FortiADC Release Notes

Version 4.8.3

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

Monday, December 18, 2017

FortiADC 4.8.3 Release Notes

First Release

TABLE OF CONTENTS

Change Log

Date	Change Description
12/18/2017	Initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 4.8.3, Build 0983.

To upgrade to FortiADC 4.8.3, 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 4.8.3 is a patch release which mainly involves bug fixes; no new feature or enhancement has been implemented in this release.

Hardware and VM support

FortiADC 4.8.3 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 4.8.3 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 4.8.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
0461874	The system may crash in the process of long-term stability test.
0462594	When too many virtual servers were configured on a global load balancing server, deleting the virtual servers could take a long time.
0462815	When you are editing interface settings, the system would print `"fail to find condition node 2122 for node 2121"` message.
0459513	Keepalived CPU usage was too high.
0461928	The user was not able to create more than 34 VDOMs on FortiADC 1000F.
0464176	Health check would stop functioning when the hasyncd daemon is locked.
0463251	The HTTP proxy could crash when sending Layer-7 HTTP traffic.
0460958	The OCSP timeout did not function as designed.
0458060	Source IP may not work well when starting different connections with the same source IP.
0438654	The system might crash during an HTTP Proxy dump session if the VS is shut down.
0463318	CPU usage could spike to 99% when you execute the `"execute log display 0"` command without filtering.
0463108	An virtual server could become inaccessible after its interface IP address was changed.
0453139	After upgrading boot loader, attempts to test 1KF restart failed.
0461593	A log message contained a typo.
0459530	Some scheduled reports could remain in pending state well past their scheduled time of execution.
0458743	Reports scheduled to start after midnight might fail to generate.
0458137	The Dashboard shows "Availability: No Policy" for objects with their hostnames set as '@'.

Bug ID	Description
0459959	The system did not forward authorization to a real server when the authentication policy is using a normal group-type.
0457387	A Diameter virtual server might not forward client responses to the intended real server.
0457608	A Diameter virtual server could not reply to DPA when a real server sends DPR requests.
0459570	The HTTP proxy could crash under circumstances.
0458236	FortiView displays an incorrect alert message when a bad IP pool was configured.
0459361	LDAP would run into bind failure for admin log-in.
0456686	Important information was lacking in SNMP traps for expiring SSL certificates.
0458663	FortiADC HA mode for SNMP Query showed incorrect HA mode.
0456825	Layer-7 virtual severs would close connections with the "`503 Service Unavailable`" error.

Known issues

This section highlights the major known issues discovered in FortiADC 4.8.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 2: Known issues

Bug ID	Description
0401984	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.
0233369	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.
0380628	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.
0401508	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.
0376784	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%.
0372459	Sometimes, the floating IP may be missing in the back-end after some operations. **Workaround:** When that happens, reconfigure the floating IP.
0414143	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.

Bug ID	Description
0377176	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.
0451722	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.
0451957	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.
0446943	SSL throughput may decrease under certain circumstances. **Workaround:** Tune the tune-bufsize to 16384.
0444752	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.
0446418	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.
0449128	The Web Application Firewall signature page may show inaccurate information. **Workaround:** Update to the latest Web Application Firewall signatures.
0449822	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.
0452815	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