run the following command:
   `fazbdctl upgrade bootloader -U <ftp_path> -u <user> -p <password>`
   Or, interactively,
   `fazbdctl upgrade bootloader`
3. Follow the onscreen instructions to select the source from FTP, SFTP, HTTP or HTTPS, and enter your server URL, upgrade bootloader file's zip file path, and FTP username and password.
4. Wait approximately 30 seconds to a few minutes, and then check the bootloader version using the following command:
   `fazbdctl show version`

9. Extract hardware detailed information by lshw

This command extracts hardware detailed information using the `lshw` command.

10. Check and repair hard drives

This command is used to verify and repair the integrity of file systems on storage devices.

11. Reset root password

This command resets the OS password of this host to the default "`fortinet@123`".

12. Reboot

The Reboot option enables you to reboot and restart the host.

sh. shell

If you enter `sh` into the Bootloader prompt, you can access the shell and use tools under `/sbin/`. For example, you can use `xfs_repair` to fix root disk errors if they occur.

General maintenance and best practices

To ensure that your FortiAnalyzer-BigData appliance runs smoothly, you need to perform regular maintenance tasks and follow best practices guidelines.

Backup and restore to external HDFS

For full instructions on how to backup and restore your data, see Data backup on page 78 and Data restore on page 83.

Schedule maintenance tasks for off-peak hours

Fortinet strongly recommends scheduling maintenance jobs for off-peak hours whenever possible, including jobs such as:

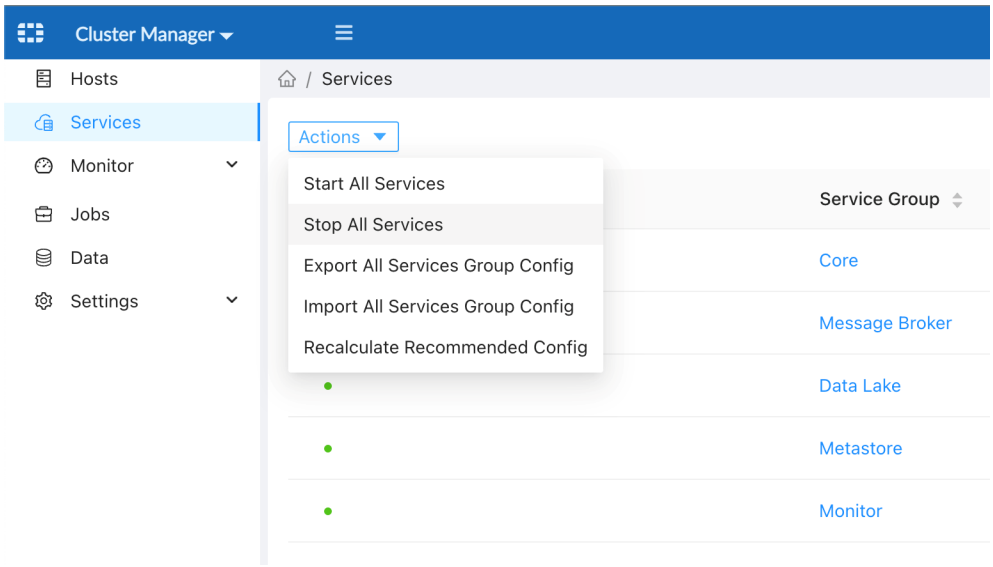
- Storage Pool Backup
- Data Rebalance

Graceful system shutdown

We recommend gracefully shutting down the FortiAnalyzer-BigData services and blades from CMM before a planned power outage in order to help prevent data corruption in the stateful workload and conflicts in the distributed consensus.

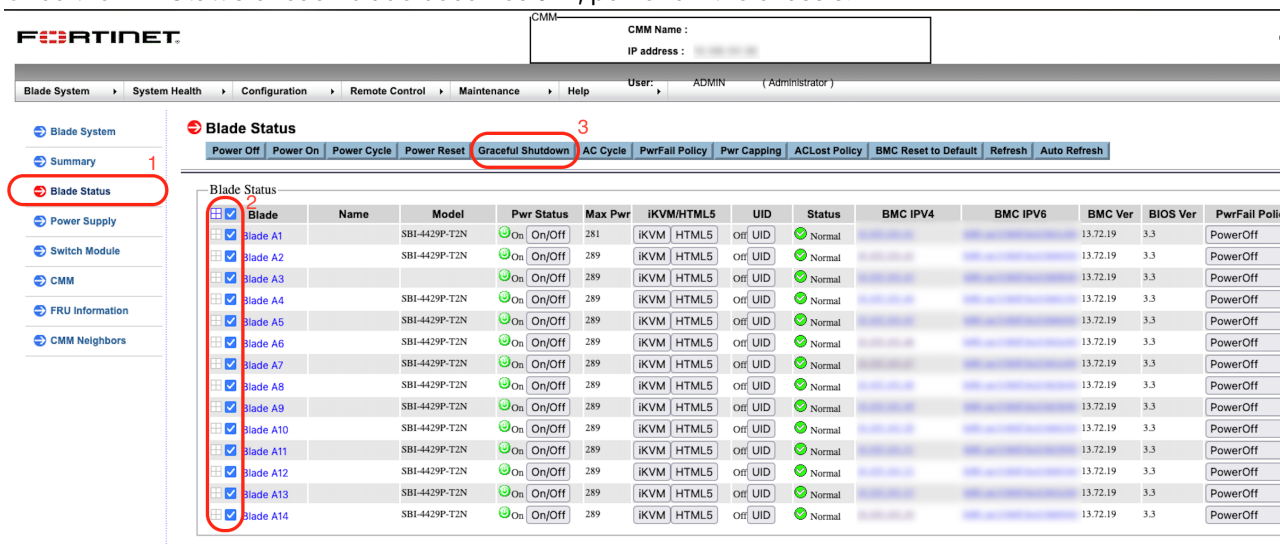
To gracefully shut down the services:

1. Go to *Cluster Manager > Services*.
2. From the *Actions* dropdown, click *Stop All Services*.
   Wait for the *Stop All Services* command to finish before proceeding in the next step to shut down blades from CMM.



To gracefully shut down the blades from CMM for 4500F:

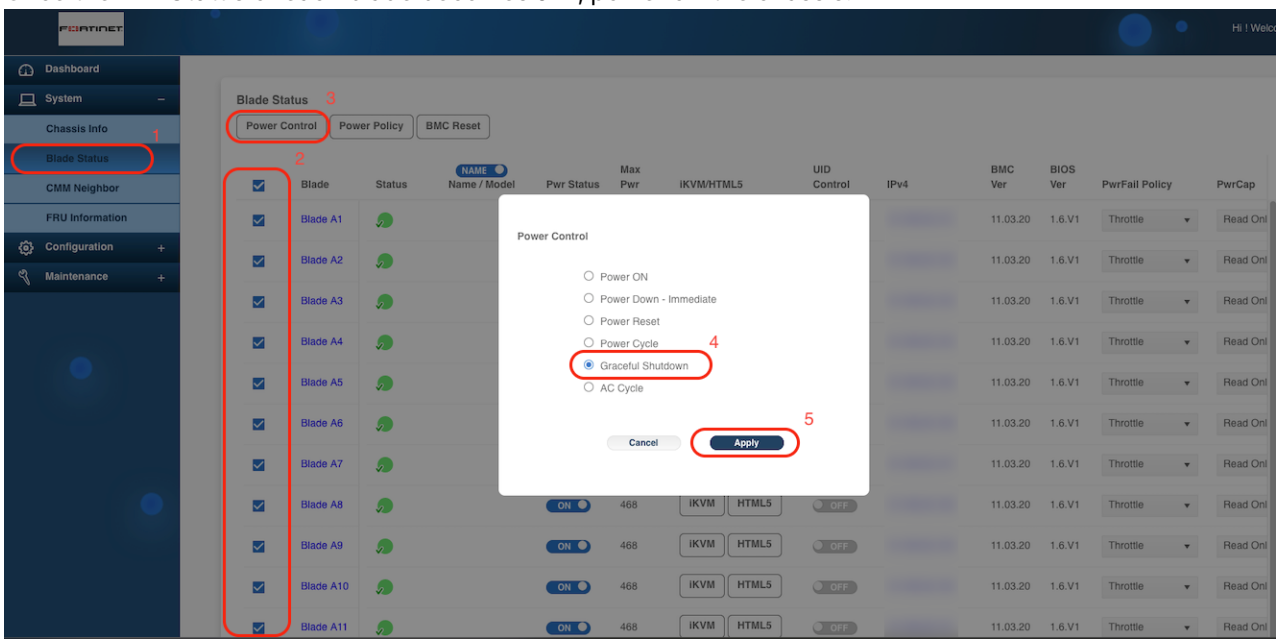
1. Go to *Blade Status*.
2. Select all blades.
3. Click *Graceful Shutdown*.
   Once the *Pwr Status* of each blade becomes `Off`, power off the chassis.



To gracefully shut down the blades from CMM for 4500G:

1. Go to *Blade Status*.
2. Select all blades.
3. Click *Power Control*.
4. In the *Power Control* dialog, select *Graceful Shutdown*.
5. Click *Apply* to start the shut down process.

Once the *Pwr Status* of each blade becomes `Off`, power off the chassis.



Maintain database integrity

To maintain database integrity, never power off a FortiAnalyzer-BigData unit without a graceful shutdown. Removing power without a proper shutdown can damage FortiAnalyzer-BigData databases.

