

FortiADC - Release Notes

Version 6.2.0

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 3, 2021

FortiADC 6.2.0 Release Notes

01-544-677187-20201112

TABLE OF CONTENTS

Change Log	5
Introduction	6
What's new	7
Load Balance	7
OAuth 2.0 support	7
CAMELLIA Encryption Algorithm	7
New scripts to support WAF events and commands	7
Health check monitoring with continuous mode	7
Security	8
WAF enhancement	8
Web Vulnerability Scanner integration with third-party report	8
Web Vulnerability Scanner auto policy	8
System	8
New platform 220F support	8
Trust IP list to limit the access to management service for the interface	8
HA pair on Azure using ARM templates	8
Transfer files between HA devices	9
Pre-login banner support for WebUI, Console and SSH login	9
New VM subscription license	9
VDOM link for inter-VDOM traffic	9
Factory reset command enhancement to keep VDOM, interface, and static route settings	9
Support -f option for grepping CLI output	9
GUI	10
Redesign of the select checkbox for all tables	10
Hardware, VM, cloud platform, and browser support	11
Known issues	13
Resolved issues	14
Image checksums	16
Upgrade notes	17
Supported upgrade paths	17
6.0.x to 6.1.x	17
5.4.x to 6.0.x	17
5.3.x to 5.4.x	17
5.2.x to 5.3.x	17
5.1.x to 5.2.x	18
5.0.4 to 5.1.x	18
5.0.0 to 5.0.4	18
4.8.x to 5.0.0	18
GUI	18
Authentication	18
System	18
GEO IP	18
4.8.4 to 4.8.4	18

4.8.2 to 4.8.3	19
4.8.1 to 4.8.2	19
4.8.0 to 4.8.1	19
GUI	19
HA	19
Platform	19
4.7.x to 4.8.0	19
4.6.x to 4.7.x	20
4.6.1 to 4.6.2	20
4.5.x to 4.6.x	20
4.4.x to 4.5.x	20
4.3.x to 4.5.x	20
4.2.x to 4.5.x	20
4.1.x to 4.5.x	21
4.0.x to 4.5.x	21
Upgrading a stand-alone appliance from 4.2.x or later	21
Upgrading an HA cluster from 4.3.x or later	22
Special notes	23

Change Log

Date	Change Description
August 3, 2021	FortiADC 6.2.0 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 6.2.0, Build 0210.

To upgrade to FortiADC 6.2.0, see [Upgrade notes](#).

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 6.2.0 offers the following new features:

Load Balance

OAuth 2.0 support

Open Authorization (OAuth) 2.0 is an authorization framework that enables applications to obtain limited access to HTTP services on behalf of a user. It works by delegating user authentication to the service that hosts the user account, and authorizing third-party applications to access the user account. OAuth 2.0 provides authorization flows for web and desktop applications, and mobile devices.

FortiADC will only be supporting OAuth 2.0 which is the most widely used form of OAuth. There will be no backwards compatibility between OAuth 1.0 and OAuth 2.0 as their specifications are so different that they cannot be used together.

CAMELLIA Encryption Algorithm

New SSL ciphers have been added in the Client SSL profile and Server SSL profile:

- ECDHE-ECDSA-CAMELLIA256-SHA384
- ECDHE-RSA-CAMELLIA256-SHA384
- DHE-RSA-CAMELLIA256-SHA256
- ECDHE-ECDSA-CAMELLIA128-SHA256
- ECDHE-RSA-CAMELLIA128-SHA256
- DHE-RSA-CAMELLIA128-SHA256
- DHE-RSA-CAMELLIA256-SHA

New scripts to support WAF events and commands

A new set of Lua scripts have been added to manage WAF related events and actions. These scripts support functionalities that include enabling/disabling the WAF function, watching an event when the WAF scan starts or an attack is detected, and other custom actions.

Health check monitoring with continuous mode

The health check monitoring functionality has been enhanced to allow more settings to monitor the check and to display more information for the check results.

Security

WAF enhancement

The following enhancements have been made for the WAF:

- Brute force protection support for offloading authentication
- Cookie security support for cookies generated by FortiADC

Web Vulnerability Scanner integration with third-party report

FortiADC now supports integrations with third-party vendor scanner reports, including FortiWeb, Acunetix, IBM Appscan, Whitehat, HP Webinspect, QualysGuard, Telefonica FFAST, ImmuniWeb reports.

