FortiAnalyzer-BigData VM - CLI Reference

Version 7.0.3

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

July 18, 2022
FortiAnalyzer-BigData VM 7.0.3 CLI Reference
58-703-822529-20220718

TABLE OF CONTENTS

Introduction

FortiAnalyzer-BigData VM improves upon base FortiAnalyzer appliances and offers analytics-powered security and event log management to process large volumes of data. Redesigned with a new distributed architecture and high-end hardware, the Security Event Manager of FortiAnalyzer-BigData VM is a horizontally scalable, high availability (HA) system that supports the needs of large enterprise organizations. The Security Event Manager of FortiAnalyzer-BigData VM 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.

FortiAnalyzer-BigData documentation

The following FortiAnalyzer-BigData product documentation is available:

- *FortiAnalyzer-BigData Administration Guide*
  This document describes how to set up the FortiAnalyzer-BigData system and use it with supported Fortinet units.
- *FortiAnalyzer-BigData CLI Reference*
  This document describes how to use the FortiAnalyzer-BigData Command Line Interface (CLI) to manage the cluster hosts.
- *FortiAnalyzer CLI Reference*
  This document describes how to use the FortiAnalyzer Command Line Interface (CLI) and contains references for FortiAnalyzer CLI commands.
- *FortiAnalyzer-BigData Release Notes*
  This document describes new features and enhancements in the FortiAnalyzer-BigData system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.

Using the Command Line Interface

This section explains how to connect to the CLI and describes the basics of using the CLI. You can use CLI commands to view all system information and to change all system configuration settings.

Connect to the FortiAnalyzer-BigData VM CLI

Once you configure the FortiAnalyzer-BigData VM network, you can use the IP addresses to access the FortiAnalyzer-BigData VM Main CLI or the cluster controller and manage the system.

To connect to the FortiAnalyzer-BigData VM Main CLI:

1. Establish an SSH connection to the Main host IP you configured during initial setup.
2. Log in using the administrator credentials you created previously.
   If you did not create a new administrator credential during initial setup, use the default credentials of username `admin` with no password.

To connect to the cluster controller CLI:

1. Establish an SSH connection to the management IP you configured during initial setup.
2. Log in using the default username `root` and password `fortinet@123`.
3. Once you establish a connection, you can use the `fazbdctl` CLI commands to manage the cluster. For more information, see FortiAnalyzer-BigData VM cluster controller CLI on page 6.

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

FortiAnalyzer-BigData VM cluster controller CLI

This section describes how to use `fazbdctl`, the FortiAnalyzer-BigData VM Command Line Interface (CLI), and contains references for all `fazbdctl` commands.

`fazbdctl` is available on the cluster controller (see Connect to the FortiAnalyzer-BigData VM CLI on page 5) and is the main command used to manage the hosts of FortiAnalyzer-BigData VM.

Syntax

```
fazbdctl <command>
```

Commands

Command	Description
`enable`	Enable/disable cluster-wide features.
`help`	Help about any command.
`init`	Initialize the FAZ-BD cluster.
`reset`	Factory-reset or re-install the OS of a single node or the whole cluster.
`set`	Set system parameters.
`show`	Display system or cluster information.
`upgrade`	Upgrade system components.

Option	Description
`-h, --help`	Help information.

Show version

```
fazbdctl show version
```

Shows the FortiAnalyzer-BigData VM version of the host.

Show members

```
fazbdctl show members
```

Lists all the cluster hosts' information managed by the cluster controller.

Option	Description
`{-o | --option} wide`	Display additional columns such as MAC address and version information in wide format.