Before removing power, always use the *Stop All Services* action from *Cluster Manager* > *Services* > *Actions*, or manually stop services in the following order:

1. Core
2. Message Broker
3. Data Lake
4. Metastore

After you power up your FortiAnalyzer-BigData unit again, you must manually select the *Start All Services* action from *Cluster Manager* > *Services* > *Actions* and make sure that all hosts, services and health checks are green before resuming system functions.

Fortinet strongly recommends connecting FortiAnalyzer-BigData units to an uninterruptible power supply (UPS) to prevent unexpected power issues that might damage internal databases.

Upgrade FortiAnalyzer-BigData

Before you upgrade FortiAnalyzer-BigData, confirm the following:

- There is an FTP server that the FortiAnalyzer-BigData Security Event Manager Controller can access.
  Put the FortiAnalyzer-BigData image on the FTP server.
- There is a valid NTP connection for FortiAnalyzer-BigData.
  This connection ensures the clock is synchronized across cluster nodes, which is essential for the database's distributed consensus. If the configured NTP server cannot be reached or fails to function, the upgrade will fail.
- You have a designated maintenance period for the upgrade.
  The upgrade takes about 45 minutes. During the upgrade, the GUI is not available. Log collecting, LogView, and FortiView operations are also not available.

It is recommended to perform the upgrade via the GUI.
The upgrade process via the CLI may fail if the SSH connection is disrupted before the Controller hosts reboot during the early upgrade stage.

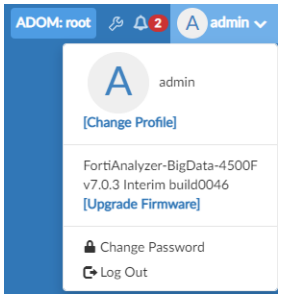
After the upgrade completes, proceed to upgrade bootloader as well. Your version of FortiAnalyzer-BigData bootloader must match your current version of FortiAnalyzer-BigData.
To upgrade the bootloader, see Upgrade Bootloader.

See below for steps:

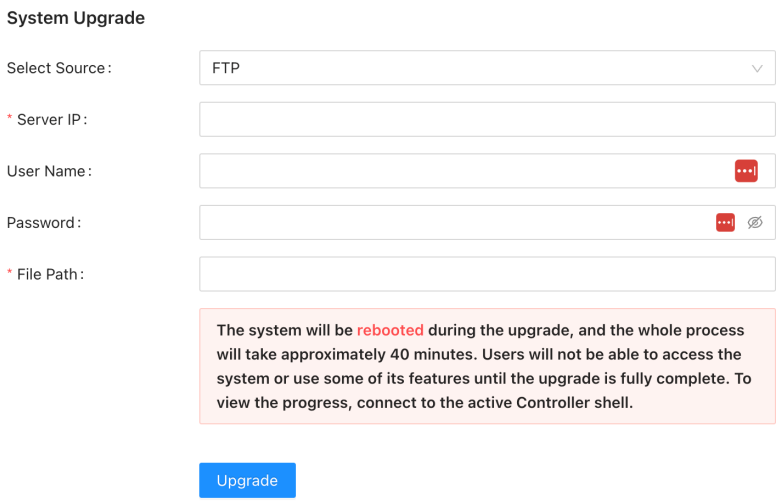
- To upgrade FortiAnalyzer-BigData with the GUI: on page 100
- To upgrade FortiAnalyzer-BigData with the CLI: on page 102

To upgrade FortiAnalyzer-BigData with the GUI:

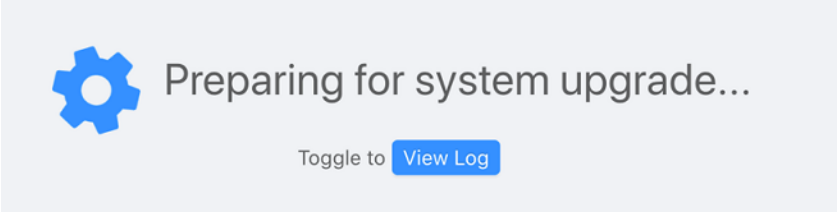
1. Using the Management IP, sign into the FortiAnalyzer-BigData GUI.
2. In the banner, open the Account menu and click *Upgrade Firmware*.



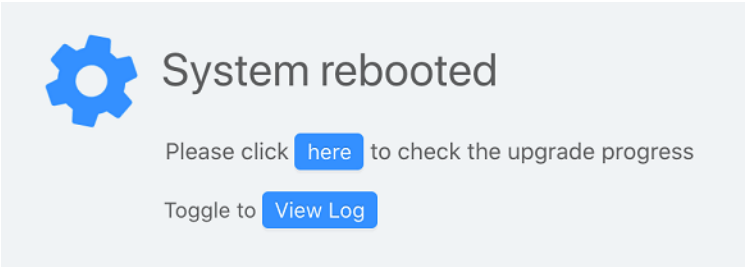
3. Click *Upgrade* to access the System Upgrade dialog box.

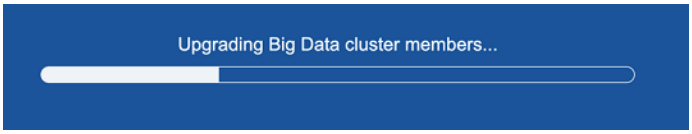


4. From the *Select Source* dropdown, select *FTP*, *SFTP*, *HTTP*, *HTTPS*, or *Upload File*.
5. Enter the source server's IP address, username, password, and file path. Leave the *User Name* and *Password* fields empty if they are not applicable.
6. Click *Upgrade*.
   The system begins to prepare for the upgrade.

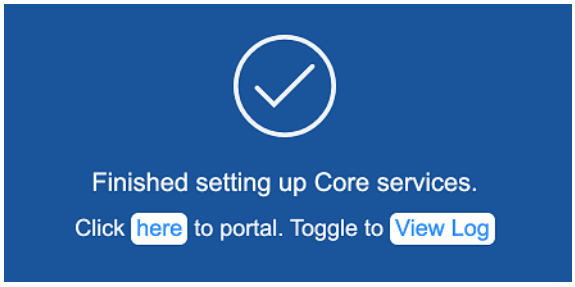


After the system finishes preparing, it loads a new page where you can see the current status and check the upgrade progress.

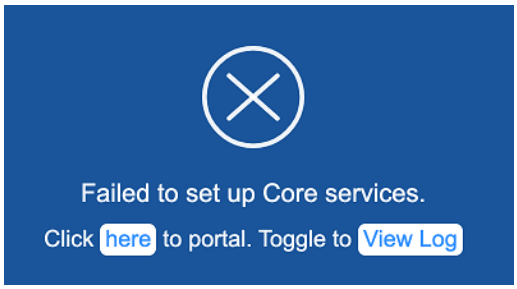




The upgrade takes about 45 minutes. If the upgrade is successful, you see the following message.



7. Click *here* to return to the FortiAnalyzer-BigData portal.
   If the upgrade fails, you see the following message:



   To troubleshoot the problem, see What to do if an upgrade fails on page 116.

To upgrade FortiAnalyzer-BigData with the CLI:

You can also upgrade your FortiAnalyzer-BigData using the `fazbdctl` CLI command on the Security Event Manager Controller.

1. Access the Security Event Manager Controller CLI by establishing an SSH connection to the Cluster Management IP. See Connect to the FortiAnalyzer-BigData CLI on page 12.

   Starting the upgrade process from the Main Host instead of the Security Event Manager Controller may result in upgrade failure.
   If this failure occurs, you must start again with a forced upgrade from the Security Event Manager Controller via SSH connection. Use the `-f` option to perform the forced upgrade. There is no forced upgrade option via the GUI.

2. Run the following command:
   `fazbdctl upgrade cluster -U <ftp_path> -u <user> -p <password>`
   Or, interactively,
   `fazbdctl upgrade cluster`
3. Follow the onscreen instructions to select the source from FTP, SFTP, HTTP or HTTPS, and enter your server URL, upgrade file's zip file path, and FTP username and password.
   The system upgrades the FortiAnalyzer-BigData Main Host and then the Security Event Manager. After a few minutes, the Security Event Manager Controller reboots.
4. After the Security Event Manager Controller reboots, reconnect to it and monitor the broadcast messages for progress.
5. Wait about 45 minutes for the following message to display on the terminal.
   `[100%] The system has been upgraded successfully.`

Downgrading to prior versions of FortiAnalyzer-BigData is not supported.

When an upgrade is in progress, upgrades with the CLI will be blocked from execution with the following error message:

```
Error: Installation Process is already in progress
Lock ID: xxxxxxxxxx
To force unlock the installation process, use command: fazbdadm force-
      unlock-install xxxxxxxxxx
```

The `force-unlock-install` CLI command can be used to force release the upgrade process lock, but it should only be used when the upgrade process stops unexpectedly without releasing the process lock.

Scaling FortiAnalyzer-BigData

Scaling FortiAnalyzer-BigData:

You might need to scale the Security Event Manager of FortiAnalyzer-BigData by stacking multiple FortiAnalyzer-BigData appliances to add more storage and query throughput. For example, if you have an existing deployment and want more disk space to store logs for a longer period of time, you can scale out by adding one or more extender chassis. The log data as well as the computing and stateful workload will be distributed across all the hosts in the stacked appliances.

How to scale out

For FortiAnalyzer-BigData, you can scale out by adding more extender chassis. See To add an extender chassis: on page 104.