Web Vulnerability Scanner auto policy

You can now generate WAF policies based on FortiADC scan reports or third-party integrated reports. Users can modify the policy as needed and submit it to the virtual server to apply directly.

System

New platform 220F support

FortiADC 6.2.0 now supports the FortiADC 220F platform. For more information, please refer to the latest FortiADC datasheet.

Trust IP list to limit the access to management service for the interface

Currently, FortiADC supports `allowaccess` to allow/deny access to the interface management service. With the new Trust IP list feature, you will have more granular control over which IP addresses may be granted access to the interface management service.

HA pair on Azure using ARM templates

FortiADC is introducing a solution for HA on Azure that can eliminate the issue caused by time-consuming IP transfers in the event of HA failovers. Please refer to the new Azure deployment guide for the new HA setup on Azure.

Transfer files between HA devices

Use the new CLI command `execute ha force transfer-file <file-name> <node-id>` to sync files between HA devices. This could be used to get debug files on the backup device from the master when the backup device is not accessible in some situations.

Pre-login banner support for WebUI, Console and SSH login

You can now customized banner messages to show prior to login through WebUI, console and SSH.

New VM subscription license

Two new SKUs for VM subscription license support has been added, including the Standard Bundle and Advanced Bundle license.

VDOM link for inter-VDOM traffic

FortiADC now supports inter-VDOM routing setups that allow the traffic to be sent between VDOMs without additional physical interfaces that was previously required for multiple VDOM setups. At this time, inter-VDOM routing is only available for these classic scenarios: static route, PBR, L4 SLB, L7 SLB and NAT. It is currently not supported in IPv6 related configurations.

Factory reset command enhancement to keep VDOM, interface, and static route settings

Currently, performing a factory reset would clear all settings on the devices entirely which may not be ideal for some users who need to keep basic networking settings. For this, FortiADC has added a new alternative factory reset command that will allow users to clear all configurations but keep the settings for VDOM, interface, and static route.

Support -f option for grepping CLI output

You can now filter for the string in CLI configurations.

For example:

```
# show full-configuration | grep -f 10.0.0.1
```

This will show all entries with the IP 10.0.0.1

GUI

Redesign of the select checkbox for all tables

The select checkbox column has been removed for all tables. Now you can make your selection by clicking the row, or press `Ctrl+Shift` to select multiple rows.

Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 6.2.0.

Supported Hardware:

- FortiADC 200D
- FortiADC 300D
- FortiADC 400D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D
- FortiADC 100F
- FortiADC 200F
- FortiADC 220F
- FortiADC 300F
- FortiADC 400F
- FortiADC 1000F
- FortiADC 1200F
- FortiADC 2000F
- FortiADC 2200F
- FortiADC 4000F
- FortiADC 4200F
- FortiADC 5000F

For more information on the supported hardware models, see FortiADC's [Hardware Documents](#).

Supported hypervisor versions:

VM environment	Tested Versions
VMware	ESXi 3.5, 4.x, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
Microsoft Hyper-V	Windows Server 2012 R2, 2016 and 2019
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
OpenStack	Pike
Nutanix	AHV

Supported cloud platforms:

- AWS (Amazon Web Services)
- Microsoft Azure
- GCP (Google Cloud Platform)
- OCI (Oracle Cloud Infrastructure)

For more information on the supported cloud platforms, see the FortiADC [Private Cloud](#) and [Public Cloud](#) documents.

Supported web browsers:

- Mozilla Firefox version 59
- Google Chrome version 65

We strongly recommend you set either of the Web browsers as your default Web browser when working with FortiADC. You may also use other (versions of the) browsers, but you may encounter certain issues with FortiADC's Web GUI.

Known issues

This section lists known issues in version FortiADC 6.2.0, but may not be a complete list. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0752290	SAML fails to function after upgrade to FortiADC 6.2.0/6.2.1/6.1.4.
0737567	<code>execute factoryreset2</code> removes default DNS settings, so the DNS server settings need to be manually added to enable connection to FDS.
0736392	Missing information in logs for firewall status change.
0736113	K8s connector cannot be configured via GUI. K8s connector token length cannot be configured with a string length exceeding 1023 via CLI.
0735937	DNS response TTL will be incorrect if it contains the same IP from different servers.
0735008	LACP status is not correct when there is only one member.
0733833	CPU Utilization will always be at 85%+ after importing user defined ISP address.
0731909	DNSD crashes when a new real server with FQDN type is added or when modifying an existing real server.
0725173	AV SMTP fnginx crash on 6.2.0:0201

