FortiAnalyzer-BigData - Release Notes

Version 7.0.1

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 22, 2022
FortiAnalyzer-BigData 7.0.1 Release Notes
58-701-744043-20221022

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-11-22	Initial release.

FortiAnalyzer-BigData version 7.0.1

This document provides information about FortiAnalyzer-BigData version 7.0.1 build 0019.

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 7.0.1 supports the following models:

FortiAnalyzer-BigData	FAZBD-4500F

What's new

For more information about what's new in FortiAnalyzer-BigData and supported by FortiAnalyzer-BigData 7.0.1, see the FortiAnalyzer New Features Guide.

Performance improvements

The followling performance improvements have been implemented in FortiAnalyzer-BigData 7.0.1:

- Storage pool support for fine-grained data retention management.
- Improved data streaming protocol and processing pipeline with better resource utilization.
- FortiAnalyzer-BigData main host high availability support in a stacked chassis setup.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer-BigData version 7.0.1.

There are currently no special notices included for FortiAnalyzer-BigData 7.0.1.

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 7.0.1 support of other Fortinet products is the same as FortiAnalyzer 7.0.1. For details, see the FortiAnalyzer 7.0.1 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 7.0.1.

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 7.0.1. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
728505	Compromised rescan tasks *Start Time* was incorrect
736474	When *Outbreak Alerts* handler is enabled, FortiAnalyzer-BigData Log insert rate dropps to around 150k due to the high CPU usage.
736741	Multiple ADOMs: Logview doe not display logs, and the left side menu is not generated; the global search returns data.
737032	*Data Balance* and *Data Balance All jobs* always fails.
737993	After system reset, ForitAnalyzer ADOM information does not sync to FortiAnalyzer-BigData.
739476	IoC rescan job can't proceed, *Connection 0 to host 10.0.0.91 left intact*.
740773	IoC rescan: *job Cannot connect to server in _trim_task_status_db, _create_metadata_tmp_file, and _create_metadata_tmp_file*.
741283	FortiAnalyzer-BigData: Retry mechanism needs to be added for FortiView and Report facet job.
742569	FortiAnalyzer-BigData does not support custom HTTPS port.
748253	Performance issue when processing a high input rate of FortiGate *Event* data.
748771	Bring back HA page on FAZ-BD GUI
748772	FAZ-BD HA slave will lost GUI after sync.
749031	FAZBD HA primary node log insert rate is low
749319	FAZBD HA upgrade, the master and slave switched, and bd-management-ip become the same cause BD controllers IP conflicts
750370	Build 703, GUI has a 500 internal error.
753158	Found facets register error : *(missing from GROUP BY clause?): devid*, and *Could not resolve column/field reference: 'dvid*.
753164	Found facet register error: *Could not resolve table reference: 'casb_file*.
753617	FortiAnalyzer-BigData fails to do both full and incremental internal backup.
754359	FortiAnalyzer-BigData Controller to Support FAZ-Blade HA.
755707	Create a new storage pool, then enter numbers as the storage pool ID. Error alert shows *ID is invalid*.
757461	Create storage pools, then create ADOMs. The ADOM creation stalls in the pending stage.

Bug ID	Description
758175	FortiAnalyzer-BigData fails to modify blade-2 BD controller external IP.
758427	FortiAnalyzer list misses one of the secondary FortiAnalyzers.
758530	When upgrading FortiAnalyzer-BigData from 6.4.6 GA to 7.0, the process stops at *30%: Aborted syncing due to abnormally long duration*.
759268	*Data Balance* does not work properly
760452	After one blade is assigned a role, an existing blade does not receive FAZ traffic.
760614	`Debug` command could break the proxy, and the GUI cannot be accessed
761469	When changing HA mode to *standalone*, the log insert process is stopped.

Known Issues

The following issues have been identified in FortiAnalyzer-BigData version 7.0.1. For inquires about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

LogView

Bug ID	Description
756913	The values for some fields are unreasonable in the *Traffic* details.

FortiSoC

Bug ID	Description
759751	Run playbook *Get Software Inventory from EMS (EMS Connector)* fails.

FortiView

Bug ID	Description
760229	Get FortiView data fails on FortiGate if the data source is FortiAnalyzer-BigData.
757023	Exception *Could not resolve column/field reference: http_version* is in log for FortiWeb FortiView *Traffic*.
757022	Exception *Could not resolve column/field reference: threat_level* is in log for FortiWeb FortiView *Security*.

Monitors

Bug ID	Description
759856	Exception is thrown in log when drill down to *Log View* page in *Web Violation* tab for Endpoints(FortiClient).
757036	Exception is thrown in log when query Endpoints -> *Top Endpoint Vulnerabilities (FortiClient)* widget.

Cluster Manager

Bug ID	Description
727950	*Streaming Monitor* dashboard can only display data from around 3.5 hours ago.

Reports

Bug ID	Description
755505	The *Running report:XXX* should disappear after the report is running.
755503	Exception is thrown in log when run report "Outbreak Alert - Kaseya VSA Vulnerability for CVE-2021-30116 Report".
755502	Exception is thrown in log when running report *Outbreak Alert - DarkSide Ransomware Detection Report*.
756242	Report: Exception is thrown in log when runing a custom report with Macro *Daily Summary Total Bandwidth*.

System Setting

Bug ID	Description
757906	*System Settings/HA VIP interface is incorrect in the GUI.*
762981	Adom *Allocated Storage* need to change name.

Common

Bug ID	Description
726155	FortiAnalyzer-BigData fails to access *Cluster Manager* after Hard Reset.
727808	Data Ingestion, the blade 1 stops receiving and inserting logs when disk usage is high, needs to release disk automatically.
727944	FortiAnalyzer CLI for admon quota setting cannot support 700+ adoms.
728350	Incident Event does not tag *Ioc_Rescan* for the rescanned Compromised Host.
729100	Monitor/Dashboards/Streaming Monitor doesn't display multiple application data chart when set *ApplicationId* to *All*.
732066	Ingestion rate drops for a long time after powering off the master node.
733303	Lafka connecting timeout due to broker down.
753993	Data Nodes are running in high CPU state triggered by log search query.
755412	Kudu client fails after powering off controller blade.
756339	FortiAnalyzer-BigData setup stalls at *Create default storage pool*.
757895	FortiAnalyzer-BigData ingestion rate goes down during HA FortiSnalyzer failover.
758132	*Upgrade Firmware* left menu didn't match right side page.
758386	FortiAnalyzer-BigData suppport for Secure Protocol to transfer firmware image.

Bug ID	Description
759733	After separate HA setup in extender chassis some blades failed to join the new controller.
760289	ZTNA logs need to sync to FAZBD.
760300	For 7.0.1 ZTNA logs, FortiAnalyzer-BigData- Global Search need to add new logtype zlog.
760448	FortiAnalyzer traffic may be lost when one blade powers off.
761063	Backup fails on hdfs error.
762588	The IOC result is incorrect if the ADOM is not in *Root* storage.
762987	Admin profile's authority configuration need to add the control to the new modules: *Cluster Manager* and *Global Search*.