FortiAnalyzer-BigData - CLI Reference

Version 6.2.5

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/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

https://fortiguard.com/

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

October 29, 2020
FortiAnalyzer-BigData 6.2.5 CLI Reference
58-625-666254-20201029

TABLE OF CONTENTS

Introduction

FortiAnalyzer-BigData 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 is a horizontally scalable, high availability (HA) system that supports the needs of large enterprise organizations. The Security Event Manager of FortiAnalyzer-BigData 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 Security Event Manager 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 chapter 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.

This chapter describes:

- CLI command syntax
- Connect to the FortiAnalyzer-BigData CLIs
- Setting administrative access on an interface on page 6

CLI command syntax

This guide uses the following conventions to describe command syntax.

- Angle brackets < > indicate variables.
- Vertical bar and curly brackets { | } separate alternative, mutually exclusive required keywords.
  For example:
  ```
  set protocol {ftp | sftp}
  ```
  You can enter `set protocol ftp` or `set protocol sftp`.
- Square brackets [ ] indicate that a variable is optional.
  For example:
  ```
  show system interface [<name_str>]
  ```
  To show the settings for all interfaces, you can enter `show system interface`. To show the settings for the Port1 interface, you can enter `show system interface port1`.
- A space separates options that can be entered in any combination and must be separated by spaces.
  For example:
  ```
  set allowaccess {https ping}
  ```
  You can enter any of the following:
  ```
  set allowaccess ping
  set allowaccess https ping
  set allowaccess http https ping snmp ssh telnet webservice
  ```
  In most cases to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.
- Special characters:
  - The \ is supported to escape spaces or as a line continuation character.
  - The single quotation mark ' and the double quotation mark “ are supported, but must be used in pairs.
  - If there are spaces in a string, you must precede the spaces with the \ escape character or put the string in a pair of quotation marks.

Setting administrative access on an interface

To perform administrative functions through a FortiAnalyzer-BigData network interface, you must enable the required types of administrative access on the interface to which your management computer connects. Access to the CLI requires Secure Shell (SSH) access. If you want to use the GUI, you need HTTPS access.

To use the CLI to configure SSH access:

1. Connect and log into the CLI using the FortiAnalyzer-BigData console port and your terminal emulation software.
2. Use the following command to configure an interface to accept SSH connections:
```
config system interface
   edit <interface_name>
      set allowaccess <access_types>
   end
```
   Where <interface_name> is the name of the FortiAnalyzer-BigData interface to be configured to allow administrative access, and <access_types> is a whitespace-separated list of access types to enable.

   For example, to configure port1 to accept HTTPS and SSH connections, enter:
```
config system interface
   edit port1
      set allowaccess https ssh
   end
```
   Remember to press Enter at the end of each line in the command example. Also, type end and press Enter to commit the changes to the FortiAnalyzer-BigData configuration.
3. To confirm that you have configured SSH access correctly, enter the following command to view the access settings for the interface:
```
get system interface <interface_name>
```
   The CLI displays the settings, including the management access settings, for the named interface.

Connect to the FortiAnalyzer-BigData CLIs

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

To connect to the FortiAnalyzer-BigData Main CLI:

1. Establish an SSH connection to the Cluster Management 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 BigData Cluster Controller:

1. Establish an SSH connection to the Cluster 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 cluster controller CLI on page 8.

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

FortiAnalyzer-BigData cluster controller CLI

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

`fazbdctl` is available on the BigData Cluster Controller (see Connect to the FortiAnalyzer-BigData CLIs on page 6) and is the main command used to manage the Security Event Manager hosts of FortiAnalyzer-BigData. It can be used in the following ways:

- `fazbdctl -c show -t version`
- `fazbdctl -c show -t members`
- `fazbdctl -c upgrade [ -t fazbd | bd [ -h members | {member_ip_addr}] | faz ] [ -f ]`
- `fazbdctl -c reset [ -h [ cluster | members | local | {member_ip_addr} ] ] [ -o [ all-except-ip | all-except-ssh | all-except-ip-ssh ] ]`
- `fazbdctl -c init`
- `fazbdctl -c set -t appliance -m extender`
- `fazbdctl -c [ enable | disable ] -t ip-forward`
- `fazbdctl -c delete -h {member_ip_addr}`

Show version

```
fazbdctl -c show -t version
```

Shows the FortiAnalyzer-BigData version of the host.

Show members

```
fazbdctl -c show -t members
```

Lists all the Security Event Manager member hosts' information managed by the BigData Cluster Controller

- This command should be executed only on the BigData Cluster Controller. It has no effect if run on other hosts.

