

FortiADC Release Notes

Version 5.0.3

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



Wednesday, July 18, 2018

FortiADC 5.0.3 Release Notes

First Edition

TABLE OF CONTENTS

| | |
|--------------------------------------|-----------|
| Change Log | 4 |
| Introduction | 5 |
| What's new | 6 |
| UDP Stateless LB..... | 6 |
| Hardware and VM support | 7 |
| Resolved issues | 8 |
| Known issues | 10 |
| Image checksums | 13 |

Change Log

| Date | Change Description |
|------------|--------------------|
| 07/18/2018 | Initial release. |

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.0.3, Build 0068

To upgrade to FortiADC 5.0.3, 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 5.0.3 is mainly a patch release, but also has the following new feature:

UDP Stateless LB

FortiADC now provides a UDP stateless mode, allowing you to perform load-balancing without attempting to match the packet to a pre-existing connection in the connection table. The feature is especially useful when load-balancing syslog servers, e.g., FortiAnalyzer.

Hardware and VM support

FortiADC 5.0.3 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 5.0.3 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 5.0.3 release. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Table 1: Resolved issues

| Bug ID | Description |
|---------|--|
| 0490289 | Parsing errors were found in FortiADC MIB. |
| 0491703 | The user may be able to use generated SSO cookies to bypass the Authentication page on different FortiADC platforms. |
| 0490966 | In some cases, traffic could fail to use the default route. |
| 0492499 | The GUI did not show the ARP table associated to a VDOM. |
| 0495153 | Layer-4 server load-balance traffic logs show duration in seconds while the field on the GUI is marked as Duration (ms). |
| 0493474 | The "Permission Denied" message may pop up erroneously when you move back to the Server Load Balance page. |
| 0495642 | SMTP virtual server configuration lacks the "Keep Client Address" option. |
| 0496485 | SSH/GICD service vulnerabilities. |
| 0497168 | FortiADC security vulnerabilities. |
| 0498219 | Attempt to upload files to sites behind FortiADC could fail due to Web Application Firewall crash. |
| 0488438 | Admin User configuration lacks Group Authentication, Group Type, and Group DN options. |
| 0478703 | The VLAN interface could still be accessed in HA VRRP configurations. |
| 0499414 | Syslog message format is inconsistent between the logging and alerts pages. |
| 0499970 | Layer- 4 virtual servers could switch to Port 80 (default) even after it was set to Port 0 on the GUI. |
| 0495340 | Users with read-only rights were still able to take down port interfaces. |
| 0502634 | In some cases, Layer- 4 virtual server VDOM configuration may cause kernel hang and crash. |

| Bug ID | Description |
|---------|--|
| 0492983 | The Diffie Hellman key was 0241 instead of 204. |
| 0470119 | Quarantined memory leak was found. |
| 0491347 | Client verify through OCSP may not work properly after HSM is enabled. |
| 0491716 | In some cases, enabling compression may cause HTTP virtual server crash. |
| 0471987 | New GLB configurations may not work properly if the system time is rolled back to an earlier date and/or time. |
| 0497458 | Executing the "execute hsm" command could cause the Console to crash. |
| 0497726 | An SMTP virtual server could lose its method after its profile is changed. |
| 0499714 | Form-based authentication may not work properly in some cases |
| 0499489 | The state of a physic interface could be incorrect after the parent aggregate interface is deleted. |
| 0485299 | Deleting a VDOM could lead to statusd crash. |
| 0490944 | The anti-virus extreme DB could not be updated from the official FDS. |

Known issues

This section highlights the major known issues discovered in FortiADC 5.0.3 release. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Table 2: Known issues

| Bug ID | Description |
|---------|---|
| 0412861 | <p>The aggregate interface can not work under balance-rr/xor/broadcast with the switch in HA mode.</p> <p>Workaround: Traffic return from peer switch may go to slave node. Use another algorithm instead.</p> |
| 0455272 | <p>GEO IP configurations would get lost when restoring a pre-5.0 version from v5.0.</p> <p>Workaround: Do not restore the configuration of a lower version on a v5.0 system directly.</p> |
| 0468417 | <p>Changes made to the destination port of the VXLAN tunnel do not take effect on listening port.</p> <p>Workaround: Normally, you do not need to change the destination port. If you do, be sure to reboot the system.</p> |
| 0465516 | <p>The order of the Interfaces could get changed after removing and re-adding an interface to FortiADC in an OpenStack environment.</p> <p>Workaround: Determine the number of interfaces before configuration, and try not to delete interfaces in an OpenStack environment.</p> |
| 0470620 | <p>OpenStack lbass cannot connect to backup FortiADC devices after a failover</p> <p>Workaround: Manually configure the device settings when FortiADC is in HA-AA or HA AA-VRRP mode.</p> |
| 0471518 | <p>For Layer-2 and Layer-4 TCP or TCPS profiles, 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.</p> |
| 0471525 | <p>If <code>client-certificate-verify-option</code> in a <code>client_ssl_profile</code> is set to "Optional", the persistence type <code>LB_PERSIS_SSL_SESS_ID</code> will not work in a virtual server which uses the <code>client_ssl_profile</code>.</p> <p>Workaround: Do NOT set <code>client-certificate-verify-option</code> in a <code>client_ssl_profile</code> to "Optional".</p> |