To add an extender chassis:

The following operation removes all user data from the extender chassis.

1. Ensure both the main and extender chassis are running the same version. To do this, run the following command:
   ```
   fazbdctl show version
   ```

   Do not connect the links between both chassis until step 2 has been successfully completed; otherwise, it may cause an IP conflict and corruption in the distributed consensus.

2. On the extender chassis, access the *Security Event Manager Controller* and run the following command:
   ```
   fazbdctl set appliance <chassis_id>
   ```
   For information about accessing the Security Event Manager Controller, see To connect to the Security Event Manager Controller: on page 12.

   The chassis ID is an integer starting with 1, where 1 is the default chassis ID of the cluster formed by one chasis.

   If you are adding the first extender to a cluster with one chassis, the *chassis_id* of the extender should be set to *2*. You should increment this *chassis_id* as you stack more chassis to the cluster.

   For example, the second extender's *chassis_id* should be set to *3* before you connect it to a cluster of two chassis. This function updates the chassis id on all hosts, and hard resets the FortiAnalyzer-BigData system.

Wait for the command to finish running without errors before you proceed with the next step.

3. Power off Blade A1 in the extender chassis from CMM.
4. Connect the 40GE links with QSFP between the Internal Switch Modules (Switch Module #1) of the extender and main chassis.
5. On the main chassis, access the Security Event Manager Controller and run the following command to make sure the new hosts have been added:
   ```
   fazbdctl show members
   ```
   There should be 13 additional hosts added as members. Wait until all the hosts' status shows as *Alive*
6. Access the FortiAnalyzer-BigData GUI of the main chassis, and go to *Cluster Manager* > *Hosts*.
7. Click *Assign Role* to assign the newly added hosts.
   New hosts should have a *New* label.
8. Wait for the *Assign* job to complete for all services to become healthy.
9. Follow the *Found New recommended configurations* notification on the *Cluster Manager* > *Hosts* view to apply the optimized configuration for the newly added hosts.
10. (Recommended) To add an extender chassis after scaling out, rebalance the data across the cluster. See How to rebalance the data on page 120.

How to remove a chassis from a stacked setup

If you have an established multi-chassis FortiAnalyzer-BigData Security Event Manager and need to scale down, you can remove any extender chassis you have added to the main chassis.

Removing an extender chassis will hard reset BOTH the extender and the main chassis. All user data and configurations will be lost. The entire process takes approximately an hour.

Remove an extender chassis

Perform this process in a location where you can immediately disconnect the Internal Switch Modules at step 3. This step must be done in a timely manner.

To remove an extender chassis:

1. Reset all hosts connected to the current controller. To do this, access the Security Event Manager Controller of the main chassis and run the following command:
   ```
   fazbdctl unstack-chassis
   ```
   For information about accessing the Security Event Manager Controller, see To connect to the Security Event Manager Controller: on page 12.
   Wait for the message "`[Info] factory reset members done, and [info] factory reset the controller`" in the command output before proceeding to the next step without any delay.

2. Disconnect the connection between the *Internal Switch Modules* (Switch Module #1) between the main and extender chassis.
3. On the main chassis, access the *Security Event Manager Controller*.
   a. Access the Bootloader of the active controller. See Bootloader on page 90.
   b. From Bootloader, select option 7, *Reset OS and Clear User Data*, to hard reset the host.
   c. Wait until the Bootloader finishes rebooting and log back into the controller.
   d. Initialize the cluster using the following command:
      ```
      fazbdctl init cluster
      ```
   e. Configure the management IP and main host IP.
      For more information about setting up the network, see the Getting Started Guide for your device on the Fortinet Document Library.
4. On the extender chassis, access Blade A2.
   a. Access the Bootloader of the Blade A2. See Bootloader on page 90.
   b. From Bootloader, select option 3, *Set Role, input choice: Controller*, to set the role to *Controller*.
   c. From Bootloader, select option 7, *Reset OS and Clear User Data*, to hard reset the host.
   d. Wait until the Bootloader finishes rebooting and log back into the controller.
   e. Initialize the cluster by running the following command:
      ```
      fazbdctl init cluster
      ```
   f. Configure the management IP and main host IP.
      For more information about setting up the network, see the Getting Started Guide for your device on the Fortinet Document Library.

Reset FortiAnalyzer-BigData

This section contains information on how to reset FortiAnalyzer-BigData. There are two ways to perform a reset:

- Soft reset FortiAnalyzer-BigData on page 107
- Hard reset FortiAnalyzer-BigData on page 108

Soft reset FortiAnalyzer-BigData

You can try to soft reset your FortiAnalyzer-BigData Security Event Manager to recover from a system level failure. This process takes about 45 minutes.

Soft reset does the following:

- Reset the OS partition on each of the hosts while keeping all data volume intact.
- Reset the FortiAnalyzer-BigData power.
- Align all the host OS.

To soft reset FortiAnalyzer-BigData:

Before proceeding with the steps below, your version of FortiAnalyzer-BigData bootloader must match your current version of FortiAnalyzer-BigData. Check the version of your bootloader and upgrade it to match your FortiAnalyzer-BigData as needed.

To check the bootloader version, run the following command from the *Security Event Manager Controller*: `fazbdctl show version`

To upgrade the bootloader, see Upgrade Bootloader.

1. Access the Security Event Manager Controller (see To connect to the Security Event Manager Controller: on page 12) and run the following command:
   `fazbdctl reset cluster`
   For more information and additional CLI options, see the `reset` command in the CLI Reference in the Fortinet Doc Library.
   The Security Event Manager Controller will reboot after a few minutes.
2. Reconnect to the Security Event Manager Controller after it reboots and monitor the broadcast messages for progress.
3. Wait about 45 minutes until the following message is displayed on the terminal:
   `[100%] The system has been upgraded successfully.`

Hard reset FortiAnalyzer-BigData

Improperly resetting your FortiAnalyzer-BigData may result in losing all data.

When you hard reset your device, the command resets the OS on each host and formats all data drives. All log data and configurations will be lost. FortiAnalyzer-BigData shuts down during the reset process. The entire process takes approximately 45 minutes.

You can add an extra option to the reset command to keep certain configurations constant:

- `all-settings` resets all settings.
- `all-except-ip` keeps the public IP constant
- `all-except-ip-ssh` keeps the ssh public key constant.
- `all-except-ip-ssh` keeps the ssh public key and public IP constant.

For more information about extra CLI options, see the `reset` command in the CLI Reference in the Fortinet Doc Library..

To hard reset your FortiAnalyzer-BigData:

Before proceeding with the steps below, your version of FortiAnalyzer-BigData bootloader must match your current version of FortiAnalyzer-BigData. Check the version of your bootloader and upgrade it to match your FortiAnalyzer-BigData as needed.

To check the bootloader version, run the following command from the *Security Event Manager Controller*: `fazbdctl show version`

To upgrade the bootloader, see Upgrade Bootloader.

1. Access the Security Event Manager Controller, and run the following command:
   `fazbdctl reset cluster [--all-settings|--all-except-ip|--all-except-ssh|--all-except-ip-ssh]`
   The Security Event Manager Controller reboots after a few minutes.
2. After the Security Event Manager Controller reboots, re-connect to it and run the following command to verify that all members are detected and that the version is up-to-date:
   `fazbdctl show members`
3. After verifying that all the members have a *Joined* state and status is not failed, run the following command to initialize the Security Event Manager:
   `fazbdctl init cluster`
4. Wait about 45 minutes until the following message is displayed on the terminal:
   `[100%] The system has been initialized successfully.`

Data-at-rest encryption on FortiAnalyzer-BigData 4500F

The FortiAnalyzer-BigData 4500F offers data-at-rest encryption support to enhance the security of log data stored in the system. By leveraging Linux Unified Key Setup (LUKS) and dm-crypt, it encrypts all data disk partitions on the cluster hosts while no changes are required on the application logic or schema. This ensures that the log data remains protected and inaccessible even if unauthorized access to the physical storage is obtained. This encryption is managed through a cluster-level passphrase that provides consistency and simplifies administration.

Consider the following limitations to make an informed decision regarding the implementation of data-at-rest encryption in your FortiAnalyzer-BigData 4500F:

- The Main host blade does not undergo encryption, which means that raw logs may be buffered in the FAZ blade for a short period.
- Only the data disks of the Security Event Manager cluster hosts can be encrypted. The OS boot drive, which solely contains binaries, scripts, and server logs, is not encrypted.
- Enabling encryption necessitates re-formatting of the partitions. This process can only be performed during a fresh installation or a hard reset.
- No reversal of encryption once enabled. Once encryption is enabled, there is no way to revert it unless a factory reset is performed.

We strongly suggest you save the passphrase in a secure place. If the passphrase is lost and the encrypted volume is inactive (luks closed), data in the encrypted volumes will no longer be accessible.

Enabling data-at-rest encryption may lead to a performance degradation: a 17% slower disk I/O performance based on our lab test. However, the overall impact on performance may not be significant (< 10%) as most workloads are not heavily dependent on disk I/O.

Initialize data-at-rest encryption

Data-at-rest encryption can only be performed during a fresh installation or after a factory reset.

To initialize data-at-rest encryption as part of a factory reset, you must execute the `init` command with `--encrypt-data-disks`. See the steps below.