Resolved issues

The following issues have been resolved in FortiADC 6.2.0 release. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0732434	Edits made to an existing PTR record does not show in the zone record.
0730683	The system interface link status changes to unknown when the physical interface becomes a member of aggregate or softswitch.
0730184	WVS policy still exists after deleting. It can only be removed after refreshing the browser.
0730183	WVS policy does not show in the WebUI after creating it.
0728582	httproxy crashed with content-rewrite match with . * and http traffic url included //.
0728103	Content route matching IP 0.0.0.0 takes precedence which overwrites other content route matching on different IP.
0728077	SNMP retrieves the wrong status for Real Server.
0725917	FortiGuard Tunneling Username required.
0725481	SLB-L7 SMTP returns 502 response when setting <code>disable-command-status</code> to <code>disable</code> .
0723984	Httpoxy crash related to auth form-based and HTTP Traffic with no host.
0722531	Password change on first login is broken in Azure.
0722299	FortiView Security Logs issue with table columns.
0722298	FortiView Threat Map links to the wrong log file.
0722296	FortiView Threat Map showing the wrong threat details.
0722088	WAF URL exception return match fail issue.
0721840	CLI command need to be added to control if "hold 200-" or not in SLBL7 SMTP.
0719687	Multiple issues after configuring DDoS configuration.
0717445	FTP response code 550 is overwritten with 420 in some instances.
0715641	LB crash issue.
0714353	Token ID does not submit when pressing the <code>Enter</code> key to submit.
0714038	Need to enlarge the max-length of private-key-file from 64 to 251.
0709943	HA member leaves group when configuration changes were being made.

Bug ID	Description
0708219	OpenSSL 1.1.1k security fixes.
0703777	FortiADC continues to ask the client to switch to STARTTLS even when the Starttls Active Mode is set to 'Allow' in the SMTP LB profile.
0696003	Alignment issue with the WAF common attacks HTTP protocol page.
0690909	Issue with the order of the status buttons.
0660920	DNS query does not work with Google 8.8.8.8.

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.

Customer Service & Support image checksum tool

The screenshot shows the Fortinet Customer Service & Support website. At the top, a blue banner displays 'Home' and 'Welcome Samuel Liu' with a note about time zones. Below this is a 'Customer Support Bulletin' section with three items: 'AV engine 5.355 released to FortiGuard AV engine update will be available on the FortiGuard network...', 'IPS engine 3.532 released to FortiGuard for FDS 5.4 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.4)...', and 'IPS engine 3.532 released to FortiGuard for FDS 5.6 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.6)...'. A 'More' button is present. The main content area is divided into 'Asset' and 'Assistance' sections. 'Asset' includes 'Register/Renew' and 'Manage Products'. 'Assistance' includes 'Create a Ticket', 'Manage Tickets', 'View Active Tickets', 'Technical Web Chat', and 'Contact Support'. At the bottom, there are 'Quick Links' and 'Resources' sections. In the 'Quick Links' section, 'Firmware Images' and 'VM Images Download' are highlighted with a red box. The 'Resources' section lists 'Customer Support Bulletin', 'Knowledge Base', 'Fortinet Video Library', 'Fortinet Document Library', 'Discussion Forums', and 'Training & Certification'.

Home Welcome Samuel Liu
Please be aware that all dates and times shown on this web site are Pacific Standard Time or Pacific Daylight Time.

Customer Support Bulletin

1. AV engine 5.355 released to FortiGuard AV engine update will be available on the FortiGuard network...
2. IPS engine 3.532 released to FortiGuard for FDS 5.4 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.4)...
3. IPS engine 3.532 released to FortiGuard for FDS 5.6 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.6)...

More

Asset

Register/Renew
Register HW/Virtual appliance or software; Activate service contract or license on your registered product.

Manage Products
Search, update or generate report for your registered products. Like product entitlement, description, location, entitlement and reseller etc.

Assistance

Create a Ticket
The recommended way to contact Fortinet support team for your registered product. Please provide detailed information in the ticket to ensure efficient support.

Manage Tickets
Check ticket status, add comment, update contact or view history etc.

View Active Tickets
Check latest active tickets for current user; update ticket information or change ticket status.

Technical Web Chat
Provide quick answers on-line for general technical questions.

Contact Support
Contact information of Fortinet worldwide support centers.

