FortiADC Release Notes

Version 5.0.0

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

Monday, March 5, 2018

FortiADC 5.0.0 Release Notes

Second Revision

TABLE OF CONTENTS

Change Log

Date	Change Description
03/05/2018	Second revision. • Removed "SSL update" from "What's new". • Added Bugs 0471525 and 0471518 to "Known issues".
02/26/2018	First revision, adding Bug 0475733 to the Known Issues section.
02/01/2018	FortiADC 5.0.0 Initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.0.0, Build 0045.

To upgrade to FortiADC 5.0.0, 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 5.0.0 offers the following new features and enhancements:

Security Fabric

- FortiSandbox integration—You can now use a file upload restriction policy to submit uploaded files to FortiSandbox for evaluation. If FortiSandbox identifies a file as a threat, FortiADC generates a corresponding attack log message and blocks further attempts to upload the file.
- Antivirus—FortiADC now supports the FortiSandbox's Malware Signature Database. This feature is available on all FortiADC hardware platforms, except FortiADC 60F.

Management, GUI, and logs

- Dynamic Dashboard—You can customize the Dashboard according to your preferences
  - Create or edit a dashboard
  - Add or remove Dashboard widgets
- FortiView enhancement—Adding new statistics for
  - Server load balancing—Caching, Compression, and SSL
  - Link load balancing
  - Global load balancing
- Alert system enhancement—Allow to configure alert threshold based SLB (BW, Client RTT, or Connection) and Interface Avg. Bandwidth.
- Automated configuration backup via FTP/SFTP

Server load balance (SLB)

- Layer-4 virtual server tunnel—In tunnel mode, FortiADC encapsulates the packet within an IP datagram and forwards it to the chosen server.
- Diameter Load balancing SSL enhancement—FortiADC supports Diameter traffic over SSL (client SSL).
- Source Pool NAT in Layer 7—Now it’s possible to configure pool NAT when using Layer-7 virtual servers.

Global load balance (GLB)

- Global load balancing authentication—Provide TCP-MD5SIG or authentication verify between two or more FortiADC appliances working in global load balancing.

Scripts and predefined commands

Scripts

- CLASS_SEARCH_n_MATCH
- OPTIONAL_CLIENT_AUTHENTICATION
- UTILITY_FUNCTIONS_DEMO (updated)
- COOKIE_COMMANDS
- IP_COMMANDS
- MANAGEMENT_COMMANDS
- SSL_EVENTS_n_COMMANDS
- TCP_EVENTS_n_COMMANDS

Web Application Firewall (WAF)

- SOAP validation—Enhances ForitADC's WAF B2B features with SOAP messages validation. It allows you to perform SOAP validation using a Web Services Description Language (WSDL) document.

SSL

- OCSP verification caching—Allows to speed up OCSP checking using OCSP caching. The first time a client accesses FortiADC or FortiADC accesses a real server, FortiADC will query the certificate’s status using OCSP and cache the response.
- Dual certificates (RSA and ECDSA) support—Allows you to create certificate groups containing both RSA and ECDSA certificates for improved SSL performance.
- Support SSL renegotiation—FortiADC now supports SSL renegotiation between client and server. It allows the use of the existing SSL connection when client authentication is required.

System

- Openstack integration—FortiADC provides load balancing services for OpenStack cloud applications. With Openstack integration, FortiADC is able to provide load balancing functionality and advanced application delivery services within OpenStack.
- NVGRE and VXLAN support—FortiADC allow to use overlay tunnel with virtual network NVGRE and VXLAN segments in either multicast (VXLAN) and unicast (NVGRE/VXLAN) modes.
- BGP Route Health Injection (RHI)—Allows to advertising route to virtual address based on the health status of the corresponding service

Hardware and VM support

FortiADC 5.0.0 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 5.0.0 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 sections lists the major known issues that have been resolved in this 5.0.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Note: This 5.0.0 release has also fixed all the known issues found in 4.8.1, 4.8.2, 4.8.3, and 4.8.4 releases, even though they are not listed here.