To initialize data-at-rest encryption as part of a factory reset:

1. Access the Security Event Manager Controller, and run the following command:
   `fazbdctl reset cluster [--all-settings|--all-except-ip|--all-except-ssh|--all-except-ip-ssh]`
   The Security Event Manager Controller reboots after a few minutes.
2. After the Security Event Manager Controller reboots, re-connect to it and run the following command to verify that all members are detected and that the version is up-to-date:
   `fazbdctl show members`
3. After verifying that all the members have a *Joined* state and status is not failed, run the following command:
   `fazbdctl init cluster --encrypt-data-disks`
4. Follow the prompt to set a passphrase. Record the passphrase in a secure place and follow the remaining reset steps to complete initializing the cluster.
   See Hard reset FortiAnalyzer-BigData on page 108.

Open encrypted data disk partitions

This topic contains examples of opening the encrypted data disk partitions in the following scenarios:

- After a blade power cycle
- After a graceful chassis power cycle
- When performing an upgrade or soft reset
- When scaling out the cluster or replacing a blade

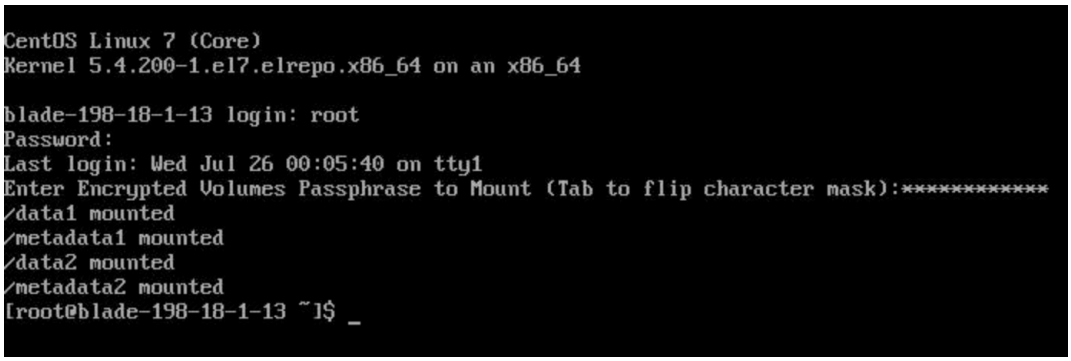
After a blade power cycle

Every time the FortiAnalyzer-BigData OS boots up after a planned or unplanned power cycle, you need to open the encrypted data disk partitions with your passphrase.

There are two methods to open them.

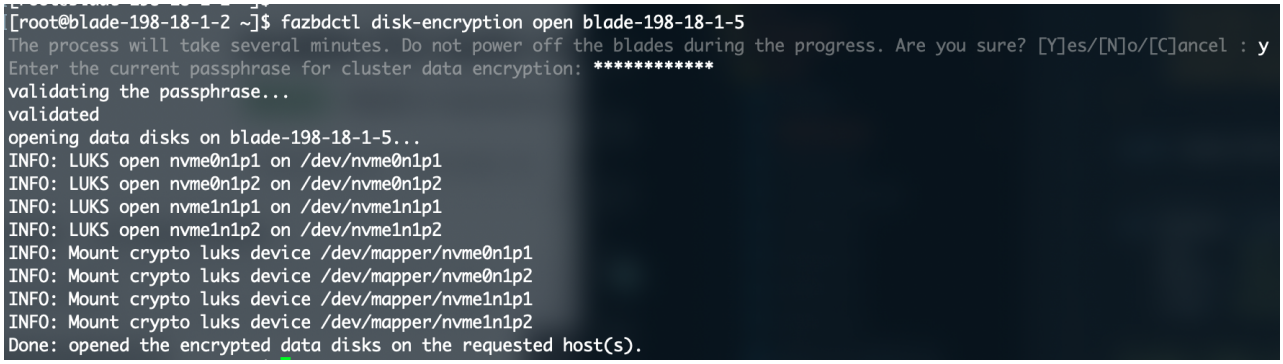
To open the encrypted data disk partitions via the BMC remote console:

1. Access the BMC remote console of the restarted blade.
2. Log in to the OS using root credentials.
3. Follow the prompt to enter the cluster encryption passphrase for opening the data disk partitions.



To open the encrypted data disk partitions via the Controller shell:

1. Connect to the Controller shell.
2. Utilize the `fazbdctl disk-encryption open {host}` command to open the encrypted disk partitions on the restarted blade.



After a graceful chassis power cycle

To open the encrypted data disk partitions after a graceful chassis power cycle:

1. Follow steps to gracefully shut down services in the GUI.
   Go to *Cluster Manager* > *Services* > *Actions* > *Stop All Services*, and then power off the blades.
   See steps to perform a graceful system shutdown in General maintenance and best practices on page 97.
2. Once the chassis (including all blades) is powered on again, the web GUI will display the Setup Wizard upon opening.

3. Follow the instructions to connect to the Controller shell and open the encrypted disk partitions. See To open the encrypted data disk partitions via the Controller shell: on page 111.
4. Once the data disk partitions are opened, proceed with the Setup Wizard GUI to start all services.

When performing an upgrade or soft reset

To open the encrypted data disk partitions during an upgrade or soft reset:

1. Follow steps to perform a system upgrade or soft reset.
   For steps to upgrade, see Upgrade FortiAnalyzer-BigData on page 100.
   For steps to soft reset, see Soft reset FortiAnalyzer-BigData on page 107.
2. After completing the pre-upgrade phases, the Controller will reboot and start to sync all members.
   Once the members have re-joined, the upgrade process will pause for you to open the encrypted data disk partitions.
3. To proceed, reconnect to the Controller shell and follow the message prompts to open the encrypted disk partitions on all cluster hosts.
   Once the encrypted disk partitions are opened, the upgrade will continue automatically.

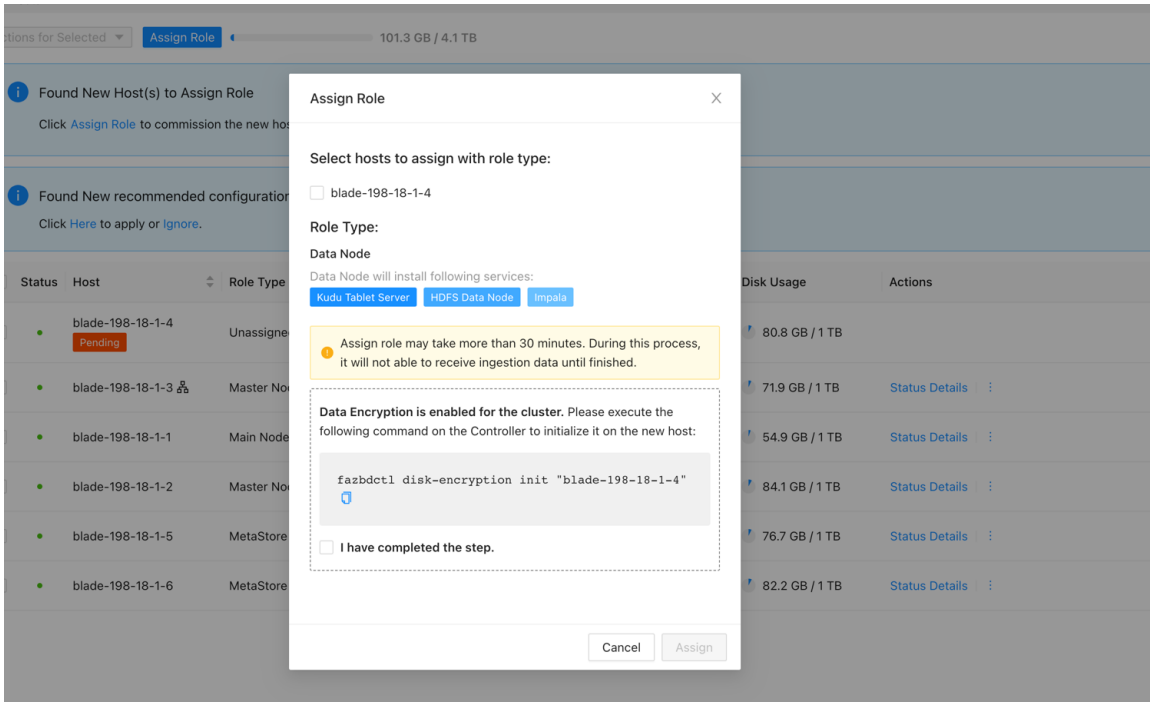
```
[40%] Upgrade/Reset progress has been paused due to data encryption. Please execute [fazbdctl disk-encryption open all] to continue the progress.


[root@blade-198-18-1-2 ~]$ fazbdctl disk-encryption open all
The process will take several minutes. Do not power off the blades during the progress. Are you sure? [Y]es/[N]o/[C]ancel : y
Enter the current passphrase for cluster data encryption: ***********
validating the passphrase...
validated
opening encrypted data disks on 198.18.1.10...
opening encrypted data disks on 198.18.1.11...
opening encrypted data disks on 198.18.1.12...
opening encrypted data disks on 198.18.1.13...
opening encrypted data disks on 198.18.1.2...
opening encrypted data disks on 198.18.1.3...
opening encrypted data disks on 198.18.1.4...
opening encrypted data disks on 198.18.1.5...
opening encrypted data disks on 198.18.1.6...
opening encrypted data disks on 198.18.1.7...
opening encrypted data disks on 198.18.1.8...
opening encrypted data disks on 198.18.1.9...
```

When scaling out the cluster or replacing a blade

To open the encrypted data disk partitions when scaling out or replacing a blade:

1. Follow steps to scale out or replace a blade.
   For steps to scale out, see How to scale out on page 104.
   For steps to replace a blade, see How to replace a blade on a FortiAnalyzer-BigData appliance on page 118.
2. During the step to Assign Role for the blade, a confirmation prompt will appear in the GUI. This prompt will provide instructions on how to initialize data encryption on the new or replaced host(s).