Example response

In this example:

- `Management IP/Mask` is `10.106.2.168/24`
- `Mainhost IP/Mask` is `10.106.2.167/24`

Field name	Chassis	Blade	Role	Address	Ext Address	Host Name
Value example	1	1	Controller	10.0.1.1		blade-10-0-1-1
	1	2	Member	10.0.1.2	10.106.2.170	blade-10-0-1-2
	1	32	Member	10.0.1.32	10.106.2.174	blade-10-0-1-32

Field name	State	Status	Tips
Value example	Joined	Alive	Main host
	Joined	Alive	
	Upgrading	Alive	Need upgrade

Field descriptions

Field name	Description
Management IP/Mask	This is the management IP address that is configured.
Mainhost IP/Mask	This is the Main host IP address that is configured.
Chassis	By default, the Chassis ID is 1.
Blade	Represents the slot sequence of the hosts in the cluster, starting from 1.
Role	Role is either controller or member.
Address	The internal IP address is immutable and is generated from the host's Chassis ID and Blade ID. 10.0.{chass ID}.{blade ID}

Field name	Description
Ext Address	The external IP address is set by users through `fazbdctl set` command.
Host Name	The host name.
State	The current status of the host. • **joined**: The host has joined the cluster. • **upgrading**: The host has joined this cluster and is running the upgrade process.
Status	The current status of the host. • **alive**: The host is up and running. • **failed**: The host fails to run.
Tips	Tips and notes about the host. • **Need upgrade**: The host’s version does not match the controller's version. • **Main host**: This host is the Main host.

Example response in wide format

In this example:

- `Management IP/Mask` is `10.106.2.168/24`
- `Mainhost IP/Mask` is `10.106.2.167/24`
- `Management Gateway` is `10.106.2.254`
- `Main Host Gateway` is `10.106.2.254`

Field name	Chassis	Blade	Role	Address	Ext Address	Ext Gateway	Host Name
Value example	1	2	Controller	10.0.1.1			blade-10-0-1-1
	1	2	Member	10.0.1.2	10.106.2.170	10.106.2.254	blade 10-0-1-2
	1	32	Member	10.0.1.32	10.106.2.174	10.106.2.254	blade-10-0-1-32

Field name	MAC	Version	State	Status	Tips
Value example	00:50:56:b2:7d:77	FortiAnalyzer-BigData-VM64 1.2.0	Joined	Alive	Main host
	00:50:56:db:2a:33	FortiAnalyzer-BigData-VM64 1.2.0	Joined	Alive	
	00:50:56:b2:e2:7b	FortiAnalyzer-BigData-VM64 1.1.0	Upgrading	Alive	Need upgrade

Additional field descriptions for wide format

Field name	Description
Management Gateway	This is the gateway for the management IP address that is configured.

Field name	Description
Main Host Gateway	This is the gateway for the Main host IP address that is configured.
Ext Gateway	The gateway for the external IP address.
MAC	The MAC address of the internal interface.
Version	The FortiAnalyzer-BigData VM version number running on the host.

Upgrade

```
fazbdctl upgrade {bootloader | fazbd | cluster} [-U <URL>][-o <option>][-p <password>][-u
      <username>]
```

Use this command to upgrade bootloader with argument "bootloader" and upgrade FortiAnalyzer-BigData OS with argument "fazbd" or "cluster" for the whole cluster. For more information, see the FortiAnalyzer-BigData Administration Guide in the Fortinet Doc Library.

- This command should be executed only on the cluster controller. It has no effect if run on other hosts.
- This command is only allowed when all the FortiAnalyzer-BigData VM services are healthy, but you can use `-f` to force the upgrade to run.

Extra options	Description
`{-U	--image-url} <URL>`	URL for the image to be downloaded and installed.
`{-o	--option} <Option>`	Re-run options when failed: `skip	retry	restart`.
`{-p	--password} [<password>]`	Password for the download server if there is one.
`{-u	--username} [<user name>]`	Username for the download server if there is one.

Examples

Command	Description
`fazbdctl upgrade cluster`	Interactively upgrade FortiAnalyzer-BigData.
`fazbdctl upgrade cluster -o retry`	If last upgrade fails, retry from the state where the upgrade fails.

