FortiAnalyzer-BigData - Release Notes

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

October 26, 2022
FortiAnalyzer-BigData 7.0.3 Release Notes
58-703-0813708-20221026

TABLE OF CONTENTS

Change Log 4
FortiAnalyzer-BigData version 7.0.3 5
Supported models 5
New features and enhancements 5
Special Notices 6
Ports 6
Log Files 6
Product Integration and Support 7
Firmware Upgrade Paths 8
Fortinet Security Fabric 8
Resolved Issues 9
Known Issues 11
FortiAnalyzer-BigData VM Limitations 14

Change Log

Date	Change Description
2022-03-24	Initial release.
2022-03-30	Updated Resolved Issues on page 9.
2022-06-02	Patch release, build 0118.
2022-06-24	807486 added to Resolved Issues on page 9.
2022-07-18	FortiAnalyzer-BigData VM release. • Updated Known Issues on page 11. • Added FortiAnalyzer-BigData VM Limitations on page 14.

FortiAnalyzer-BigData version 7.0.3

This document provides information about FortiAnalyzer-BigData version 7.0.3 build 0118.

The recommended minimum screen resolution for the FortiAnalyzer-BigData GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

Supported models

FortiAnalyzer-BigData version 7.0.3 supports the following models:

FortiAnalyzer-BigData	FAZBD-4500F
FortiAnalyzer-BigData VM	FAZBD-VM64

New features and enhancements

For more information about what's new in FortiAnalyzer-BigData and supported by FortiAnalyzer-BigData 7.0.3, see the FortiAnalyzer 7.0 New Features Guide.

Data management

- FortiAnalyzer-BigData7.0.3 supports migrating an ADOM to another storage pool. For information, see Migrate an ADOM to a Storage Pool.

Hyperscale firewall logging support

- Support for Hyperscale FortiGate logging in Syslog format. For information, see Configure FortiAnalyzer-BigData as log server on hyperscale FortiGate.
- A new normalized FortiGate-Hyperscale log type for Hyperscale logs in both Syslog and IPFIX format. For information, see Search Hyperscale log in Log View.
- Improved query engine resource utilization.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer-BigData version 7.0.3.

There are currently no special notices included for FortiAnalyzer-BigData 7.0.3.

Ports

Please be aware of the limitations for the following ports:

- Port 2055 reserved.
- Default Admin https port 443 cannot be customized.

Log Files

The log file rolling size setting should be smaller than the minimum ADOM cache allocation size of blade1.

Product Integration and Support

FortiAnalyzer-BigData 7.0.3 support of other Fortinet products is the same as FortiAnalyzer 7.0.3. For details, see the FortiAnalyzer 7.0.3 Release Notes in the Document Library.

Upgrade bootloader

If you are currently using FortiAnalyzer-BigData, we recommend upgrading bootloader.

To upgrade bootloader, connect to the Security Event Manager Controller and run the following command:

```
fazbdctl upgrade bootloader
```

Firmware Upgrade Paths

You can upgrade FortiAnalyzer-BigData 6.4.0 or later to FortiAnalyzer 7.0.3.

The following table identifies the supported FortiAnalyzer-BigData upgrade paths and whether the upgrade requires a rebuild of the log database. If you need information about upgrading to FortiAnalyzer 6.2 or 6.4, see the corresponding FortiAnalyzer Upgrade Guide.

Initial Version	Upgrade to	Log Database Rebuild
6.4.5 or later	Latest 6.4 version, then to latest 7.0 version	No
6.2.1 or later	Latest 6.2 version, then to latest 6.4 version	No

FortiGate units with logdisk buffer log data while FortiAnalyzer units are rebooting. In most cases, the buffer is enough to cover the time needed for FortiAnalyzer to reboot. However, Fortinet still recommends configuring multiple log destinations to ensure no logs are lost.

Fortinet Security Fabric

If you are upgrading the firmware for a FortiAnalyzer-BigData unit that is part of a FortiOS Security Fabric, be aware of how the FortiOS Security Fabric upgrade affects the FortiAnalyzer-BigDataupgrade. You must upgrade the products in the Security Fabric in a specific order. For example, you must upgrade FortiAnalyzer-BigData to 7.0.0 or later before you upgrade FortiOS to 7.0.0 or later.