3. Follow the instructions provided in the prompt to connect to the Controller shell and initialize the encrypted disk partitions on the new or replacement host(s). For example, connect to the Controller shell and enter the following command: `fazbdctl disk-encryption init {host}`.
   Once completed, you can proceed with the Assign Role process.

If the step to initialize the encrypted disk partitions is missed, the Assign Role task will fail during the pre-flight check.

Troubleshooting

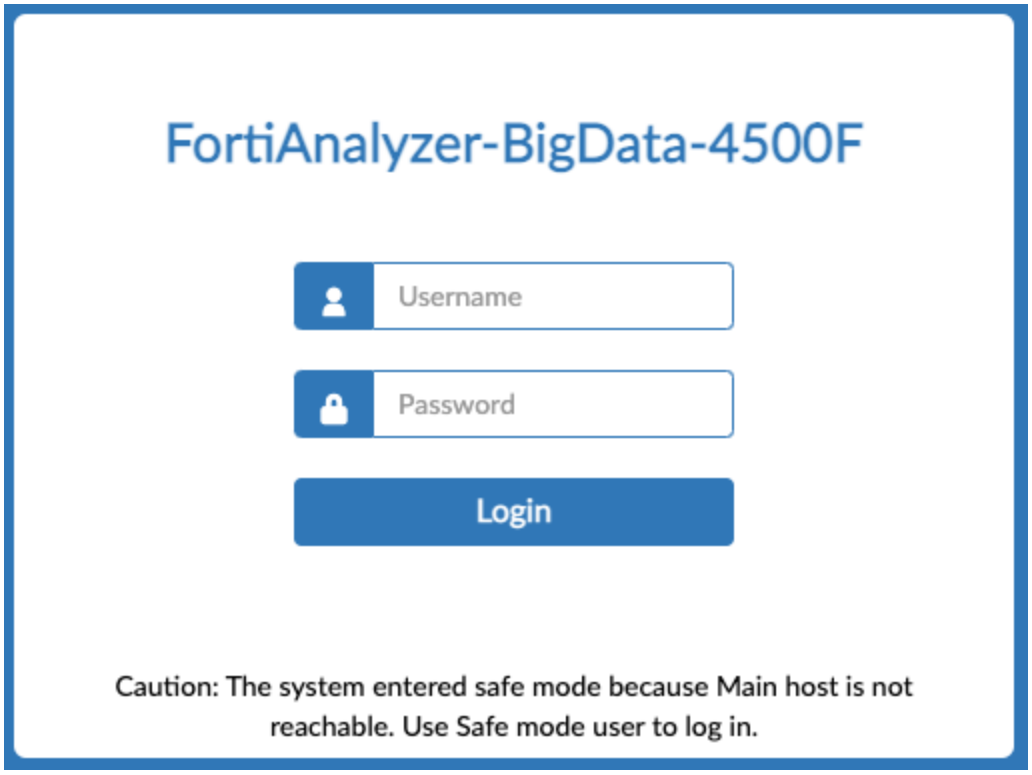
This section contains troubleshooting tips for issues you might encounter when working with FortiAnalyzer-BigData.

Safe Mode

The FortiAnalyzer-BigData web GUI will enter *Safe Mode* when the Main host becomes unhealthy or unreachable from the Security Event Manager. This can be caused by a loss of power to the Main host, hardware failure, network segregation, Main host OS crash, etc. Once in Safe Mode, only Global Search and Cluster Manager are accessible. The other tiles on the home page are grayed out.

To log in to FortiAnalyzer-BigData in Safe Mode, enter the Username `admin` and no password. You will be prompted to change the password the first time you log in.

For example, see the image below from a FortiAnalyzer-BigData 4500F GUI.



FortiAnalyzer-BigData will exit Safe Mode once the Main host is healthy again.

What to do if an upgrade fails

An upgrade might fail with the following error conditions:

Error condition	Troubleshooting suggestion
An error message displaying: • "get image failed" • "could not find image"	Make sure image from the hosting server is accessible.
An error message displaying: • "checksum verification failed"	Check the image file integrality.
The Security Event Manager Controller cannot boot up after an upgrade and you cannot connect to the Security Event Manager Controller	Perform the following steps: 1. Access the bootloader of the Security Event Manager Controller (see Bootloader on page 90). 2. Select the "Backup" option to restore the last working OS image to the system.

The upgrade fails after several retries, and one or more hosts remain stuck in the “upgrading” or "joining" state in the fazbdctl show member output	1. Check blade power status in the Chassis Management Module (CMM).
	• Access the CMM GUI and confirm the blade’s power status is green.
	• If the blade’s power status is red, perform an AC Cycle:
	  • In CMM GUI > *Blade Status*, select the blade.
	  • Under *Power Control*, click *AC Cycle*.
	2. Check the health of the blade via the Blade Management Console (BMC).
	• In CMM GUI, go to *Blade System* > *Blade Status*, in the *Blade* column, click on the blade with the issue, and open the “*Health Event Log*” tab in the “*Blade Info*” selection.
	• Access the BMC remote console of the problematic blade. Verify if the console reports any errors (for example, disk corruption).
	• If needed, try a *Power Cycle*:
	  • In CMM GUI > *Blade Status*, select the blade.
	  • Under *Power Control*, click *Power Cycle*.
	3. (4500G only) Reset the BMC if the GUI becomes unresponsive.
	• If the BMC GUI or Remote Console is not responding, but the IP is reachable, perform a BMC Reset:
	  • In CMM GUI > *Blade Status*, select the blade.
	  • Under *Power Control*, click *BMC Reset*.

You can also retry a failed upgrade by using the option flag `-o` in the upgrade command.

Enter the following command to retry upgrading from where it fails:

```
fazbdctl upgrade cluster -o retry
```

What to do if a soft reset fails

A soft reset might fail with the following error conditions:

Error condition	Troubleshooting suggestion
An error message displaying: • "checksum verification failed" • "could not find image"	Perform an upgrade with the image of the intended version or latest version.
The Security Event Manager Controller cannot boot up after an upgrade and you cannot connect to the Security Event Manager Controller	Perform the following steps: 1. Access the bootloader of the Security Event Manager Controller (see Bootloader on page 90). 2. Select the "Backup" option to restore the last working OS image to the system. 3. Access the Security Event Manager Controller and perform an upgrade via `fazbdctl` CLI commands (see Upgrade FortiAnalyzer-BigData on page 100) with the image of the intended version or latest version. 4. Rerun the reset command to perform a soft reset.

You can also retry a soft reset by using the option flag (`-o`) in the rest command:

- Enter the following command to retry soft reset on the cluster from where it fails:
  `fazbdctl reset cluster -o retry`
- Or enter the following command to retry soft reset on the cluster from the very beginning:
  `fazbdctl reset cluster -o restart`

What to do if a hard reset fails

A hard reset might fail with the following error conditions:

Error condition	Troubleshooting suggestion
The reset failed to complete before the Security Event Manager Controller reboots	Upgrade the system to latest version (see Upgrade FortiAnalyzer-BigData on page 100) and then try resetting again.
The Security Event Manager Controller cannot start or the system is not accessible after a hard reset.	Perform the following steps: 1. Access the bootloader of the Security Event Manager Controller (see Bootloader on page 90). 2. Select the "Backup" option to restore the last working OS image to the system.

Error condition	Troubleshooting suggestion
	3. Access the Security Event Manager Controller and perform an upgrade via `fazbdctl` CLI commands with the image of the intended version or latest version. 4. Rerun the reset command to perform a hard reset.

How to repair disk failures

If you see a "disk failure" message is any system logs, it might indicate that the FortiAnalyzer-BigData is experiencing hard disk issues. You can try to repair these issues using software methods.

To repair disk failure issues:

1. Access the bootloader of the host that has disk failure symptoms (see Bootloader on page 90).
2. From the bootloader, enter `sh` to enter the shell.
3. In the shell, run `xfs_repair` to fix the hard disk issue.

If the problem persists after running the software fix, you may need to replace the hard disk.

How to replace a blade on a FortiAnalyzer-BigData appliance

This section contains instructions on how to gracefully remove and replace a malfunctioning hardware blade running one of the hosts in an active system. In order to allow the high availability mechanism to take effect, only one blade can be decommissioned at a time.

Finding a blade's location

A blade's host name uses the following naming convention:

```
blade-198-18-{chassis ID}-{blade ID}
```

For example, in a blade named *blade-198-18-1-3*, the number *1* represents the `chassis ID` and *3* represents the `blade ID`. Therefore, the blade is the third blade to the left on the first chassis. The internal IP of the blade is *198.18.1.3*.

To replace a blade:

Before proceeding with the steps below, your version of FortiAnalyzer-BigData bootloader must match your current version of FortiAnalyzer-BigData. Check the version of your bootloader and upgrade it to match your FortiAnalyzer-BigData as needed.

To check the bootloader version, run the following command from the *Security Event Manager Controller*: `fazbdctl show version`

To upgrade the bootloader, see Upgrade Bootloader.

