FortiADC Release Notes

Version 4.8.1

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

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

Tuesday, October 3, 2017

FortiADC 4.8.1 Release Notes

First Edition

TABLE OF CONTENTS

Change Log

Date	Change Description
09/29/2017	Initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 4.8.1, Build 0970.

To upgrade to FortiADC 4.8.1, see FortiADC Upgrade Instructions.

FortiADC provides load balancing, both locally and globally, and application delivery control. For more information, visit: http://docs.fortinet.com/fortiadc-d-series/.

What's new

FortiADC 4.8.1 release offers the following new features and enhancements:

Management

FortiView—provides a real-time and historical traffic data from log devices by source, domain, destination, threat map, RTT, and application health check. You can filter the data by a variety of attributes, as well as by device and time period.

- Server load balance:
  - Client and server RTT
  - Performance (throughput, CPS, and requests)
  - Health check
  - Sessions and persistence
  - Top locations, browsers, domains, and OSs
- Security (Web Application Firewall, GEO IP, IP Reputation, and DDoS):
  - Threat map
  - Top attacks, Geo IP sources, IP Reputation attacks
- System:
  - System logs
  - Traffic logs
  - System alerts

Server load-balancing (SLB)

- Diameter Load-Balancing—offers the following features:
  - Dispatch Diameter messages to multiple servers
  - Server health monitoring and failover
  - Session ID persistence and source address persistence
- Schedule Pool—supports schedule pool that determines the times the system uses pool servers
- RADIUS persistence enchantment—supports AND/OR persistence relationship for multiple RADIUS attributes
- HTTP Content Rewrite enhancement:
  - Supports add/delete user-defined HTTP header
  - Supports capture groups and back reference regular expressions - Support in rewrite host, URL, referrer, location
- HTTP to HTTPS redirection in one VS:
  - Able to redirect users using only one virtual server

Global load-balancing (GLB)

- GLB protocol extends to work across all FortiADC versions.

System

- Two-factor authentication
  - Supports admin access
  - Two-factor authentication and validation using token by FortiAuthenticator
- RADIUS wildcard
  - Allows admin user authentication wildcard on remote RADIUS and LDAP servers

New hardware platform

- FortiADC 200F (Available on October 1, 2017)

Hardware and VM support

FortiADC 4.8.1 supports the following hardware models:

- FortiADC 200D
- FortiADC 300D
- FortiADC 400D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D
- FortiADC 60F (without HSM and PageSpeed features)
- FortiADC 100F
- FortiADC 200F
- FortiADC 1000F
- FortiADC 2000F
- FortiADC 4000F

FortiADC Release 4.8.1 supports deployment of FortiADC-VM in the following virtual machine environments:

VM environment	Tested Versions
VMware	ESXi 3.5, 4.x, 5.0, 5.1, 5.5, 6.0
Microsoft Hyper-V	Windows Server 2012 R2
KVM	Linux version 3.19.0 qemu-img v2.0.0, qemu-img v2.2
Citrix Xen	XenServer 6.5.0
Xen Project Hypervisor	4.4.2, 4.5

Resolved issues

This sections lists the major known issues that have been resolved in this 4.8.1 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
448680	FortiADC FortiGuard frequently sends packets to Port 53 or 8888,
448126	OSCP import uses HTTP 1.0 without the hostname header.
448122	CRL HTTP request uses HTTP 1.0 without the hostname header.
446972	The Session table and the Persist table under Dashboard > Session Monitor is not visible for read-only access profiles.
446563	The GUI lacks clear hints (screen messages) for importing SSL certificates.
446277	The master device in a high availability (HA) may stop listening on Port 50001.
446265	The system may generate too many SSL handshake failure logs with the error string `"error:0000000".`
444867	FortiADC will present both the local certificate and the CA in verify configuration to clients in server certificate messages if the clocal certificate happens to be issued by the CA configured in the verify configuration.
443058	Changing traffic shaper bandwidth configuration in Link Load Balance > Link Group > Gateway would bring down the link.
443056	Changing link load-balancing method from `LLB_PERSIS_SRC` to `LLB_PERSIS_SRC_DST` would cause CPU usage to spike up to 100%, resulting in GUI freeze.
442260	SNMP queries for virtual server throughput data tend to return 0 (no value).
441930	Layer-4 virtual servers may stop accepting traffic in certain customer scenarios.
441656	The default certificate is set to be the local certificate instead of the local certificate group.
440618	The hardware SSL HA proxy sometimes becomes unresponsive when FortiADC is under heavy traffic or used in complicated configurations.
440224	The GUI treats "co.jp" in alert email address setting as "invalid value".

