FortiADC Release Notes

Version 5.2.4

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

Friday, July 12, 2019

FortiADC 5.2.4 Release Notes

First Edition

TABLE OF CONTENTS

Change Log

Date	Change Description
07/12/2019	FortiADC 5.2.4 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.2.4, Build 0454.

To upgrade to FortiADC 5.2.4, 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 5.2.4 is a patch release only; no new feature or enhancement has been implemented in this release.

Upgrade notes

CVE-2017-17544

To fix the vulnerability CVE-2017-17544, only super admin are allowed to restore configuration from 5.2.3

Hyper-V

New template for Hyper-V 2016/2019 support

Statistics data format converting

After upgrading to V5.2.3, the old statistics data will not be converted to the new version automatically; instead, there is a warning on the top right position. The client may click the warning to start the converting. However, the converting may consume CPU and memory resources. Only clients upgrading from prior to 5.2.0 can have old statistic data.

allow-ssl-version

There is an old SSL version in the allow-ssl-version config that is not recommend; but the client may have configured it before. This is removed when you upgrade from 5.0.x to 5.1.x/5.2.x. The client may need to add it back manually for compatibility.

Adjust boot partition

VM's prior to 5.1.x had a size limit to the boot partition. Thus, you need to upgrade to 5.1.x, first, to adjust the boot partition. Then you can upgrade to 5.2.3. Otherwise it will report "Unmatched partition size."

No such issue for physical platforms.

Dynamic auth feature

It is suggested that the customer should only enable "dynamic auth feature" on RADIUS accounting virtual servers.

Hardware and VM support

FortiADC 5.2.4 supports the following hardware models:

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

FortiADC Release 5.2.4 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, 6.5, 6.7
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 section lists the major known issues that have been resolved in this 5.2.4 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
0556273	udproxy process consumes high cpu utilization in some special circumstances.
0534085	Need to clear ocsp cache items when editing ocsp memory size.
0552273	GUI cannot show signature description which has header tag <A>.
0567631	There should be a warning if a conflict occurs when changing GLB location
0567345	GLB server-performance works reverse for CPU and memory.
0558190	Changing the IP address range of the NAT Source Pool in HA-VRRP mode may not work.
0564591	Healthcheck match string fails if header is greater than 4096 bytes
0563908	A httproxy-ssl crash happens sometimes
0562231	There could occur a server-unavailable error for L7-HTTP/HTTPS VS when concurrent session is high.
0560927	OU are increased depending on number of space when generating local certificate through GUI.
0553011	The validation necessary to check local crt is issued by issue crt on OCSP Stapling page.
0558956	Unable to change the ahead time/interval on OCSP Stapling.
0561679	When saml-sp and idp use long name the shibd ps does not start.
0561466	In AWS, migrating floating IP could fail when the HA failover occurs.
0555980	There could occur an httproxy crash when the WAF of L7-HTTP/HTTPS VS is enabled and large amounts of traffic are going through the VS.
0550571	GLB statistic total response number will add "2" to its count even if sending only one DNS response.
0554666	L4 traffic is reconnected and stopped if status is set from enable to maintain in "Real Server".

Bug ID	Description
0558820	For OCI, the output of the console is cut off when the ADC reboots.
0481306	Rebooting ADC via OCI reboot button takes more than 15 minutes.
0551354	Lost ip address when changing the Interface mode from dhcp to static.
0557564	ADC cannot forward icmp(type 0, code 4) to RS on L4VS mode.
0550399	lb routing in script does not work when a content-routing name contains another content-routing name.
0555919	There could occur a memory leak if the WAF is enabled in particular conditions.
0556292	Interface speed does not negotiate correctly after upgrading OS from 5.1 to 5.2.
0552401	The traffic could still be forwarded to a no longer existent real-server if the session doesn't expire in some circumstances.
0551735	Some operations combinations on GUI may lead to log filters not work properly.
0555060	RTT and APP response in RS reversed on Fortiview.
0554604	Using HTML form on 'Client Authentication Method' removes character from LDAP username.
0551142	L7 FTP traffic goes to backup RS when persistence is enabled.
0526487	Loss support of "abort-on-close" option could lead to mobile Email not refreshing properly.
0552367	Particular operation order on GUI could lead to log filter dropdown becoming abnormal sometimes.

Known issues

There are no known issues discovered in FortiADC 5.2.4 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

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