SECURITY MANAGEMENT

FortiAnalyzer-Big Data Release Notes

VERSION 3.3.0

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

Friday, July 21, 2017

FortiAnalyzer-Big Data 3.3.0 Release Notes

1st Edition

TABLE OF CONTENTS

Introduction

FortiAnalyzer-Big Data 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 3.3.0, build 0353. 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:

- **Table revamp**—Tables have been revamped for the following log types: Web Attack, Web Traffic, VPN, VoIP, Router, WAN Opt., and Cache. All logs in these tables will be lost.
- **Collector support**—FortiGate 5.4 predefined collectors are now supported.
- **Log View style**—The Log View module is now stylistically similar to FortiGate 5.4.
- **Log download**—Users can now download queried logs in text or CSV format.
- **Log export**—Log files stored in Hive can be imported and exported.
- **Report format**—Users can now generate reports in CSV format.
- **Stop report**—Users can now stop reports while the report task is running.
- **Report status**—If there are multiple widgets in a report, the report process status changes whenever a widget finishes.
- **Report invalidation**—Users can invalidate and edit running report policies.
- **Predefined report template**—Predefined report policies are now report templates. Report templates can be seen for both root and ADOM users. Users can view and clone a report template.
- **Default trigger action**—The default trigger action for all log types is false. To allow logs to trigger action, users must set Trigger Action to true in the corresponding log type.
- **Device manager enhancement**—Users can now add devices using a wizard. There is no longer a need to configure collectors.
- **Collector restart**—Users can now restart all collectors by clicking "Restart All" in the collectors list page.
- **Third-Party Device and Scan Device trigger**—Two triggers were added for third-party devices and scan features. Users can set these triggers through CLI commands. Both third-party devices and scan devices are disabled by default.
- **System monitor enhancement**—Disk space usage and system resources usages are now displayed in the Log Type module and System Setting module.
- **System Monitor support**—Users can now select the System Monitor in Reports and add System Monitor widgets in Dashboard.
- **Backup enhancement**—Backup drop time partitions have been enhanced to improve performance.
- **Title changes**—Some module titles have been changed.
- **New parameters**—The following parameters have been added for Dashboard charts: Y is Percentage, Y Max Value, and Tip Type.
- **Flex widgets**—The Availability chart and Risk Trend chart have been converted from Flex to JS.

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. For devices from third-party vendors, contact Fortinet Customer Service and Support for more details: https://support.fortinet.com.

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

* 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	FortiWeb	5.5	Syslog	All log types

Hardware support

FortiAnalyzer-Big Data 3.3.0 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 3.2.1 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
0308143	The aggregation task occasionally fails due to lock wait timeout.
0385842	The IP field can't be edited from the FortiView filter.
0388651	Event main type is displayed with an eventMainType id.
0416594	ADOM users can occasionally see devices belonging to other ADOM users.
0424194	Using the back feature in FortiView resets filter parameters.
0424509	Some definitions for report template 9005012 are incorrect.
0435680	Backup tasks will not finish if an Oozie task is suspended.
0438357	Users will occasionally be unable to set up collectors for new devices.

High Performance Network Security

Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.