FortiADC Release Notes

Version 5.2.1

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

Friday, February 8, 2019

FortiADC 5.2.1 Release Notes

First Edition

TABLE OF CONTENTS

Change Log

Date	Change Description
1/29/2019	FortiADC 5.2.1 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.2.1, Build 0430.

To upgrade to FortiADC 5.2.1, 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 5.2.1 offers the following new features:

Security

Fortinet Security Fabric support

The Fortinet Security Fabric delivers broad protection and visibility to every network segment, device, and appliance, whether virtual, in the cloud, or on-premises. After adding FortiADC to Security Fabric, it will show the real-time visibility of FortiADC, including Virtual Server status, and various statistics.

Web Cache Communication Protocol (WCCP) support

The Web Cache Communication Protocol (WCCP) allows the server to be enabled for transparent redirection to discover, verify, and advertise connectivity to one or more web-caches. You can configure FortiADC as a WCCP server to redirect HTTP/HTTPS VS traffic to 3rd party device for caching or more security inspection.

Global Load Balance

DNS notification and zone transfer

Allows FortiADC DNS service to send zone notification to slave servers, and also receive and process incoming zone transfer message from slave servers.

Public/private IP support for SLB server behind NAT

Customer can provide a public IP address for the GLB discovered virtual server address, which is necessary for the deployment which whose server is behind NAT.

Allow multiple PTR DNS Resource Records with the same IP address

Service Load Balance

Radius Change of Authorization (CoA) message support

The Radius Change of Authorization (CoA), defined in RFC5176, provides a mechanism to dynamically change the attributes of an AAA session after the user or device is authenticated. By this feature, FortiADC can process CoA messages from external Radius server and send the traffic to the right dynamic authorization server through persistence.

System

CRLDP authentication protocol (RFC5280) support

Certificate Revocation List Distribution Point (CRLDP) defines how to get a CRL file from a distribution point, which is LDAP URI or HTTP/HTTPS URL, to verify client certificate.

Download CRL file from LDAP server

Support multiple CRL files for a single certificate verification object

Log reporting enhancement for more virtual server statistics

Collect statistics like RPS, CPS, transaction latency, session duration, throughput per virtual server/real server, and generate reports including these metrics.

Traffic log browser GUI redesign

Usually if you enable traffic log, there will be a huge volume of traffic logs. In this situation, to browse or filter traffic log is much too slow; with this feature, we redesign the traffic log browser page to show and locate logs quickly.

Upgrade notes

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 5.2.0. Otherwise it will report "Unmatched partition size."

No such issue for physical platforms.

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

Hardware and VM support

FortiADC 5.2.1 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 5.2.0 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 section lists the major known issues that have been resolved in this 5.2.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
531477	"keepalived: checker" daemon not optimized to utilize more CPU resource
0534894	Can configure two VS with same IP and same port. GUI and CLI do not give error
0524984	Files sent to FortiCloud sandbox could take too long; a per-minute limit has been added
0498312	Checking traffic log causes higher CPU
0526581	Ability to search Virtual Server is missing in 5.1.x
0527717	FortiADC on SLB L7, -- the amount of connection of the "Connection Limit" setting in VS is exceeding the threshold configured
0536248	Ldap in crldp causes memory leak
0524984	Add per-minute limit for sending files to FortiCloud sendbox
0529777	Memory increases over 7 day period, then drops back down
0535725	ADC forwards CoA-ACK with wrong source and destination ports in non-root vdom.
0529639	ADC cannot sync CoA table between nodes.
0442462	Vendor-Specific radius attribute with the same id and type can be configured by modifying the existed radius attribute.
0529099	Fortiview SLB dynamic charts empty out when it has attack fast report
0535026	The 0 entry in report is not the same format.
0529812	The 'setting' button on Quarantine Monitor page does not work.
0533692	GLB VS IP and information are not updated when auto-sync is enabled, or when refreshing after changing theVS type in SLB
0531238	The command execute update-now does not work.

Bug ID	Description
0532797	Supports GLB PTR record for same address
0530651	if one restapi is locked, other restapi do not work, causing login fail
0530390	code commit for support DNS zone transfer and notification
0526897	httproxy memory leak occurs when set/unset content routing and scripting config to VS for a long time
0532612	httproxy crashed on customer side
0529215	Dynamic Resources shows "Concurrent Session" with max value

Known issues

This section highlights the major known issues discovered in FortiADC 5.2.0 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 5.2.0. **Workaround**: before upgrading to 5.2.0, redo the backup with another admin user whose name does not include '_'.
515275	5.2.0 Global Load Balance supports a new "server-performance" method in the virtual server pool. But remote servers which are running images prior to 5.2.0 will not report information to the 5.2.0 GLB server. As a result, it will be treated as the worst performance server in the pool.
526074	In theslave 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.
523216	If the backup configuration is saved by admin user whose name includes '_' before 5.1.2, it will not be listed after upgrading to 5.2.0 **Workaround**: Before upgrading to5.2.0, redo backup by another admin user which name not includes '_'
515275	Global Load Balance supports new "server-performance" method in virtual server pool, but for the remote servers which are running an image before 5.2.0, it will not report performance information to GLB server, so it will be treated as the worst performance server in the pool.
526074	In slave device of HA AP mode, ping HA mgmt ip of itself may fail
518447 518448 518446 518449 517138	On Google Cloud Platform(GCP) VM does not support the following features: • HA AP mode • HA AA mode • Floating IP of interface • IPv6 • VLAN interface • Softswitch interface • Aggregate interface

Bug ID	Description
530020	On Azure the VM does not support the following features: • HA AP mode • HA AA mode • VLAN interface • Softswitch interface • Aggregate interface
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 be reminded that the system will reload and traffic may be interrupted after you upgrade/reset "Geo IP"
528695	In Cloud platform(AWS/GCP/AZure/Aliyun), after changing the IP settings in ADC, like VS IP, or interface ip/secondary ip etc, please also change the IP configuration of the interface in cloud networking
514583	GUI>Global>System File, -- it only supports uploading a file up to 300M.
0537052	After the customer upgrades to V5.2.1, the ADC will take some CPU resources to transform the old data to new format, possibly resulting in higher CPU usage for some time.
0537058	If the VDOM is not enabled, the WCCP can only be configured on CLI. However, if the VDOM is enabled, you can configure it on both CLI and GUI.

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