1. Power off the malfunctioned blade, and then remove the blade from the chassis.
2. From *Security Event Manager Controller* run the following command to enable installation of system software on the new blade: `fazbdctl decommission <host name or blade IP of the blade to replace>`

   If the replacement blade already has FortiAnalyzer-BigData firmware image installed (for example, if the blade was previously used in another chassis), you must perform a wipe before proceeding. This ensures the Controller can properly initialize and provision the blade.

   To perform a wipe:

   1. Insert and power on the replacement blade. Enter the BMC Web Console to prepare for the bootloader operations. See Bootloader on page 90.
   2. When the "FAZBD Boot Menu" appears during boot, immediately press the Arrow key to enter the Bootloader menu. Do not allow the blade to boot into the OS.
   3. At the Bootloader prompt, type "`wipe`" and press Enter. Confirm the operation.
   4. After the wipe, the blade will automatically PXE boot from the Controller for reinstallation. Continue with the remaining steps to finish the replacement.
3. Insert the replacement blade, and power it on.
4. Monitor the status of the blade from CMM. See *Remotely control blades via CMM* in the FortiAnalyzer-BigData Getting Started Guide for your appliance: 4500F or 4500G.
   Wait until the host OS completes booting. This may take 5-10 minutes.
5. After the host boots up and joins the cluster, it will appear in *Cluster Manager > Hosts* web GUI.
6. Go to *Cluster Manager > Hosts* and click *Assign Role* to recover the host. The new host will have a *pending* status.
7. Wait for the *Assign job* to complete for all services to become healthy.
8. Follow the *Found New* recommended configurations notification in the *Cluster Manager > Hosts* view (if it appears) to apply the optimized configuration for the newly added hosts.
9. (Recommended) After the *Assign Role* job is complete, rebalance the data across the cluster. See How to rebalance the data on page 120.

How to reset a single host

This section contains instructions on how to gracefully reset a software malfunctioned host in a running system. In order to allow the high availability mechanism to take effect, only one host can be reset at a time.

Finding a blade's location

A blade's host name uses the following naming convention:

```
blade-198-18-{chassis ID}-{blade ID}
```

For example, in a blade named *blade-198-18-1-3*, the number *1* represents the `chassis ID` and *3* represents the `blade ID`. Therefore, the blade is the third blade to the left on the first chassis. The internal IP of the blade is *198.18.1.3*.

To reset a single host:

1. Access the bootloader of the malfunctioned host (see Bootloader on page 90), enter the Reset OS option and wait until it finishes rebooting.
2. Monitor the status of the blade or host.
   a. If it is a FortiAnalyzer-BigData unit, monitor the status of the blade from the DMM. See *Remotely control blades via CMM* in the FortiAnalyzer-BigData Getting Started Guide for your appliance: 4500F or 4500G.
   Wait until the host OS completes booting. This may take 5-10 minutes.

   Cluster failover

   When resetting the *Controller* host, allow up to 15 minutes for the failover mechanism to take effect. Once the mechanism is in effect, the *Security Event Manager IP* and *Cluster Manager* can be accessed with the GUI.
3. After the host reboots and joins the cluster, it will appear in *Cluster Manager > Hosts*.
4. From the *Hosts* page, click *Assign Role* to recover the role on the host. The new host should display a *pending* label. When the *Assign Role* job is complete, the host reset is done.
5. (Recommended) After the *Assign Role* job is completed, rebalance the data across the cluster. See How to rebalance the data on page 120

How to rebalance the data

This topic contains instructions on how to rebalance the data across the *Security Event Manager* hosts. The data is balanced automatically by default. However, in the circumstances such as a host failure, reset, or replacement, data may get skewed. The *Data balance Check* in *Cluster Manager > Monitor > Health* periodically checks for data balance and fails if the data skews high. The built-in *Data Rebalance (All)* job can be used to rebalance the data.

Maintenance window

By default, the data will be unavailable during the run to ensure data integrity. Choose a maintenance window when the log receiving rate is low.

To rebalance the data:

1. Go to *Cluster Manager* > *Jobs* and click *Create Custom Job*.
2. Select *Data Rebalance (All)* and *Schedule "Manual"*, then click *Create*.
3. In the *Jobs* table, locate the *Data Rebalance (All)* row, and click *Run in Actions*. Allow approximately 1 hour for the job to execute, depending on the data size.
4. After the job is finished, go to *Cluster Manager* > *Monitor* > *Health*. If the *Data balance Check* status is *Failed*, click *Run Test* to rerun the test. Ensure the test status is *Success*.

How to recover from an unhealthy service status

The services in the Security Event Manager are highly available and fault tolerant with data are replicated three times into different data hosts. If any one of the BigData hosts goes down, you can expect some service degradation (such as dropped insert rate and query performance), but all basic functionalities (such as FortiView, and LogView) are preserved with no data loss. While the system is mostly self-healing from failures, manual operation is required to address certain failure incidents.

The Monitor page contains tools to help you monitor the status and health of the hosts and services (see Monitor on page 26). We suggest scheduling a routine monitoring and maintenance window, and set up system alerts to enable rapid remediations and fault prevention. If you need to shut down your FortiAnalyzer-BigData, follow the best practices (see General maintenance and best practices on page 97 to avoid damaging your database.

Stateful workloads occasionally require manual responses to recover from incidents. When unhealthy workloads are detected, check the status of all BigData hosts to ensure they are all functioning. In general, you should address host-level incidents first before going into the service level.

The following sections contain troubleshooting tips for when FortiAnalyzer-BigData services have an unhealthy status.

Core services

Core / Query

If Query service is unhealthy, or if FortiView or LogView stops working, you can try the following:

1. From *Cluster Manager* > *Services*, check if the Data Lake service group is healthy, if not, fix it first.
2. From *Cluster Manager* > *Services* > *Core*, manually restart the Query service, and then wait a few minutes to see if the issue is fixed.

Core / Ingestion

If the Ingestion service is unhealthy, or if the log insert rate remains at zero while receiving rate is higher, you can try the following:

1. From *Cluster Manager* > *Services*, check if the Message Broker service group is healthy, if not, fix it first.
2. In *Cluster Manager* > *Services* > *Core*, manually *Restart* the Ingestion service, and then wait a few minutes to see if the issue is fixed.
3. If the issue persists after the restart, go to *Cluster Manager* > *Jobs* > *Create Custom Job*, and select *Kafka Deep Clean* as the template.
4. Find the newly created "Kafka Deep Clean" job in the job list and click *Run*.

This will purge all the data in the queue and a start a fresh Pipeline. Any unprocessed data will be lost.

Core / Pipeline

If the Pipeline service is unhealthy, or if the Pipeline Health Check in *Monitor* > *Health* remains unhealthy for hours, you can try the following:

1. In *Cluster Manager* > *Services*, check if the Data Lake and Message Broker service groups are healthy, if not, fix them first.
2. In *Cluster Manager* > *Services* > *Core*, manually restart the Pipeline service, and then wait a few minutes to see if the issue is fixed.
3. If the issue persists after a few hours, go to *Cluster Manager* > *Jobs* > *Create Custom Job* and select *Purge Data Pipeline* as the template.
4. Find the newly created "Purge Data Pipeline" job in the job list and click *Run*.

This will purge all the data in the queue and start a fresh Pipeline. Any processed data will be lost.

Data Lake services

Data Lake / Impala

If the Impala service is unhealthy, you can try the following:

1. Check if the Metastore service group is healthy, if not, fix it first.
2. From *Cluster Manager* > *Services* > *Data Lake*, manually *Restart* the Impala service and wait a few minutes to see if the issue is fixed.

Data Lake / Kudu

If the Kudu service is unhealthy, you can try the following:

1. From *Cluster Manager* > *Services*, manually *Stop* the Core service group.
2. Check if the Metastore service group is healthy, if not, fix it first.

3. From *Cluster Manager > Services > Data Lake*, manually *Restart* the Kudu service and wait a few minutes to see if the issue is fixed.
4. If the issue persists after the restart and the log indicates that Kudu failed to synchronize time, go to *Cluster Manager > Jobs > Create Custom Job* and select *NTP Sync* as the template.
5. Find the newly created *NTP Sync* job in the job list and click *Run*.
6. After the job finishes running, manually *Start* the Kudu service again to see if the status becomes healthy.
7. Once the Kudu service is healthy, manually *Start* the Core service group again.

If the Database Health Check in *Monitor > Health* remains unhealthy for hours but the Kudu service status is healthy, you can try the following:

The Database Health Check may temporarily fail when the Storage Pool Restore or Data Rebalance job is running. Once the jobs are finished running, the status will automatically clear. Make sure those jobs are not running before troubleshooting.

1. From *Cluster Manager > Services*, manually *Stop* the Core service group.
2. Wait about 15 minutes and then navigate to *Monitor > Health* to rerun the Database Health Check.
3. If the health check returns as healthy, return to the Services page to manually *Start* the Core service group.

Data Lake / HDFS

If the HDFS service is unhealthy, or if the HDFS related Health Checks in *Monitor > Health* are remains, you can try the following:

1. From *Cluster Manager > Services > Data Lake*, manually *Restart* the HDFS service, and then wait a few minutes to see if the status changes to healthy.
2. If the issue persists after restart and the logs indicate the HDFS is in safe mode, go to *Cluster Manager > Jobs > Create Custom Job* and select *HDFS Safemode Leave* as the template.
3. Find the newly created "HDFS Safemode Leave" job in the job list and click *Run*.