Reset

```
fazbdctl reset [<worker-ip> | cluster] [-A | -I] [-o <option>][-n]
```

Reset the entire OS and optionally format all the disks for a single host or the whole cluster. When there is no argument specified, the reset applies to local host.

These are the available options in this command:

Extra options	Description
`-{-A	--all-settings}`	Resets all settings.
`{-I	--all-except-ip}`	Keeps the public IP constant.
`{-o	--option} <Option>`	Re-run options when failed in soft reset: skip, retry, restart
`{-n	--retain-internal-subnet}`	Keeps current subnet after hard-resetting cluster.

If no option is set, a soft reset will be performed. Otherwise, a hard reset will be performed to additionally format all the disks.

Examples

Command	Description
`fazbdctl reset`	Re-install the OS of this node (local).
`fazbdctl reset 10.0.1.32`	Re-install the OS of node 10.0.1.32, from a controller.
`fazbdctl reset 10.0.1.32 -A`	Factory-reset and clears all settings and data from the specified node, from a controller.
`fazbdctl reset cluster`	Re-install the OS of the whole cluster, from the controller.
`fazbdctl reset cluster -I`	Factory-reset the whole cluster from the controller, keeping the management and Main host IP addresses.
`fazbdctl reset cluster -A`	Factory-reset the whole cluster from the controller, clearing all settings and data.
`fazbdctl reset cluster -A -n`	Factory-reset the whole cluster from the controller, clearing all settings and data but retaining the original subnet after reset.

For instructions on how to reset your device, see the FortiAnalyzer-BigData VM Administration Guide in the Fortinet Doc Library.

Init

```
fazbdctl init cluster [-o <option>]
```

Initialize the FortiAnalyzer-BigData cluster. This command initializes and configures the FortiAnalyzer-BigData cluster hosts. The process takes approximately 30 to 40 minutes. For more information, see the FortiAnalyzer-BigData Administration Guide in the Fortinet Doc Library.

- This command should be executed only on the cluster controller. It has no effect if run on other hosts.

Extra options	Description
`{-o | --option} <Option>`	Re-run options when failed: `skip | retry |restart`

If you run this command on an existing cluster, it will reinitialize and cause you to lose all log data and configurations.

Set management, main host, and external addresses

```
fazbdctl {set | unset} addr {<ip address/mask> | dhcp} [<gateway>] [--management | --
     mainhost] \ [-H <host internal ip>] [-A] [-Y]
```

Set management IP address on the cluster controller and external IP addresses (used for Hyperscale logging) on cluster hosts to allow them to communicate with the outside world.

`external ip/mask` can be IP CIDR address or simply `dhcp`.

- The optional `management` flag indicates the data carried in the `ip address/mask` and `gateway` fields is used to set the management IP address. This flag is not compatible with `-H` and `-A` and is only available on the cluster controller.
- The optional `mainhost` flag indicates the data carried in the `ip address/mask` and `gateway` fields is used to set the Main host IP address and gateway. This flag is not compatible with -`H` and `-A` and is only available on the cluster controller.
- The optional `-H` flag specifies the internal IP address of a host where the external IP will be assigned. Without this flag, the external IP address is assigned to the local host.
- The optional `-A` flag sets external IP addresses on all hosts from the cluster controller. In this case, the `ip address/mask` field specifies the starting external IP address to be assigned to the first host. The remaining hosts are assigned external IP addresses incrementally from the starting external IP address within the network subnet, wrapping around when reaching the boundary of the network subnet. This flag is not compatible if `ip address/mask` is `dhcp`. Also, the Main host will not be affected by this operation.
- The optional `-Y` flag lets you skip interactive confirmation when the command is issued.

Examples

Command	Description
`fazbdctl set addr 10.160.74.174/24 10.160.74.1`	Set external IP CIDR address and gateway on local host.
`fazbdctl set addr -H 10.0.1.3 10.160.74.175/24 10.160.74.1`	Set external IP CIDR address and gateway for host 10.0.1.3.

