FortiADC Release Notes

Version 5.1.4

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, March 15, 2019

FortiADC 5.1.4 Release Notes

First Edition

TABLE OF CONTENTS

Change Log

Date	Change Description
03/15/2019	FortiADC 5.1.4 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.1.4, Build 0262.

To upgrade to FortiADC 5.1.4, 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/.

Upgrade notes

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.

Refresh

After upgrading from 5.0.x to 5.1.4, please remember to press "Ctrl + F5" to force refresh GUI.

Hardware and VM support

FortiADC 5.1.4 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 5.1.3 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 section lists the major known issues that have been resolved in this 5.1.4 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
0540882	[V5.2.2 B0433] HA-AP: Can't exit a telnet session (of 'execute ha manage 0').
0538103	Changing the DNS server config, restapi & authd still use the old dns server to fetch domain.
0538416	DNS Zone changes don't generate higher serial numbers. Zone transfers to DNS slaves aren't possible.
0543288	should show warning for memory when using persistence only for L7 http/https
0540066	Kernel Panic after activating FTP Load Balancer config (1500D)
0537952	There should be a hint to warn user the source-address persistence for L7-VS may lead high memory consumption.
0539896	After upgrade from 4.8.6 to 5.1.3 and L7VS and duplicate entry errors
0542860	Restful API crash happened during daily build automated testing.
0529928	Certificate verify using CRL with longer CN name fails.
0538679	Increasing DNS Max values
0539608	SSL version sslv3 tlsv1.0 lost if sslv2 is not select after update from 5.0.x to 5.1.x/5.2.x
0530612	change GLB zone allow transfer address group not take effect
0543331	unable to login using http and https listen port after upgrading image
0527717	FortiAD on SLB L7, the amount of connection of the "Connection Limit" setting into VS is exceeding the threslhold configurated
0541180	restapi crash when uploaded fortiguard library by restful
0542860	Restful API crash happened during daily build automated testing.
0541877	getty: ttyS0: ioctl: Input/output error

Bug ID	Description
0541332	when virtual server using hash related persistence the pool member connection-limit is not working
0539199	SSL VS failed to load after upgrading to 5.2.1 from 5.0.3
0536549	radius health check is not work
0536411	Fortiview security logs shows empty and not show correct page
0534284	no statistic for log event when edit dashboard and enable/disable log event
0539168	IP Reputation DB not updated and thus IP reputation not working

Known issues

This section highlights the major known issues discovered in FortiADC 5.1.4 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 2: Known issues

Bug ID	Description
0468417	Changes made to the destination port of the VXLAN tunnel do not take effect on the listening port. **Workaround:** Normally, you do not need to change the destination port. If you do, be sure to reboot the system.
0465516	The order of the Interfaces could get changed after removing and re-adding an interface to FortiADC in an OpenStack environment. **Workaround:** Determine the number of interfaces before configuration, and try not to delete interfaces in an OpenStack environment.
0470620	OpenStack Ibass cannot connect to backup FortiADC devices after a failover. **Workaround:** Manually configure the device settings when FortiADC is in HA-AA or HA AA-VRRP mode.
0471518	For Layer-2 and Layer-4 TCP or TCPS porfiles, and Layer-7 Turbo HTTP profile, the FortiView>Server Load Balance>Virtual Server page can display Throughput, Concurrent Connections, and Health Status of virtual servers or real servers.
0471525	If `client-certificate-verify-option` in a client_SSL_profile is set to "Optional", the persistence type LB_PERSIS_SSL_SESS_ID will not work in a virtual server which uses the client_SSL_profile. **Workaround:** Do NOT set `client-certificate-verify-option` in a client_SSL_profile to "Optional".
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.

Bug ID	Description
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 go 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.
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.
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.
0448922	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.

Bug ID	Description
0481306	On the Oracle OCI compute instance management page, rebooting an instance may take more than 10 minutes. **Workaround**: This is OCI-specific issue. Reboot Oracle OCI instances from FortiADC GUI or Console instead.
0499140	Sometimes, the **Web Application Firewall> Web Attack Signature> Signature** page does not show detailed information. **Workaround**: Refresh page, or switch to another page and then switch back.
0495277	After a file is submitted to FortiSandbox, it may take a while for the AV module to generate the "File submitted to Sandbox" log.
0488973	"diagnose antivirus database-info" shows version in format like 05/03/0018 instead of 05/03/2018.
0499175	The Web Vulnerability Scanner task page cannot refresh automatically. **Workaround**: Once a new task has started, click the Refresh button to get latest task status.
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 to 5.2.0, redo backup by another admin user whose name does not include '_'
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.
542995	HSM only supports V5.

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