Resolved Issues

The following issues have been fixed in FortiAnalyzer-BigData version 7.0.3. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
774597	FortiAnalyzer-BigData shows *No Data Appendix Jobs* failing.
790538	FortiAnalyzer-BigData Reset/upgrade fails due to expired certificates.
769855	FortiAnalyzer-BigData shows *No entry found*" for FortiView even though the graph is able to be displayed.
776865	FortiAnalyzer-BigData is not able to see recent logs after upgrade when Facet formation job is delayed.
760289	ZTNA logs need to sync to FortiAnalyzer-BigData.
762588	The IOC result is incorrect if the ADOM is not in Root storage.
728350	*Incident & Event* does not tag *Ioc_Rescan* for the rescanned *Compromised Host*.
801635	FortiAnalyzer-BigData Main Host not inserting logs after upgrade to 7.0.3.
799149	FortiAnalyzer-BigData 10K reports pending.
801969	Data Maintenance job keeps failing when data retention is over a year.
803542	Data Rebalance breaks other jobs and services.
799909	NTP sync job keeps failing.
797894	log-forward shows error message *Failed to load*.
797388	Master leader blade failed to assign role after option-6 reset.
803366	Memory leak in impala.
803582	Logs not visible in *LogV iew* of FortiAnalyzer-BigData.
804799	Report schedule breaks after upgrade to 7.0.3
806434	The date/time filter did not work in *LogView*.
794932	FortiAnalyzer-BigData oftpd hangs and FortiGate is not able to poll logs.
802292	Logs sourced from FortiAnalyzer-BigData showing the incorrect time.
787872	*FortiView*: only one point is shown for the line in drill down page for *Resource Usage*.
792961	*Resource Usage* in *FortView* never shows all devices.
807183	*LogView* > *Hyperscale* is replaced by *LogView* > *Ipfix*.
760229	Get FortiView data failed on FortiGate if the data source is *FAZBD*.

Bug ID	Description
794640	Logforwarding GUI shows "Fail to Load".
794113	Internal Address Setting Error.
782065	Custom Storage Pool Data Restore Failed.
779194	Incremental backup failed.
807486	*Device Manager* fails to load in the GUI.

Known Issues

The following issues have been identified in FortiAnalyzer-BigData version 7.0.3. For inquires about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

LogView

Bug ID	Description
718896	Download fails if *All Pages* is selected.

FortiView

Bug ID	Description
791657	The data cannot be shown in list for *Top Cloud Applications* and *Top Cloud Users* if *All Devices* is selected.
761184	The IOC task can't be cancelled.
742634 761400	The*EndTime*, *Percentage* and *Status* are incorrect for IOC task.

Monitors

Bug ID	Description
788901	Exception is thrown and no data returned for *Monitors* > *FortiMail*.

Reports

Bug ID	Description
790925	Outbreak Alerts report: Found sql err of `attackid` and `vulnid`: operands of type BIGINT and STRING are not comparable.
794226	DNS Security Report: Domain Count by Threat Level, `is_botnet` type's conflict `BOOLEAN` and `INT`.
794446	Secure SD-WAN Report could not resolve column/field reference: `$fv_plhd_timescale`.
791534	FortiMail Analysis Report found a chart that has `sql failed`.

System Setting

Bug ID	Description
792466	Dashboard's widgets do not display properly and must be adjusted manually.

Common

Bug ID	Description
792609	Found `fortilogd` stopped when dvm added to over 4300.
786016	Logs in FortiGate with `src FAZ BD` show incorrect time.
787849	FAZ DVM call to fetch devices too slow on FortiAnalyzer-BigData platform with 18500 devices and 2000 ADOMs.
787349	Create New ADOM page storage pool field issue.
777503	Log import: the GUI does not respond when *OK* is clicked.
765976	Multi-adoms report performance needs to be optimized.
757906	System Settings/HA VIP interface is incorrect in GUI.
773434	Kudu may be not working after restart MetaStore Node.

FortiAnalyzer-BigData VM

Bug ID	Description
819898	FAZBD-VM: System Dashboard - *Disk IO* widget always shows 0.
821931	In a resource-imbalanced cluster, could find: '*Failed to connect to 198.18.0.91 port 8080: Connection refused*' is shown when run IOC rescan.
822136	FAZBD-VM: Devices of IPFIX and Syslog are not listed in *GlobalSearch* > *Labels* > *DeviceID*.
822052	FAZBD-VM: BD Management UI login process is unusually slow and clearing cache is needed.
817923	FAZBD-VM Can't login Blade-1 VM console.
821638	FAZBD-VM Diagnostic logs *Collect & Download* is not working with Firefox browser.
821588	FAZBD-VM: Setting the external IPs in GUI gets signed out unexpectedly.
821298	FAZBD-VM: Set the external IPs for hyperscale log traffic failed with errors.
820211	Sometimes could find report. Error:*error: _recv_chart_result:1906: Internal error (-4)*.
816908	FAZBD-VM: ntp design may cause FAZ and BD clock out-off sync.
820188	Need add-on license for FAZBD-VM.

Bug ID	Description
822536	Need to add command for checking mainhost network settings.
810839	FAZBD-VM deploy found "A required image was missing" in ESXI 6.7. Note: ESXI 6.7.0 Update 1 (Build 10764712) has this issue.

FortiAnalyzer-BigData VM Limitations

The following commands are altered or removed when running FortiAnalyzer as a container on a FortiAnalyzer-BigData docker host:

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