Quick Links

- Firmware Images
- VM Images Download
- Service Updates
- Product Life Cycle
- Fortinet Service Terms & Conditions
- Guidelines, Policies & Documents
- Help Documents

Resources

- Customer Support Bulletin
- Knowledge Base
- Fortinet Video Library
- Fortinet Document Library
- Discussion Forums
- Training & Certification

Upgrade notes

This section includes upgrade information about FortiADC 6.2.0.



Do not upgrade to FortiADC 6.2.0/6.2.1/6.1.4 if you are currently using SAML. Once upgraded, SAML will fail to function. A solution to this issue is currently in development and will be available in the next release.

Supported upgrade paths

This section discusses the general paths to upgrade FortiADC from previous releases.

Note:

If you are upgrading to the next major version level, you will need to upgrade to the nearest major versions first. For example, if you are updating from 5.4.1 to 6.2.0, then you will need to upgrade to 6.0.0, 6.1.0, and then to 6.2.0.

For upgrading to minor versions in a higher version level, you may skip the nearest major version to update directly to the minor version. For example, if you are updating from 5.4.1 to 6.1.2, then you will need to first upgrade to 6.0.0 then upgrade directly to 6.1.2.

6.0.x to 6.1.x

Direct upgrade via the web GUI or the Console.

5.4.x to 6.0.x

Direct upgrade via the web GUI or the Console.

5.3.x to 5.4.x

Direct upgrade via the web GUI or the Console.

5.2.x to 5.3.x

Direct upgrade via the web GUI or the Console.

5.1.x to 5.2.x

Direct upgrade via the web GUI or the Console.

5.0.4 to 5.1.x

Direct upgrade via the web GUI or the Console.

Note: 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.

5.0.0 to 5.0.4

Direct upgrade via the web GUI or the Console

4.8.x to 5.0.0

Direct upgrade via the web GUI or the Console.

GUI

Due to GUI changes and enhancements, we strongly recommend refreshing (Ctrl +F5) your web browser when access the FortiADC web GUI after the upgrade.

Authentication

This upgrade addresses the compatibility with other devices. Therefore, you must download the new FortiADC SAML SP and upload it to the SAML IDP peer. You do not need to modify the FortiADC SP file anymore.

System

It will take more time to upgrade to 5.0.0 because FortiADC has to create quarantine partition for the AV feature.

GEO IP

You will lose your existing GEO IP protection region configurations when upgrading from 4.7.x to 5.0.0.

4.8.4 to 4.8.4

Direct upgrade via the web GUI or the Console.

4.8.2 to 4.8.3

Direct upgrade via the web GUI or the Console.

4.8.1 to 4.8.2

Direct upgrade via the web GUI or the Console.

4.8.0 to 4.8.1

Direct upgrade via the web GUI or the Console.

GUI

- Due to GUI changes, be sure to refresh your web browser when the upgrade is completed (Ctrl + F5).
- FortiADC 60F supports Google Chrome only.

HA

- To synchronize system image upgrade in HA mode, make sure that all the devices in the HA cluster use exactly the same version of the image.
- Use the management interface in HA mode instead of a dedicated interface.

Platform

- Upgrade your VM01 to 4 GB of memory in virtual platform.

4.7.x to 4.8.0

Direct upgrade via the web GUI or the Console.

- GUI—Due to GUI changes, be sure to refresh (CTRL+F5) your web browser when access FortiADC upon upgrade.
- HA—(For physical devices) Upon upgrade, wait for a few minutes for the HA state to stabilize and the configuration to sync.
- Service—When upgrading to 4.8.x from 4.7.x or lower, FortiADC will add 28 predefined services. If you have old services with the same names as those of the predefined services, FortiADC will rename those "old" services to "oldname_upgrade".
- Global Load Balance—If there was a virtual server pool that was not referenced by any GLB Host in the 4.7.x configuration, the Default Feedback IP configuration in this virtual server pool will be lost upon upgrade. To keep this Default Feedback IP, you MUST reference this virtual server pool in the GLB Host before upgrading the system.

4.6.x to 4.7.x

Direct upgrade via the web UI or the CLI.

- GUI—Due to GUI changes, refresh (CTRL+F5) your web browser when access FortiADC upon upgrade.
- HA—(For physical devices) Upon upgrade, wait for a few minutes for the HA state to stabilize and the configuration to sync.
- Service—When upgrading to 4.7.x from 4.6.x or lower, FortiADC will add 28 predefined services. If you have old services with the same names as those of the predefined services, FortiADC will rename those "old" services to "oldname_upgrade".
- Global Load Balance—If there was a virtual server pool that was not referenced by any GLB Host in 4.7.x configuration, the Default Feedback IP configuration in this virtual server pool will be lost upon upgrade. To keep this Default Feedback IP, you MUST reference this virtual server pool in the GLB Host before upgrading the system.