Message Broker services

Message Broker / Kafka

1. If the Kafka service is unhealthy, you can try the following:
2. From *Cluster Manager > Services*, manually *Stop* the Core service group.
3. Go to *Cluster Manager > Services > Message Broker*, and manually *Restart* the Kafka service and check that the status becomes healthy.
4. If the issue remains after the restart, go to *Cluster Manager > Jobs > Create Custom Job* and select *Kafka Deep Clean* as template.
5. Find the newly created "Kafka Deep Clean" job in the job list and click *Run*.

This will purge all the data in the queue and start a fresh Pipeline. Any processed data will be lost.

6. Return to *Cluster Manager > Services* and manually *Start* the Core service group.

How to recover from a full disk

The FortiAnalyzer-BigData data life cycle can be managed via Cluster Manager GUI (see Manage storage policy on page 77). If the data disk on your hosts begin to reach full capacity and are causing the Data Lake services to become unhealthy, you can do the following:

1. From *Cluster Manager > Services*, manually *Stop* the Core service group except the catalog service. The catalog service needs to continue running.
2. Go to *Cluster Manager > Data*, expand the *Root* Storage Pool and click *Action > Manage Data Lifecycle*.
3. In the *Maximum Age* field, reduce the number of days for storing data and click *OK*.
4. Go to *Cluster Manager > Jobs*, and locate and *Run* the Data Retention job in the job list.
5. Wait a for the Data Retention job to finish running.
6. From *Cluster Manager > Services > Data Lake*, manually *Restart* the Kudu service.
7. Check that the Kudu service has a healthy status.
8. If you still receive messages about the disk being full in the log, you might need to repeat steps 4-6.
9. When you stop receiving messages, go to *Cluster Manager > Services* and manually *Start* the Core service group.

How to fix Kudu metadata corruption

In rare situations, the Kudu tablet consensus may break and the metadata may corrupt, such as when an ungraceful host is powered off. When this occurs, *Monitor > Health > Database Health Check* will fail and report table conflict, unavailable, or under-replicated in the check result.

Example 1:

```
Tablet fcdb22e988f54674bf7bd81957d96d99 of table db_log_public.__root_fgt_hyperscale is conflicted:
      1 replicas' active configurations disagree with the leader master's:
   69c7e95e57f748bd801be9562db9684e (blade-10-0-1-6:7050): RUNNING
   538735a93bb8421b8fc2794fb31c52a7 (blade-10-0-1-5:7050): RUNNING
   077b5c932f2e4266820d13fb23442964 (blade-10-0-1-7:7050): RUNNING [LEADER]
All reported replicas are:
   A = 69c7e95e57f748bd801be9562db9684e
   B = 538735a93bb8421b8fc2794fb31c52a7
   C = 077b5c932f2e4266820d13fb23442964
   D = d06a84c881704e5d9f363a77cfd721d5
```

Example 2:

```
Tablet 13762b6c83fa4e18843bdabccb4ecdc6 of table 'db_log_public.__kavsprwq_fgt_traffic' is
      unavailable: 2 replica(s) not RUNNING
   2504215476754ff59ad3f0fcb0d58355 (blade-198-18-1-9:7050): RUNNING
   04735952e86f4a4a98f748d1c2546fd8 (blade-198-18-1-8:7050): not running [LEADER]
      State: FAILED
      Data state: TABLET_DATA_READY
      Last status: Corruption: Failed log replay. Reason: ...
```

```
      799029fbd6e54dbf8d7c52f4bb837111 (blade-198-18-1-2:7050): not running
      State: FAILED
      Data state: TABLET_DATA_READY
      Last status: Corruption: Failed log replay. Reason: ...
All reported replicas are:
   A = 2504215476754ff59ad3f0fcb0d58355
   B = 04735952e86f4a4a98f748d1c2546fd8
   C = 799029fbd6e54dbf8d7c52f4bb837111
```

Example 3:

```
Tablet 2aaf23af4cc241e1865d292462418046 of table 'db_log_public.__kavsprwq_fgt_traffic' is under-
      replicated: 1 replica(s) not RUNNING
   4df0f22bb51948fbbc0540383b0cfe74 (blade-198-18-1-5:7050): RUNNING
   e84166ee4a1f4fb58753d5570273eaa1 (blade-198-18-1-10:7050): RUNNING [LEADER]
   f02719025c0a41db92c64e0f37b94c53 (blade-198-18-1-4:7050): not running
      State: FAILED
      Data state: TABLET_DATA_READY
      Last status: Corruption: Failed log replay. Reason: ...
All reported replicas are:
   A = 4df0f22bb51948fbbc0540383b0cfe74
   B = e84166ee4a1f4fb58753d5570273eaa1
   C = f02719025c0a41db92c64e0f37b94c53
```

To fix the metadata corruption:

1. Rerun the Database Health Check multiple times and see if the issue persists. Sometimes Kudu may be able to heal by itself.
2. If the issue persists after a few retries, go to *Cluster Manager > Jobs > Create Custom Job*.
3. From the *Template* dropdown, select *Kudu Recover Corrupted Tablets* and Create.
4. In the *Jobs* table view, find the *Kudu Recover Corrupted Tablets* row, and click *Run in Actions*.
   After the job is submitted, the tablet goes into recovering mode (see the example Database Health Check result below). The recovery may take several minutes, depending on the tablet size. Run the Database Health Check repeatedly until the health check returns success.

Example:

```
   Tablet fcdb22e988f54674bf7bd81957d96d99 of table 'db_log_public.__root_fgt_hyperscale' is
         recovering: 1 on-going tablet copies
   69c7e95e57f748bd801be9562db9684e (blade-10-0-1-6:7050): not running
   State: INITIALIZED
   Data state: TABLET_DATA_COPYING
   Last status: Tablet Copy: Downloading block 0000000022163966 (8961/25704)
   538735a93bb8421b8fc2794fb31c52a7 (blade-10-0-1-5:7050): RUNNING
   077b5c932f2e4266820d13fb23442964 (blade-10-0-1-7:7050): RUNNING [LEADER]
```

If all replicas fail, you cannot fix the metadata corruption. Instead, the entire tablet must be deleted in the recover job. See To delete the entire tablet: on page 126.

In the below example, all replicas have failed.

```
Tablet 92ff614879504ee78b7c185a7d500d87 of table 'db_log_public.__8nhzlsno_facet_result' is
      unavailable: 3 replica(s) not RUNNING
```

```
fadb45339c9e426b95f060d831faa4cc (blade-198-18-1-8:7050): not running
   State: STOPPED
   Data state: TABLET_DATA_TOMBSTONED
   Last status: Deleted tablet blocks from disk
780c0e107ce54dc384f75766906f4177 (blade-198-18-2-14:7050): not running [LEADER]
   State: STOPPED
   Data state: TABLET_DATA_TOMBSTONED
   Last status: Deleted tablet blocks from disk
bc3d03488e5a47909135510210f899f5 (blade-198-18-1-10:7050): not running
   State: STOPPED
   Data state: TABLET_DATA_TOMBSTONED
   Last status: Deleted tablet blocks from disk
```

To delete the entire tablet:

1. Go to *Cluster Manager > Jobs > Create Custom Job*.
2. From the *Template* dropdown, select *Kudu Recover Corrupted Tablets*.
3. Enable *Delete Entire Tablet*.
4. Click *Create*.
5. In the *Jobs* table view, find the *Kudu Recover Corrupted Tablets* row, and click *Run in Actions*.

How to enable/disable PXE boot server on Security Event Manager Controller

Security Event Manager Controller requires a PXE boot server to boot the network hosts in order to process deployment, scale-up or blade replacement. In a FortiAnalyzer-BigData 4500F and FortiAnalyzer-BigData 4500G appliance, this PXE boot server is disabled by default. You may want to enable it to allow certain operations, or disable it to avoid any unintended network boot in the FortiAnalyzer-BigData deployment's internal network. To minimize unexpected side effect, PXE can only be enabled to run once. After the operation, PXE will be disabled again automatically.

To disable the PXE boot server:

Access the Security Event Manager Controller (see To connect to the Security Event Manager Controller) and run the following command to disable installation of system software:

```
fazbdadm disable pxe
```

To enable the PXE boot server to run once only:

Access the Security Event Manager Controller (see To connect to the Security Event Manager Controller) and run the following command to enable installation of system software:

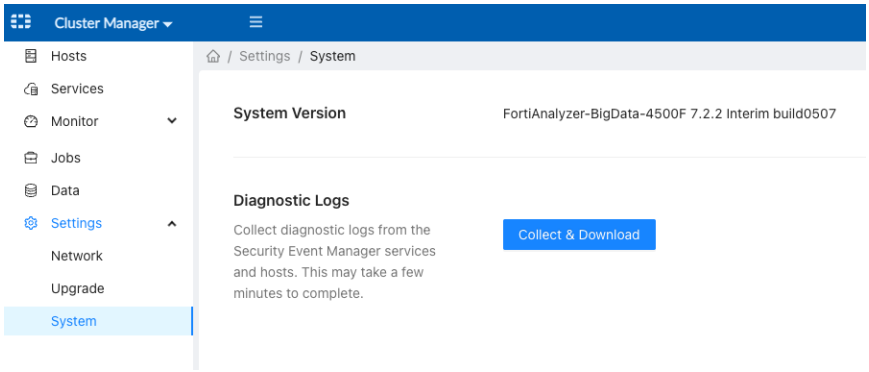
```
fazbdadm enable pxe-once
```

How to collect Diagnostic Logs

Diagnostic logs of the Security Event Manager services and host OSs can be collected from the Cluster Manager GUI.

