FortiADC Release Notes

Version 5.2.3

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

Friday, May 17, 2019

FortiADC 5.2.3 Release Notes

First Edition

TABLE OF CONTENTS

Change Log

Date	Change Description
05/01/2019	FortiADC 5.2.3 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.2.3, Build 0446.

To upgrade to FortiADC 5.2.3, 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 5.2.3 offers the following new features:

Add a “response-half-closed-request” option to HTTP/HTTPS/TCPS/RDP load-balance profile

This option will allow the FortiADC to serve the request and send back the response even if the client closes the output channel.

In some cases, the client may close the output channel even after sending out the request; but at the same time the client will be waiting for a response. If this option is disabled, the FortiADC will abort, and will not serve the request anymore once it receives notice that the client has closed the channel. This may cause clients tocomplain of failures.

Forward SNI to RS under ssl-forward-proxy mode

In SSL forward deployment, the second ADC (HTTP->HTTPS) may not forward any SNI to backend Real Server, causing failure for some servers. In this feature, if “SNI forward flag” in server SSL is enabled, it will forward host in HTTP header as SNI to Real Server by default. If there is no host in HTTP header, it will forward the ssl-sni settings as SNI to Real Server.

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 5.2.3 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 5.2.3 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, 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 5.2.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
0546520	Kernel memory leak issue for L4 VS
0546251	Switching ports on FADC occasionally loses member ports previously configured on GUI
0546827	High CPU usage was caused by TCP half type health check when networking down
0548490	When using CHASH method, L7VS was forwarding traffic to a server that was disabled
0549539	Import cert failed by REST API because of the size limit, but no error in response
0550011	In Fortiview SLB session chart, it only showed no more than 100 sessions
0545652	Virtual Tunnel in LLB may drop packets with CHASH method after interface physically turns off and on again
0549758	IP pool exhaust alert caused when packet TTL equals 0
0551142	L7 FTP traffic goes to backup RS when persistence is enabled
0550194	Importing san-certificate for management makes https go down, because of a bug when it handles rsassaPss signature algorithm
0551144	Corrected the GSLB backup state propagation on FortiView
0547931	FortiADC VM vulnerability to CWE-250
0526487	Mobile Email Not Refreshing because client shutdown channel before receive the HTTP response
0539896	Get duplicate L7 VS entry after deleting the entry and adding it back
0552895	HTTP VS may crash when using SSL session id as persistence in HA deployment
0549676	Deploy FortiADC VM on Hyper-V 2016/2019 by importing template failed
0551735	Logs may disappear after filter changes when browsing

Bug ID	Description
0553318	DDOS statistics on dashboard are not showing properly
0538163	Admin User Authenticated by LDAP Cannot Change the ‘Global Admin’ Value
0552636	FortiADC vulnerability to CVE-2017-17544
0552901	Sync List Not Working
0553019	Increase the Health Check size limit to 512
0547736	Support successful SSL session logging by option in client-ssl-profile

Known issues

This section highlights the major known issues discovered in FortiADC 5.2.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 2: Known issues

Bug ID	Description
523216	If a prior-to-5.1.2 backup configuration is saved by an admin user who happens to have '_' in his name, the configuration will not be listed after upgrading to 5.2.3. **Workaround**: before upgrading to 5.2.3, redo the backup with another admin user whose name does not include '_'.
515275	5.2.3 Global Load Balance supports a new "server-performance" method in the virtual server pool. But remote servers which are running images prior to 5.2.3 will not report information to the 5.2.3 GLB server. As a result, it will be treated as the worst performance server in the pool.
526074	In the slave device of HA AP mode, it may fail to ping its HA mgmt IP.
518447	On Google Cloud Platform (GCP), the VM does not support the following features: • HA AP mode • HA AA mode • Floating IP of interface • IPv6 • Vlan interface • Softswitch interface • Aggregate interface
530020	On Azure the VM does not support the following features: • HA AP mode • HA AA mode • VLAN interface • Softswitch interface • Aggregate interface

Bug ID	Description
530017	On AWS the VM does not support the following features: • HA AP mode • HA AA mode • VLAN interface • Softswitch interface • Aggregate interface
524335	SIP sessions CPS performance drops, when source address is enabled
518048	In FortiGuard Services, please remember that the system will reload and traffic may interrupt after upgrade/reset "Geo IP"
528695	In Cloud platform(AWS/GCP/AZure/Aliyun), after changing the IP settings in ADC, like VS IP, interface ip/secondary ip etc, please also change the IP configuration of the interface in cloud networking.
514583	In GUI>Global>System File, it is only able to upload a file up to 300MB.

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