FortiADC Release Notes

Version 5.2.0

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, December 21, 2018

FortiADC 5.2.0 Release Notes

First Edition

TABLE OF CONTENTS

Change Log

Date	Change Description
12/14/2018	FortiADC 5.2.0 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.2.0, Build 0423.

To upgrade to FortiADC 5.2.0, 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 5.2.0 offers the following new features:

Server Load Balance

L2 TCP/UDP/IP VS support content routing

Supports specific routing (schedule pool, persistence, method) by source address

L7 FTP VS with FULLNAT/DNAT/Transparent mode support

Oracle DB health check support on VM platforms

Dynamic Load method enhancement

Prior to 5.2.0, all connections are cleared if RS is detected to be exceeding the threshold; now, however, when RS exceeds the threshold, the old connection is kept while not dispatching new connections

Fully ADFS proxy replacement

The ADFS Proxy is a service that brokers a connection between external users and internal ADFS servers, also called a Web Applicaition Proxy (WAP). More and more ADFS require the proxy to support MS-ADFSPIP (ADFS Proxy Integration Protocol) which involves client certificate authentication between proxy and ADFS, trust establishment, header injection, and more. FADC from 5.2.0 has support for MS-ADFSPIP.

SIP VS enhancement:

- support NAT of Media server address
- keep client address of UDP traffic for SIP server

Script new support function:

- Authentication event and operation
- Cookie encrypt/decrypt
- AES encrypt/decrypt
- crypto hash/sign/verify
- URL encode/decode/parse
- Base32
- File operation
- Random generation
- get_pid
- HTTP:respond

Global Load Balance

New dispatch method by server CPU/Memory usage

The "Server-Performance" method dynamically dispatches the DNS request to the server with the lowest CPU/Memory usage

Security

Web Vulnerable Scanner report enhancement

JSON schema validation support

JSON Schema provides a contract for what JSON data is required for a given application and how to interact with it. This feature supports the user uploading a JSON schema to validate JSON data, just like the XML validation that we had before.

IP Reputation black list support

Now possible to upload a list of IPs or CIDRs to the IP reputation black list, then blocking them by enabling "IP reputation" in Application Profile for VS.

Antivirus quarantine monitor page on GUI

New function to show/delete quarantined files on FortiADC by GUI (Network Security -> Quarantine Monitor)

All the certificate private key file on the ADC are encrypted now for more security

Dynamic TLS record sizing support to improve SSL latency and throughput

GEO support more accurate province

System

AWS/GCP/Azure/Aliyun BYOL VM support

Now supports uploading and deploying VM images on these public cloud platforms; you can easily extend existing FortiADC services to the cloud.

HA failover enhancement to avoid unnecessary switch after slave(former master) return back

In HA AP scenarios, the slave device will become master if the master device is down, but after the former master comes back, there will be a new switchover (the former master takes the master role, and the current master, the former slave, switches back to slave). This switchover is unnecessary and may impact traffic, so the enhancement here is to avoid doing the switchover after the former master comes back.

Debug enhancement, support collect all debug information and download by GUI

Before, in order to submit information to Help Support, the customer needed to gather files from different places; now, this debug enhancement automatically collects all necessary debug information into one file, so it's easier to submit to Help Support.

Support to upload/download a file to/from FADC by GUI

Support FortiADCManager

FortiADCManager is a central management tool to manage all your FortiADC devices in your network, providing visibility and the ability to create/edit server load balance configurations for all FortiADC devices.

Upgrade kernel to latest version

Support “| grep <fileter-string>” to filter the output on CLI

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.

Hardware and VM support

FortiADC 5.2.0 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
0505200	Can't delete the content routing and rewrite rules after turning off the content on VS
0518690	Security vulnerability on Health Check Script
0524114	Creating admin user from CLI doesn't respect the regexp that is required by the GUI
0512946	VIP response ICMP unreachable with translated real server IP instead of its external IP
0523086	Management interface answered to ICMP timestamp request
0518040	SMTP VS hangs up resulting in TCP reset connection in some scenarios
0503902	Username and version displayed incorrectly under System > Settings
0515939	Uneven distribution to real server pool members
0516532	Cross-site scripting vulnerability, for some encoded scripts
0521332	Email Alert doesn't work
0521273	ADC doesn't respond to dns request for several minutes
0514525	CLI `execute ping6-option source` failed
0526560	Multiple event log like "xxx has dropped below its connection limit xx sesssions" with very few connections
0525427	Health Check of "TCP Half open connection" not working properly
0528552	Health Check of "L2 Detection" may not work on non-root vdom
0527999	MYSQL VS crash on 60F platform in some cases

Bug ID	Description
0527547	Status crash happens during delete vdom and reboot
0523625	System event log message ID is not right after upgrading and causes disorder when vdom name is long
0527030	LLB link policy's iif filter can't work well under non-root vdom
0526599	Aggregate interface aggregate-algorithm is not allowed to change
0523201	DNS service vulnerability fix(CVE-2017-3135/CVE-2017-3136/CVE-2017-3138/CVE-2017-3142/CVE-2017-3143)
0525649	Restore av-package via tftp may fail in some cases
0529081	L7 VS session table information is missing RS name
0527717	In HTTP VS, the amount of connection in fortiview is exceeding the configured connection-limit threshold

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.

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