Command	Description
`fazbdctl set addr dhcp`	Set external IP CIDR address via DHCP on local host.
`fazbdctl set addr 10.160.74.174/24`	Set external IP CIDR address on local host.
`fazbdctl set addr 10.160.74.174/24 10.160.74.1 --management`	Set IP CIDR address with gateway for management interface.
`fazbdctl set addr 10.160.74.175/24 10.160.74.1 --mainhost`	Set IP CIDR address with gateway for Main host interface.
`fazbdctl unset addr -H 10.0.1.3`	Unset external IP CIDR address on host 10.0.1.3.
`fazbdctl unset addr --management`	Unset the management IP CIDR address.
`fazbdctl set addr 10.160.74.174/24 10.160.74.1 -A`	Set external IP CIDR address on all members, starting from 10.160.74.174.
`fazbdctl unset addr -A`	Unset external IP CIDR address on all members.

Enable/Disable IP-Forward

```
fazbdctl [ enable | disable ] ip-forward
```

By default, all the cluster hosts except the cluster controller have no external network access. In some cases, you might want to allow external network access for all hosts, for example, to backup and restore data to external HDFS, to support Hyperscale log ingestion, etc.. This command allows you to forward packets from your internal network by enabling or disabling the NAT setup on the cluster controller.

- This command should be executed only on the cluster controller. It has no effect if run on other hosts.

FortiAnalyzer-BigData VM Main CLI

The FortiAnalyzer-BigData VM Main CLI consists of the following command branches:

config system	**config fmupdate**	**get**
show	**diagnose**	**execute**

system

Use `system` to configure options related to the overall operation of the FortiAnalyzer-BigData VM unit.

The following commands are unique to FortiAnalyzer-BigData VM.
For all other `system` commands, see the FortiAnalyzer CLI Reference.

fmupdate

Use `fmupdate` to configure settings related to FortiGuard service updates and the FortiAnalyzer-BigData VM's built-in FortiGuard Distribution Server (FDS).

For information on `fmupdate` commands, see the FortiAnalyzer CLI Reference.

execute

The `execute` commands perform immediate operations on the FortiAnalyzer-BigData VM unit. You can:

- Back up and restore the system settings, or reset the unit to factory settings.
- Set the unit date and time.
- Use ping to diagnose network problems.
- View the processes running on the FortiAnalyzer-BigData VM unit.
- Start and stop the FortiAnalyzer-BigData VM unit.
- Reset or shut down the FortiAnalyzer-BigData VM unit.

For information on `execute` commands, see the FortiAnalyzer CLI Reference.

diagnose

The `diagnose` commands display diagnostic information that help you to troubleshoot problems.

For information on `diagnose` commands, see the FortiAnalyzer CLI Reference.

get

The `get` commands display a part of your FortiAnalyzer-BigData VM unit's configuration in the form of a list of settings and their values.

The `get` command displays all settings, including settings that are in their default state.

Unlike the `show` command, `get` requires that the object or table whose settings you want to display are specified, unless the command is being used from within an object or table.

For example, at the root prompt, this command would be valid:

```
get system status
```

and this command would not:

```
get
```

For information on `get` commands, see the FortiAnalyzer CLI Reference.

show

The `show` commands display a part of your unit's configuration in the form of the commands that are required to achieve that configuration from the firmware's default state.

Unlike the `get` command, `show` does not display settings that are in their default state.

For information on `show` commands, see the FortiAnalyzer CLI Reference.

Limitations for the FortiAnalyzer-BigData VM virtual appliance

The following commands are altered or removed from FortiAnalyzer-BigData virtual appliance:

- `config system interface`
- `config system route`
- `config system docker`
- `execute reset`
- `diagnose system interface`
- `diagnose system print interface`

Change Log

Date	Change Description
2022-07-18	Initial release.