Table 1: Resolved issues

Bug ID	Description
0468169	The Script Log is not sent to the syslog server.
0467459	HTTPS health check does not send "hostname" as part of the SSL client hello SNI extension.
0466098	Cross-site scripting vulnerability was reported.
0464807	FortiADC fails to take the default action (overwrite) when the disk space used for local logs has reach 30% of the total disk space.
0642848	Double-byte characters could be used in the name of "client-ssl-profile" and "LB Method" configurations.
0462200	CPU usage might shoot up and remain high after a Layer-7 virtual sever was deleted.
0459570	HTTP requests without the "User-Agent" header could lead to HTTP proxy crash.
0458947	Valid and expired certificates could show up in "Pending" status.
0455894	The default Geo IP action (Deny) is not logged in the GEO IP Security Log.
0454565	FTP data traffic was delayed by nine seconds while going through FortiADC.
0441446	Packet accepted by a firewall policy is not forwarded if the firewall policy's default action is "Deny".
0439646	The Script Log on the GUI doesn't work.
0436405	The system went into a Kernel panic during stress tests.
0434781	The operator `"ends_with"` was mistakenly written as `"ands_with"` in the Handbook.
0469920	Underscores are allowed in certain DNS entries.

Bug ID	Description
0469848	An admin user was not able to log into the system via the PAP protocol if the remote server is a Cisco ACS server.
0463318	The logging process could cause high CPU usage (99%).
0463108	A virtual sever could become inaccessible after its interface's IP address is changed.
0459530	Scheduled reports could remain in pending state.
0459361	The LDAP remote server was unable to authenticate a user with the Regular Bind Type in its domain credentials.
0461774	The Handbook Admin does not mention HTTP-HTTPS toggle in virtual sever settings.

Known issues

This section highlights the major known issues discovered in FortiADC 5.0.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 2: Known issues

Bug ID	Description
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".
0475733	Script content was lost when downgrading from 5.0.0 to 4.8.4. **Workaround:** Downgrading from 5.0.0 to lower versions is not supported. Be sure to back up your configuration before upgrading to 5.0.0.
0471418	No report can be generated when the report disk is full. **Workaround:**Delete some old reports.
0470620	The OpenStack Ibass cannot connect to the backup FortiADC after a failover. **Workaround:** Manually configure FortiADC settings when it is used in HA-AA or HA AA-VRRP mode.
0465516	The interface sequences are changed after removing and adding back an interface to FortiADC in an OpenStack environment. **Workaround:** Check the number of interfaces before configuration, and avoid deleting interfaces from an Openstack environment.
0466316	Disabling WAF SOAP-WSDL or XML-Schema would not unset the related WSDL file. **Workaround:** By design, you must re-enable the SOAP-WSDL or the XML-Schema in XML-validation first before changing it to any other file or resetting it to empty first.

Bug ID	Description
0471332	CPU usage could reach 100% when browsing traffic logs. **Workaround:** Only huge log on a virtual machine could trigger this issue. CPU usage will come down after a few seconds.
0468417	Changes made to the VXLAN tunnel destination port does not take effect on the listen port. **Workaround:**In general, changing the destination port is NOT recommended. If you ever want to change it, be sure to reboot the system after the change is made.
0464862	The Remote IP Monitor health check still works after setting HA to standalone. **Workaround:** You MUST disable the remote gateway monitor before switching to standalone mode.
0455272	Restoring the configuration of a lower version to a 5.0 system may result in GEO IP-related configuration loss. **Workaround:**Do not attempt to restore a lower-version configuration to a v5.0 system directly.
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.
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.

Bug ID	Description
0376784	Some traffic log data may get 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.
0446418	After migrating RADIUS persistence profiles to Version 4.8.1, some vendor-specific attributes may get lost during backup and restore. **Workaround:** Vendor-specific attributes with empty values are for backward compatibility, and not intended for RADIUS persistence. You need to modify the configuration in 4.8.1.
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.

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