Bug ID	Description
439850	Traffic reports and logs sometimes show inconsistent data.
438700	When /dev/root directory is full, you are unable to log into the GUI which will display a bad gateway error message.
438168	Asynchronous traffic to an AA cluster could fail when no Layer-4 virtual server is enabled.
437586	FortiADC may not clean error message queue after some failed SSL session hand-shakes, causing normal connections to fail.
435467	Missing script files cause HA nodes out of sync.
434913	Invalid script could cause certain HA proxy daemon to restart.
424588	RDP sessions could be dropped after the number of connections exceeds 200.
423931	The Event System log on the GUI gives no indication when a virtual server s having a problem.
422535	The GLB log shows that SLB servers are frequently disconnecting and reconnecting.
402841	Layer-7 SLB DNS may not function well with zone transfers.
368723	FortiADC did not support multiple RADIUS persistence settings.
452202	The color of network interface icons remains GREEN even when their status is DOWN.

Known issues

This section highlights the major known issues discovered in FortiADC 4.8.1 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 2: Known issues

Bug ID	Description
401984	The IP table rules created by rtsp_vs could not sync to the slave device in HA mode. **Workaround:** You must re-connect to the RTSP server when performing HA sync.
233369	Shutting down the PPPoE interface sometimes could cause the default route to be deleted from the default route table. **Workaround:** Reconfigure the default route table after shutting down the PPPoE interface.
380628	Sometimes, global load-balance link member configuration in HA VRRP configuration could not be fully synced to the slave device. **Workaround:** When that happens, execute the command "`execute ha force sync-config`" to sync the configuration.
379236	Sometimes, the HA slave may still show "not sync" after you've executed the command "`execute ha force sync-config`" in the master node. **Workaround:** Clear the slave configuration, and then execute the command "`execute ha force sync-config`" again.
401508	When FortiADC is in an HA active-passive configuration using a switch in transparent mode with the STP function enabled, traffic could get interrupted briefly when a fail-over occurs. **Workaround:** The interruption occurs because STP needs time to re-learn in order to adjust. This is not a FortiADC issue. You can change STP configuration in the switch to prevent this from happening.
376784	Some traffic log data may get missing when FortiADC is under heavy traffic stress. **Workaround:** Enable traffic logging only in normal traffic conditions; do NOT enable it when CPU usage exceeds 60%.
372459	Sometimes, the floating IP may be missing in the back-end after some operations. **Workaround:** When that happens, reconfigure the floating IP.

Bug ID	Description
414143	The traffic limit control for FortiADC inbound/outbound packets in each VDOM only works for TCP traffic; it does not work for UDP traffic. **Workaround:** Do NOT impose the traffic limit on UDP traffic.
377176	The OSPF neighbor won't be built if the floating IP is the same as the interface IP. **Workaround:** Avoid setting the floating IP the same as the interface IP.
451722	Logging into FortiADc 60F immediately after boot-up may get an error message. **Workaround:** This may be because some daemon is still loading when you are logging in. It does not affect FortiADC in any way.
451957	The CLI on FortiADC 60F may freeze if you make configuration changes while switching from HA mode to standalone mode. **Workaround:** Do not attempt to change the appliance's configuration and HA mode at the same time.
446943	SSL throughput may decrease under certain circumstances. **Workaround:** Tune the tune-bufsize to 16384.
444752	When 300 wildcard administrators using different RADIUS servers in the system, it may take up to 5 minutes to log in. **Workaround:** Try to use no more than 10 RADIUS/LDAP servers for wildcard administrator authentication.
446418	After migrating RADIUS persistence profiles to Version 4.8.1, some vendor-specific attributes may get lost during backup and restore. **Workaround:** Vendor-specific attributes with empty values are for backward compatibility, and not intended for RADIUS persistence. You need to modify the configuration in 4.8.1.
449128	The Web Application Firewall signature page may show inaccurate information. **Workaround:** Update to the latest Web Application Firewall signatures.
449822	Some VDOM configurations may remain in the system if you delete a VDOM shortly after it is created. **Workaround:** Do not create and delete VDOMS in a rapid fashion.
452815	A verify process could fail when a real server is using a certificate signed by an intermediate CA.

Image checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, near the bottom of the page, click the Firmware Image Checksums button. (The button appears only if one or more of your devices has a current support contract.) In the File Name field, enter the firmware image file name including its extension, then click Get Checksum Code.

Figure 1: Customer Service & Support image checksum tool