Example response:

Field name	Chassis ID	Blade ID	Internal IP address	Internal interface MAC address	Version number	Current Status	Tips
Value example	1	3	10.0.1.3	ac:1f:6b:5a:9d:ba	20200131-102049	JOINED	
	2	5	10.0.2.5	ac:1f:6b:5a:92:16	20200118-111231	UPGRADING	Needs upgrade

Field description

Chassis ID	By default, the Chassis ID is 1. If you want to designate an appliance as an extender appliance, change the Chassis ID to a range between 2-254.
Blade ID	Represents which slot the blade is located in. The order of the blade slots starts from the left side of the FortiAnalyzer-BigData appliance, starting from 1 to 14.
Internal IP address	The internal IP is immutable and is generated from blade's Chassis ID and Blade ID. 10.0.{chass ID}.{blade ID}
Internal interface MAC address	The MAC address of the internal interface.
Version number	The FortiAnalyzer-BigData version number running on the host.
Current status	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.
Tips	Tips and notes about the host. • Need upgrade: The host's version does not match the controller's version.

Upgrade

```
fazbdctl -c upgrade [ -t fazbd | bd [ -h members | {member_ip_addr}] | faz ] [-f]
```

Generally used to upgrade the system. For more information, see the FortiAnalyzer-BigData Administration Guide in the Fortinet Doc Library.

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

`fazbdctl -c upgrade -t fazbd`	Upgrade the FortiAnalyzer-BigData system (default, if no option is passing).
`fazbdctl -c upgrade [ -h members | {member_ip_addr}]`	(Advanced) Upgrade the member host(s) to the current BigData Cluster Controller's version.
`fazbdctl -c upgrade -t bd`	(Advanced) Upgrade the BigData Cluster alone.
`fazbdctl -c upgrade -t faz`	(Advanced) Upgrade the FortiAnalyzer-BigData Main host alone

Reset

```
fazbdctl -c reset [-h [cluster | members | local | {member_ip_addr}]] [-o[all-except-ip | all-
     except-ssh | all-except-ip-ssh] ]
```

Reset the entire OS of the blades and optionally format all the disks. There are four available options in this command:

Extra options	Description
`-o all-settings`	Resets all settings.
`-o all-except-ip`	Keeps the public IP constant.
`-o all-except-ssh`	Keeps the ssh public key constant.
`-o all-except-ip-ssh`	Keeps the ssh public key and public IP constant.

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

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

Init

```
fazbdctl -c init
```

Initialize the Security Event Manager after a hard reset. This command initializes and configures the Security Event Manager. The process takes approximately 30 to 40 minutes to complete. For more inforation, see the FortiAnalyzer-BigData Administration Guide in the Fortinet Doc Library.

- This command should be executed only on the BigData Cluster Controller. It has no effect if run on other hosts.

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

Set appliance role

```
fazbdctl -c set -t appliance -m extender
```

Designate an appliance as an extender appliance so you can add it as an extender to the main appliance. For instructions on assigning a new chassis ID to the extender appliance, see the FortiAnalyzer-BigData Administration Guide in the Fortinet Doc Library.

- This command should be executed only on the BigData Cluster Controller. It has no effect if run on other hosts.

Enable/Disable IP-Forward

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

By default, all the BigData Cluster hosts except the BigData 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. This command allows you to forward packets from your internal network by enabling or disabling the NAT setup on the BigData Cluster Controller.

- This command should be executed only on the BigData Cluster Controller. It has no effect if run on other hosts.

Delete host

```
fazbdctl -c delete -h {member_ip_addr}
```

Decommission a host in the BigData Cluster members. For more information, see the FortiAnalyzer-BigData Administration Guide in the Fortinet Doc Library.

- This command should be executed only on the BigData Cluster Controller. It has no effect if run on other hosts.

FortiAnalyzer-BigData Main CLI

The FortiAnalyzer-BigData 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 unit.

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

global

```
config system global
   set bd-management-gateway <string>
   set bd-management-ip <string>
end
```

Variable	Description
bd-management-gateway <string>	Set the Gateway for the FortiAnalyzer-BigData management GUI.
bd-management-ip <string>	Set the IP of the FortiAnalyzer-BigData management GUI.

fmupdate

Use `fmupdate` to configure settings related to FortiGuard service updates and the FortiAnalyzer-BigData unit’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 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 unit.
- Start and stop the FortiAnalyzer-BigData unit.
- Reset or shut down the FortiAnalyzer-BigData 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 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.

Change Log

Date	Change Description
2020-10-29	Initial release.