4.6.1 to 4.6.2

Direct upgrade via the web UI or CLI.

4.5.x to 4.6.x

Direct upgrade to FortiADC 4.6.0 from any version prior to 4.5.x is NOT supported via the GUI. The best way to upgrade is via the CLI using the `restore image` command. If you prefer to upgrade via the GUI, you MUST first upgrade the image to 4.5.x and then to 4.6.x.

- GUI — Due to GUI changes in 4.6.x, be sure to refresh your browser when accessing the new FortiADC web GUI.
- Global Load Balance — If your existing configuration contains the ISP feature, reconfigure it. This is because the ISP option has been moved.
- HA —Update the firmware if HA Sync is enabled. The process normally takes about 10 minutes to complete.

4.4.x to 4.5.x

Direct upgrade via the web UI or the CLI.

4.3.x to 4.5.x

Direct upgrade via the web UI or the CLI.

4.2.x to 4.5.x

Direct upgrade via the web UI or the CLI.

4.1.x to 4.5.x

You can upgrade from FortiADC 4.1.x using the CLI. Direct upgrade from 4.1.x to 4.5.x is not supported from the web UI. See the FortiADC Handbook for instructions on upgrading with the CLI.

4.0.x to 4.5.x

Direct upgrade from 4.0.x and earlier is not supported. You must first upgrade to FortiADC 4.1.x, and the system must be in an operable state.

Upgrading a stand-alone appliance from 4.2.x or later

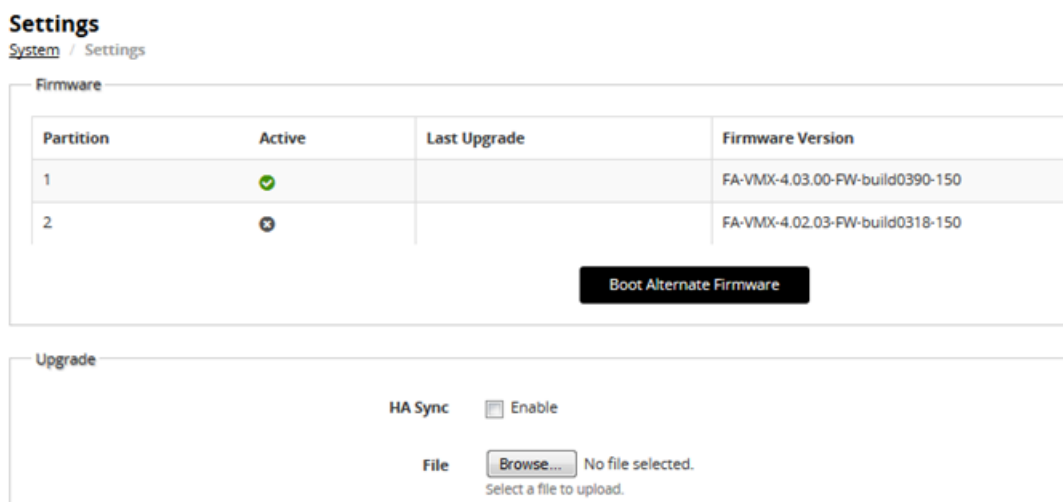
The following figure shows the user interface for managing firmware (either upgrades or downgrades). Firmware can be loaded on two disk partitions: the active partition and the alternate partition. The upgrade procedure:

- Updates the firmware on the inactive partition and then makes it the active partition.
- Copies the firmware on the active partition, upgrades it, and installs it in place of the configuration on the inactive partition.

For example, if partition 1 is active, and you perform the upgrade procedure:

- Partition 2 is upgraded and becomes the active partition; partition 1 becomes the alternate partition.
- The configuration on partition 1 remains in place; it is copied, upgraded, and installed in place of the configuration on partition 2.

This is designed to preserve the working system state in the event the upgrade fails or is aborted.




Before you begin:

- You must have super user permission (user admin) to upgrade firmware.
- Download the firmware file from the Fortinet Customer Service & Support website:
<https://support.fortinet.com/>

- Back up your configuration before beginning this procedure. Reverting to an earlier firmware version could reset settings that are not compatible with the new firmware.
- You upgrade the alternate partition. Decide which partition you want to upgrade. If necessary, click **Boot Alternate Firmware** to change the active/alternate partitions.

