SECURITY MANAGEMENT

FortiAnalyzer-Big Data Release Notes

VERSION 3.2.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

CLI REFERENCE

http://cli.fortinet.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

Wednesday, March 22, 2017

FortiAnalyzer-Big Data 3.2.0 Release Notes

1st Edition

TABLE OF CONTENTS

Introduction

FortiAnalyzer-Big Data (formerly known as FortiMonitor) is a horizontally scalable, Hadoop (big data) based platform for collecting, analyzing, and correlating log data from Fortinet network security devices.

Note: If you are currently using FortiMonitor, continue to use the FortiMonitor product name for your specific platform. Also, make sure you are using the images for the FortiMonitor-3000D hardware.

This document provides installation instructions and caveats, resolved issues, and known issues for FortiAnalyzer-Big Data version 3.2.0, build 0211. It includes the following key features:

- **Asset management** – FortiAnalyzer-Big Data lets you monitor security events by asset, including individual hosts and host groups, websites, and network segments.
- **Event normalization/standardization** – FortiAnalyzer-Big Data collects security logs from devices that have different manufacturers and log formats. After it collects the original logs, FortiAnalyzer-Big Data uses knowledge base definitions to normalize them as security events. FortiAnalyzer-Big Data can parse and normalize any logs from user-defined data sources that use the syslog message standard.
- **Scan management** – FortiAnalyzer-Big Data can use scan services provided by third-party devices to perform web and system scans, and host, service, or defacement detection. FortiAnalyzer-Big Data normalizes any detected vulnerabilities and performs cross-correlation to calculate their reliability. An additional cross-correlation feature relates these vulnerabilities to attack events from devices such as intrusion defense systems (IDS), intrusion prevention systems (IPS), and web application firewalls (WAF).
- **Correlation analysis** – FortiAnalyzer-Big Data provides four types of data correlation: inventory correlation, asset correlation, logical correlation, and cross-correlation. You can use the web UI to customize the policy for all the correlation types, and create custom logical correlation rules and import them into FortiAnalyzer-Big Data.
- **Machine Learning** – FortiAnalyzer-Big Data's machine learning technology detects hosts infected by bots by performing an in-depth analysis of the traffic logs of requested domains. FortiAnalyzer-Big Data provides two algorithms to detect hosts infected by bots based on the black list that the Fortinet data center provides: Bayesian Algorithm and C&C Server List. The Bayesian algorithm training tasks can generate models to use in Bayesian Algorithm prediction tasks, which predict infected hosts. The C&C Sever List algorithm detects the infected hosts using the black list directly.
- **KRI (Key Risk Indicator)** – FortiAnalyzer-Big Data makes a Security Assessment based on a KRI (Key Risk Indicator). FortiAnalyzer-Big Data calculates KRIs for diverse targets (such as overall network, region, host group, host, and website) based on the risk of security events and vulnerabilities. It then uses KRI values to generate the hierarchical security risk indicator system with multiple dimensions (asset vulnerability indicator, threat growth indicator, security threat indicator, and so on). You can also use the web UI to view the events that contribute to the KRI in detail ("drill down" feature).
- **Risk Calculation** – FortiAnalyzer-Big Data can periodically calculate risk for all assets based on several factors, such as the reliability or severity of an event or vulnerability, and the value of an asset.
- **Reporting** – FortiAnalyzer-Big Data supports flexible, customized reports.

For more information, see http://docs.fortinet.com/fortimonitor/

What's new

This release contains the following enhanced features:

- **Change Persistent Type** – Administrators can now configure the storage type, database or Hadoop, for each event type. Administrators can also configure the Hive/Hadoop partition sizes as hourly or daily. (The FortiAnalyzer-Big Data team recommends opening a support ticket for engineering first before changing the default values. The optimal settings will depend on the log volumes and retention requirements for the user environment.)
- **Large HDD** – GPT has been introduced to support large disks on new platforms. (This does not affect the FMR-3000D and FAZ-BD-4000D.)
- **Menu** – FortiAnalyzer-Big Data's menu style and main menu groups have been changed to match FortiAnalyzer.
- **Process Bar** – A progress bar has been added to searches in FortiView and Log View for improved usability.
- **Collector Enhancements:**

  Collectors can now be restarted from the web UI.

  New user-defined event types are now synchronized to collectors automatically. (For the most common use cases, the user won't be expected to create new event types.)

  If an error occurs, events are not re-sent to the Java Message Service. (This change is to prevent old events from building up and preventing the system from responding to new events.)

Monitor settings and browser support

- **Monitor settings for web UI access** – To view all objects in the web UI properly, set your monitor to a screen resolution of 1280x1024.
- **Web browser support** – The FortiAnalyzer-Big Data web UI supports the following web browsers:
  - Internet Explorer 11.x
  - Firefox 40+
  - Chrome 43+
  - Opera 37+

Supported security devices

FortiAnalyzer-Big Data supports both pre-defined and user-defined device data sources. Templates for user-defined devices are provided by engineering when introducing support for new devices or OS versions, such as FortiOS 5.4.

The table below lists the supported device types for both pre-defined and user-defined templates.

Vendor	Device	Version	Log protocol	Log type
Fortinet	FortiGate	4.0/5.0/5.2/5.4*	Syslog	All log types
	FortiDB	5.1.4	FTP	Audit/Alert
	FortiDB	5.1.0, build 1130	Syslog & FTP	Audit/Alert
	FortiMail	5.2	Syslog	All log types
	FortiWeb	4.3/4.4/5.4*	Syslog	Attack/Traffic/Event
NSFocus	NSFocus NIDS1200B	5.6.6.164	Syslog	IPS
Symantec	Symantec SEP	12.1	Syslog	Virus
Venustech	Venus	4A	Syslog	Audit 4A
CNGate	CNGate-NGIPS	5.4	Syslog	IPS

* requires user-defined templates available from the support site: https://support.fortinet.com.

Supported user-defined device templates

FortiAnalyzer-Big Data provides user-predefined Fortinet device templates as listed in the table below.

Vendor	Device	Version	Log protocol	Log type
Fortinet	FortiGate	5.4	Syslog	All log types
	FortiWeb	5.5	Syslog	All log types

Supported scanners

You can configure FortiAnalyzer-Big Data version 3.2.0 to manage and receive data from the following vulnerability scanners:

- DBAPPSecurity 4.0.4.30
- IBM AppScan Enterprise 8.70.0.0 (Chinese version only)
- Knownsec 4.x
- Nessus 5.x, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8
- NSFocus RSAS-E 5.0, RSAS-M-S 5.0
- RJ-iTop 3.0.8.0
- WebRavor NWRPC 2013

Hardware support

FortiAnalyzer-Big Data 3.2.0 supports the following hardware platforms:

- FortiAnalyzer-Big Data 3000D
- FortiAnalyzer-Big Data 4000D/4100D

Upgrade instructions

This is a minor release of FortiAnalyzer-Big Data. To upgrade from FortiAnalyzer-Big Data 3.1.1 or earlier, download the new firmware files and execute an upgrade on each server blade individually. For detailed firmware installation instructions, see the *FortiAnalyzer - Big Data Handbook*.

Resolved issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support or go to https://support.fortinet.com.

Resolved issues

Bug ID	Description
0407374	System-JMS Server: Flow control is triggered when total message quantity is larger than 1T.
0409565	If the table of an event main type is locked for backup, logs of other event main types will be blocked.
0410188	From v3.1.1, data in the database will be backed-up to hive in duplicate after the backup policy is run more than 3 times.

High Performance Network Security