SECURITY MANAGEMENT

FortiAnalyzer-Big Data Release Notes

VERSION 3.3.1

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, August 23, 2017

FortiAnalyzer-Big Data 3.3.1 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 3.3.1, build 0373. 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 Server 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:

- **Remote authentication**— FortiAnalyzer-Big Data supports remote authentication of administrators using Remote Authentication Dial-In User Service (RADIUS), Lightweight Directory Access Protocol (LDAP), and Terminal Access Controller Access-Control System Plus (TACACS+) servers.
- **System monitor**—System Monitor now supports Log Rate History and Log Rate Details. Log Rate displays the rate at which FortiAnalyzer-Big Data receives logs over a specified time period. This information is categorized depending on the widget it is accessed from.
  - The Log Type widget displays Log Rate data categorized by log type.
  - The Collector Server widget displays Log Rate data categorized by collector server.
  - The Device widget displays Log Rate data categorized by device.

  Users can also view Log Rate details categorized by log type, collector server, device, or VDOM.

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. User-defined templates may be provided by engineering when introducing support for new Fortinet devices or software releases.

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	4.3/4.4/5.5*	Syslog	Attack/Traffic/Event

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

Hardware support

FortiAnalyzer-Big Data 3.3.1 supports the following hardware platforms:

- FortiAnalyzer-Big Data 3000D
- FortiAnalyzer-Big Data 4000D/4100D
- FortiAnalyzer-Big Data 4500D/4600D

Upgrade instructions

This is a minor release of FortiAnalyzer-Big Data. To upgrade from FortiAnalyzer-Big Data 3.3.0 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
0411567	The log in script.log is incorrect after the CS blade fails to resync data from the DB blade.
0438165	Log view caches logs when downloading data.
0439884	Users without view event permissions can still access the Log view and FortiView menus.
0440062	Users without view menu permissions can view the menu, as long as they have permissions related to the menu.
0442089	FortiAnalyzer-Big Data cannot generate PDF reports if the Report File Name contains spaces.
0442311	Users without view password permissions can occasionally see Password Policy settings.
0443762	Upgrades from version 3.2 to 3.3 will fail due to third party device control settings.
0443934	S3Rule_System.drl has the wrong empty srcIP filter condition.
0443938	FortiAnalyzer-Big Data will, under specific circumstances, repeatedly generate logical correlation events.
0439524	The collector server will collect duplicated logs when one device IP is a subset of another device IP.
0445137	The scan task timeout period is too short to fully receive a large file when the scan server is operating at a low performance level.
0445278	FortiAnalyzer-Big Data cannot scan host groups correctly when the hosts are imported or manually created.
0445611	The web scan cannot generate a report if the website has no real domain and is located in Windows OS.
0445650	Users cannot select user-defined data sources as KRI sources.

High Performance Network Security