To update firmware:

1. Go to System > Settings.
2. Click the **Maintenance** tab.
3. Scroll to the Upgrade section.
4. Click **Browse** to locate and select the file.
5. Click  to upload the firmware and reboot.
The system replaces the firmware on the alternate partition and reboots. The alternate (upgraded) partition becomes the active, and the active becomes the alternate.
6. Clear the cache of your web browser and restart it to ensure that it reloads the web UI and correctly displays all interface changes.

Upgrading an HA cluster from 4.3.x or later

The upgrade page for Release 4.3.0 and later includes an option to upgrade the firmware on all nodes in an HA cluster from the primary node.

The following chain of events occurs when you use this option:

1. The primary node pushes the firmware image to the member nodes.
2. The primary node notifies the member nodes of the upgrade, and takes on their user traffic during the upgrade.
3. The upgrade command is run on the member nodes, the systems are rebooted, and the member nodes send the primary node an acknowledgment that the upgrade has been completed.
4. The upgrade command is run on the primary node, and it reboots. While the primary node is rebooting, a member node assumes the primary node status, and traffic fails over from the former primary node to the new primary node.

After the upgrade process is completed, the system determines whether the original node becomes the primary node, according to the HA Override settings:


- If Override is enabled, the cluster considers the Device Priority setting. Both nodes usually make a second failover in order to resume their original roles.
- If Override is disabled, the cluster considers the uptime first. The original primary node will have a smaller uptime due to the order of reboots during the firmware upgrade. Therefore, it will not resume its active role. Instead, the node with the greatest uptime will remain the new primary node. A second failover will not occur.

Before you begin, do the following:

1. Make sure that you have super user permission (user admin) on the appliance whose firmware you want to upgrade.
2. Download the firmware file from the Fortinet Customer Service & Support website:
<https://support.fortinet.com/>

3. Back up your configuration before beginning this procedure. Reverting to an earlier version of the firmware could reset the settings that are not compatible with the new firmware.
4. Verify that the cluster node members are powered on and available on all of the network interfaces that you have configured. (Note: If required ports are not available, HA port monitoring could inadvertently trigger an additional failover, resulting in traffic interruption during the firmware update.)
5. You upgrade the alternate partition. Decide which partition you want to upgrade. If necessary, click **Boot Alternate Firmware** to change the active/alternate partitions.

To update the firmware for an HA cluster:

1. Log into the Web UI of the primary node as the admin administrator.
2. Go to System > Settings.
3. Click the **Maintenance** tab.
4. Scroll to the Upgrade section.
5. Click **Browse** to locate and select the file.
6. Enable the **HA Sync** option.
7. Click  to upload the firmware and start the upgrade process.
8. Wait for the system to reboot and log you out to complete the upgrade.
9. Clear the cache of your Web browser and restart it to ensure that it reloads the web UI and correctly displays all interface changes.

Note: Normally, it takes approximately up to 10 minutes to upgrade with HA Sync.

Special notes

Suggestions

- HSM doesn't support TLS v1.3. If the HSM certificate is used in VS, the TLS v1.3 handshake will fail.
Workaround: Uncheck the TLSv1.3 in the SSL profile if you're using the HSM certificate to avoid potential handshake failure.
- The backup config file in versions 5.2.0-5.2.4/5.3.0-5.3.1 containing certificate config might not be restored properly (causing config to be lost). After upgrading to version 6.2.0, please discard the old 5.2.x/5.3.x config file and back up the config file in 6.2.0 again.
- Keep the old SSL version predefined config to ensure a smooth upgrade.
- Since the v4.7.x release, FortiADC has introduced a parameter called `config-priority` for HA configuration. It allows you to determine which configuration the system uses when synchronizing the configuration between the HA nodes. Therefore, upon upgrading to FortiADC 4.7.x or higher, we strongly recommend that you use this option to manually set different HA configuration priority values on the HA nodes. Otherwise, you'll have no control over the system's primary-secondary configuration sync behavior.

When the configuration priority values are identical on both nodes (whether by default or by configuration), the system uses the configuration of the appliance with the larger serial number to override that of the appliance with the smaller serial number. When the configuration priority values on the nodes are different, the configuration of the appliance with the lower configuration priority will prevail.

The request-body-detection in the WAF web-attack-signature profile will be changed from "disable" to

"enable" automatically after upgrading to FortiADC 5.4.0.

- In version 6.2.0, the default mode of QAT SSL has been changed to polling.



FORTINET®



Copyright© 2021 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.