| Bug ID | Description |
|---------|--|
| 0475733 | <p>Script content was lost when downgrading from 5.0.0 to 4.8.4.</p> <p>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.</p> |
| 0401984 | <p>The IP table rules created by rtsp_vs could not sync to the slave device in HA mode.</p> <p>Workaround: You must re-connect to the RTSP server when performing HA sync.</p> |
| 0233369 | <p>Shutting down the PPPoE interface sometimes could cause the default route to be deleted from the default route table.</p> <p>Workaround: Reconfigure the default route table after shutting down the PPPoE interface.</p> |
| 0380628 | <p>Sometimes, global load-balance link member configuration in HA VRRP configuration could not be fully synced to the slave device.</p> <p>Workaround: When that happens, execute the command "<code>execute ha force sync-config</code>" to sync the configuration.</p> |
| 0401508 | <p>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.</p> <p>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.</p> |
| 0376784 | <p>Some traffic log data may get missing when FortiADC is under heavy traffic stress.</p> <p>Workaround: Enable traffic logging only in normal traffic conditions; do NOT enable it when CPU usage exceeds 60%.</p> |
| 0372459 | <p>Sometimes, the floating IP may be missing in the back-end after some operations.</p> <p>Workaround: When that happens, reconfigure the floating IP.</p> |
| 0414143 | <p>The traffic limit control for FortiADC inbound/outbound packets in each VDOM only works for TCP traffic; it does not work for UDP traffic.</p> <p>Workaround: Do NOT impose the traffic limit on UDP traffic.</p> |
| 0377176 | <p>The OSPF neighbor won't be built if the floating IP is the same as the interface IP.</p> <p>Workaround: Avoid setting the floating IP the same as the interface IP.</p> |
| 0446943 | <p>SSL throughput may decrease under certain circumstances.</p> <p>Workaround: Tune the tune-bufsize to 16384.</p> |

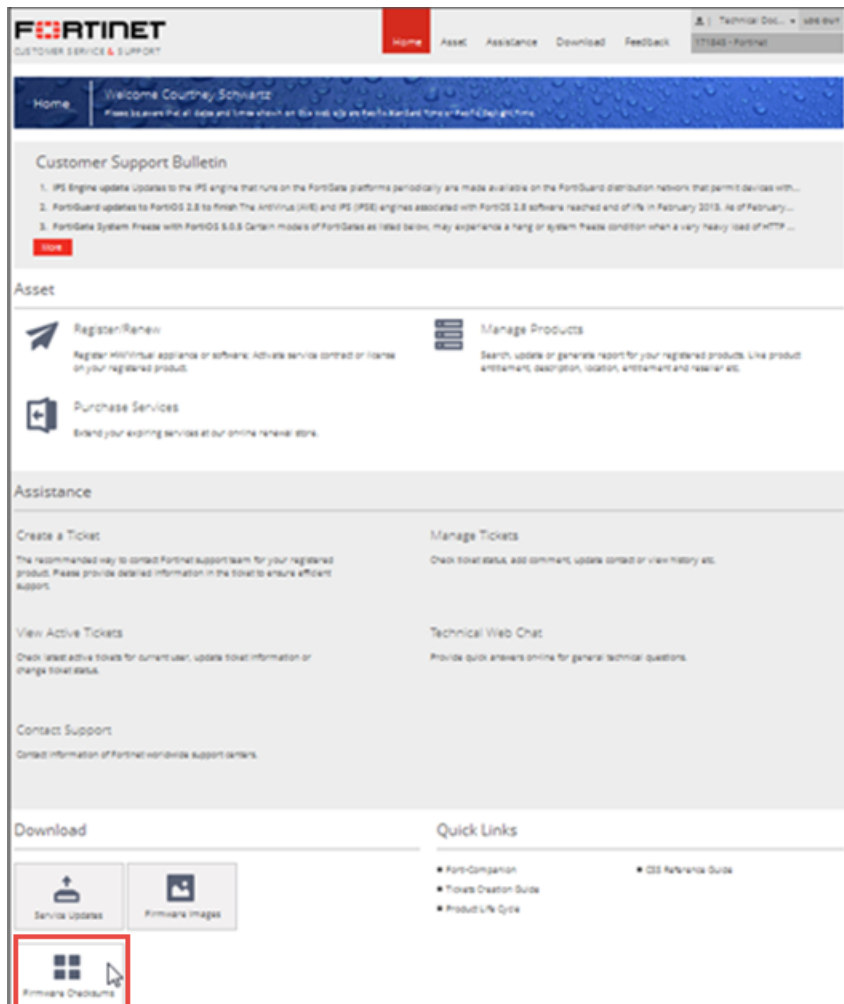
| Bug ID | Description |
|---------|---|
| 0444752 | <p>When 300 wildcard administrators using different RADIUS servers in the system, it may take up to 5 minutes to log in.</p> <p>Workaround: Try to use no more than 10 RADIUS/LDAP servers for wildcard administrator authentication.</p> |
| 0446418 | <p>After migrating RADIUS persistence profiles to Version 4.8.1, some vendor-specific attributes may get lost during backup and restore.</p> <p>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.</p> |
| 0448922 | <p>Some VDOM configurations may remain in the system if you delete a VDOM shortly after it is created.</p> <p>Workaround: Do not create and delete VDOMS in a rapid fashion.</p> |

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



FORTINET®

High Performance Network Security



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.