To collect diagnostic logs via the GUI:

1. Go to *Cluster Manager* > *Settings* > *System*.
2. In the *Diagnostic Logs* section, click *Collect & Download*.



To collect diagnostic logs via the CLI:

1. Access the Security Event Manager Controller (see To connect to the Security Event Manager Controller: on page 12).
2. Enter the following command to collect the logs. Follow the output to locate the generated file with the logs packaged.

```
fazbdadm log export all
```

How to troubleshoot NTP time synchronization issues

Accurate time synchronization is essential for FortiAnalyzer-BigData operations. The NTP server ensures cluster-wide data consistency, which is required for reliable logging, monitoring, and analytics. The following section lists the most common NTP issues and provides troubleshooting guidance.

Scenario 1: NTP server unavailability causes FortiAnalyzer-BigData upgrade failure

FortiAnalyzer-BigData upgrade failed with the following error message being displayed:

```
[Pre-upgrade check] NTP connection check failed. A valid NTP server is required for distributed
consensus. Please configure a valid NTP via System Settings GUI or Main host CLI, and then rerun
the upgrade.
```

This indicates that the upgrade process cannot proceed because the cluster does not have a valid or reachable NTP server configured.

To debug and troubleshoot:

Run the following CLI command on the controller:

```
fazbdadm check ntp
```

The following error message displays to indicate NTP server issues:

```
NTP server <server IP> is not valid or not reachable
```

To resolve the issue:

Change to use a reliable NTP server through the GUI or FortiAnalyzer CLI, and then retry the upgrade process using the following CLI command:

```
fazbdctl upgrade cluster -o retry
```

Scenario 2: Kudu service down due to out-of-sync NTP clock

Kudu master/tablet server logs contain entries such as, "`clock beyond the error threshold of…`" or "`clock error estimate xxx too high`".

For example:

```
F0609 11:40:54.180898 7803 raft_consensus.cc:1554] Check failed: _s.ok() Bad status: Invalid
argument: tried to update clock beyond the error threshold of 20000000us: now 6778061021924950016,
to_update 6778061915287728128 (now_physical 1654800054180896, to_update_physical 1654800272287043)
```

Kudu relies on the system's NTP-synchronized wall clock to provide hybrid timestamps for the distributed consensus. This situation occurs when Kudu initially receives valid NTP samples, and the error estimate (uncertainty window) from the time source is beyond the threshold (default: 10 seconds). This can be caused by stale, jittery, delayed, or missing NTP responses.

To debug and troubleshoot:

1. From the *Cluster Manager* GUI, check the status and result of the *NTP Health Check* job in *Monitor > Health*.
2. From the FortiAnalyzer CLI, execute the following command:

   ```
   diagnose sys ntp status
   ```

- Check Stratum: Make sure the stratum is not relatively high (not too many hops away from the direct source of time). A high stratum may indicate reliance on an upstream server for synchronization.
- Check Last sample: This value represents the uncertainty or error bound of the time source. A high error margin indicates that the NTP discipline process does not have strong confidence in the clock's accuracy. If the margin exceeds the threshold that the database can tolerate, Kudu will stop accepting requests.

3. Check from the NTP server.
   If the NTP server host is accessible, the following command can be executed on the host to diagnose:

   ```
   ntpq -pn
   ```

   or

   ```
   chronyc sources
   ```

   - Look for the upstream NTP source.
   - If it has a *: synced to the current source.
   - If it does not have a * (only +, -, or nothing): not synced.
   - If the offset column shows a value of several seconds, it indicates a serious synchronization problem.
4. Check the kernel's error estimate.

   ```
   ntptime
   ```

   or

   ```
   chronyc tracking
   ```

   - Check the status: it should say `synchronized`.
   - Check the maximum error and the estimated error:
     - Healthy: hundreds of microseconds (µs) or a few milliseconds.
     - Bad: in the millions of µs (seconds).
5. How to check from the NTP client (FortiAnalyzer-BigData):

   Use this method if you have no access to the NTP source host.

   a. Query the configured NTP source directly.
      For example:

      ```
      ntpdate -q ntp1.fortinet.net
      ```

      or

      ```
      chronyd -Q -t 15 'server ntp1.fortinet.net iburst'
      ```

   b. Assuming the host is routable, query against a well-known time source. For example, "`0.pool.ntp.org`".
      For example:

```
ntpdate -q pool.ntp.org
```

or

```
chronyd -Q -t 15 'server pool.ntp.org iburst'
```

c. Compare the offset against pool.ntp.org (or another trusted public server) to determine if the configured NTP source is drifting.

To resolve the issue:

Run an NTP Sync job through the GUI (*Cluster Manager* > *Jobs* > *Create Job*) to force a synchronization.

If the issue persists, switch to a more reliable NTP source.

FAQ

Why does FAZBD4500F have physical ports 10G, 40G on SW module #1 & #2 when module #1 is for cluster internal connection?

By default, module #1 is for internal connections. If you need to expand the chassis, then you will need to link 2 boxes through the module #1 interfaces.

If there is no need for chassis expansion, you would not touch switch module #1.

Do port2 of FAZ Blade (slot 1) and Big Data hosts (Slots 2-14) have to be in the same subnet?

The recommended topology and the best practice is to use the same subnet.

If there is a second chassis (as for storage) are Blade 1 and Blade 2 used the same as Blade 3-14 or do they have special functions?

For the second chassis:

- Blade 1 is not used and should be powered off.
- Blade 2 does not have special functions, it is the same as Blades 3-14.

How many power supplies can fail without issues?

It is based on the workloads' power consumption. The field needs to observe the symptom and ensure the power supply to make it work.

Can we replace Blades/Switches for RMA?

Yes.

What happens if Blade 1 malfunctions?

If Blade 1 fails, it currently cannot failover to the other standby blade. However, as of v7.0.1, if you stack two FAZ-BD chassis, HA mode can be enabled across the two FAZ blades.

If Blade 2 fails, does it delegate its role to another blade?

If Blade 2 fails, it can failover to the other Big Data host.

Big Data controller's IP is configured in FortiAnalyzer Blade 1. Does this mean that this IP is "shared" between all Big Data hosts (Blades 2-14)?

The controller IP is not shared. It is configured on the Big Data controller. When the controller fails over, the IP is re-configured on a new controller.

When a blade fails, does it delegate its role to another blade?

When Blades 2-14 fails, the node with the same role will take over.

Does "3 K8s Master" mean there are 3 blades for this function?

Yes, it means there are 3 blades/hosts that are masters.

Is "3" the default replication factor?

Yes, there are 3 replications.

This means that 3 copies are stored in the system:

- 1 original copy
- 2 replicated copies

Is the allocated disk usage for the FortiAnalyzer blade or for the Big Data blade?

It is for FortiAnalyzer to cache the log data before they are ingested to the Big Data cluster.

To view the allocated disk usage, go to *Settings > Manage Storage Policy > Data Policy > Disk Usage > Allocated*.

In *Hosts* view, is the last number the actual slot?

The last number is the blade ID. It is important to install blades into slots according to IDs.

Is the blade ID labeled on the blades?

Yes.

If the blade is labeled, when a particular faulty blade is on RMA, should the RMA return with the same blade labeled with the same blade ID?

The RMA will ship a blade with the OS and bootloader wiped, so all the Big Data blades are the same no matter which blade ID it belongs to. Once it is injected into the slots, you will need to set the blade ID accordingly in bootloader. The Big Data controller will bootstrap it with a cluster role.

Does this mean HA is no longer supported?

For 6.2 & 6.4, the Blade 2-14 HA is supported by the Big Data architecture design.

Previous to v6.4.6, recovering/replacing a non-Data role node may fail and require a manual recovery process in some scenarios. This has been resolved in v6.4.6.

Can I migrate old logs after removing fetch management?

Data migration is not supported.

Is the upgrade started from the Big Data controller going to upgrade all the blades including Blade 1?

Yes. CLI runs on the controller node, then it will upgrade all the nodes, starting with and including Blade 1.

Will the size of the database affect the amount of time it takes to upgrade? For example, will it take less time to upgrade a 1Tb vs 150Tb?

Based on the Big Data architecture, the database is not rebuilt. Therefore, the size of the database will not impact the upgrade time.

Will Log View and Reports show data from its own cache and Big Data storage?

Data is stored in Big Data storage. When you query the log data from *Log View* and *Reports*, the query request will be sent to the Big Data. All the data returned comes from the Big Data cluster.

How much free storage is required for upgrade?

The system has a mechanism to reserve space for upgrade and other operations.

For upgrade, will all Big Data blades reboot at the same time, or in the order of the blade that finished downloading the image first?

The infrared controller handles the order of the blades. They will be rebooted parallel of each other.

When the system is working normally (not specific to upgrade), is log ingestion from the ADOM cache to Big Data storage in real time or is there a delay?

It is near real time. The delay will be several minutes at most.

Does "same version" mean same main branch (v7.2 to v7.2) or same patch level (v7.2.12 to v7.2.12)?

"Same version" means same patch level GA release.

Will the system rollback if an upgrade fails for certain blades?

The system will not rollback. However, you can use the CLI console to redo upgrading to recover.

```
fazbdctl upgrade fazbd -o retry
```

Change Log

Date	Change Description
2026-05-21	Initial release v7.2.12.

www.fortinet.com