FortiADC - Release Notes

Version 7.0.3

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

September 2, 2022
FortiADC 7.0.3 Release Notes
01-544-677187-20220902

TABLE OF CONTENTS

Change Log

Date	Change Description
September 2, 2022	FortiADC 7.0.3 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 7.0.3, Build 0039.

To upgrade to FortiADC 7.0.3, see Upgrade notes.

FortiADC provides load balancing, both locally and globally, and application delivery control. For more information, visit: https://docs.fortinet.com/product/fortiadc.

What's new

FortiADC 7.0.3 is a patch release, where no new features and enhancements are covered in this release. See Known issues on page 12 and Resolved issues on page 9 for details.

Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 7.0.3.

Supported Hardware:

- FortiADC 200D
- FortiADC 300D
- FortiADC 400D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D
- FortiADC 100F
- FortiADC 120F
- FortiADC 200F
- FortiADC 220F
- FortiADC 300F
- FortiADC 400F
- FortiADC 1000F
- FortiADC 1200F
- FortiADC 2000F
- FortiADC 2200F
- FortiADC 4000F
- FortiADC 4200F
- FortiADC 5000F

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)
- Alibaba Cloud

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.

Resolved issues

The following issues have been resolved in FortiADC 7.0.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0833188	miglogd crash for debug function.
0832344	Alertd crashed after using Automation to send out "show full" results, via Email action.
0831420	SAP SDN Connector parsing issues.
0831166	SNMP trap action is unable to add on Automation page.
0830087	FortiADC Web UI does not show VDOMs in drop-down menu.
0829822	sapd sdn filter retrieves null pointer.
0829750	fnginxctld crash based on issue with longer loading time for websites going through FortiADC.
0828136	In the GUI, FortiView > Virtual Server Session filtering does not work.
0827748	FortiADC performance issues as a result of exceeding total tcp_mem limit.
0827447	miglogd crash related to FortiAnalyzer.
0824625	FTP passive response retransmit packet has the real-server IP in the payload.
0824584	HTTP proxy crashes when uploading WAF JSON schema.
0823553	Dashboard is not displaying data.
0822767	Allowlist to permit false positive Bots is not working for Bot Detection policy.
0821776	Kernel panic while removing VLAN interface.
0820934	FortiADC GUI interfaces displaying as disabled.
0819733	FortiADC PAYG VM is crashing after getting deployed through GCP Marketplace.
0819216	REST API crashed when trying to upload CAPTCHA file.
0819214	Error page is not responding properly to ZTNA triggered deny action. The root of the issue is caused by ZTNA sending the error response too early, causing the error page to be blocked.
0819097	Error message "merge warning" triggers when synchronizing GSLB through Sync List.

Bug ID	Description
0818711	Following a successful request, some WAF modules are not scanning subsequent requests within the same session. Affected WAF modules: Brute Force Attack Detection, Cookie Security, JSON Detection, OpenAPI Validation, and XML Detection.
0818663	Cloned IPS signatures cannot be modified.
0818128	Cannot edit JSON schema entry.
0817934	JSON schema import failing.
0816794	Requests are incorrectly blocked when the Cookie Security is in "Signed" mode.
0816768	REST API crashed when uploading file to SAML IdP.
0816734	Cannot update CORS headers list.
0816089	FortiSandbox Fabric Connector cannot connect type FSA.
0815653	RADIUS persistence is not working.
0815454	Client timeout settings limited to 3600 seconds or less.
0814475	Google OAuth authentication code verification fails with "Malformed auth code" and "match scope failed".
0811223	ZTNA rules cannot be applied properly if multiple EMS have the same ZTNA tag. The ZTNA profile cannot differentiate between the different EMS when the tag is the same.
0810998	Local and remote administrative users unable to log in through GUI.
0806675	L7 SMTP operation issues occurring after firmware update.
0806321	Email alerts is being sent in TLS 1.0, but since TLS versions 1.2 or lower has been deprecated, connections lower than TLS 1.2 is not being accepted.
0804514	HA status incorrectly show as "Not Sync".
0802844	Unable to login to FortiADC GUI and abnormal behavior in some virtual servers due to tmpfs_control leak issue.
0796054	Unable to control SNMP Trap community with Automation Stitches.
0783548	FortiADC resets MySQL connection when concurrent connections are set for MySQL service in L7 VS.

Common Vulnerabilities and Exposures

For more information, visit https://www.fortiguard.com/psirt.

Bug ID	Description
0833644	FortiADC 7.0.3 is no longer vulnerable to the following CVE-Reference: CWE-295: Improper Certificate Validation.
0825708	FortiADC 7.0.3 is no longer vulnerable to the following CVE-Reference: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ("SQL Injection").
0825707	FortiADC 7.0.3 is no longer vulnerable to the following CVE-Reference: CWE-20: Improper Input Validation.
0823097	FortiADC 7.0.3 is no longer vulnerable to the following CVE-Reference: CWE-79: Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting").
0822315	FortiADC 7.0.3 is no longer vulnerable to the following CVE-Reference: CWE-228: Improper Handling of Syntactically Invalid Structure.
0797261	FortiADC 7.0.3 is no longer vulnerable to the following CVE-Reference: CVE-2018-25032.

Known issues

This section lists known issues in FortiADC 7.0.3, but may not be a complete list. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0833592	FortiADC fails to send files to FortiSandBox Cloud.
0829597	HA A-A mode secondary unit traffic log shows gateway as none.
0826540	In the GUI, failed to append child list when configuring Automation. This results when an alert type has reached the maximum entry capacity. The current maximum is 256 entries for each alert type, as categorized in the backend CLI: • `config system alert-policy` • `config system alert-action` • `config system alert` • `config system alert-email` • `config system alert-snmp-trap` • `config system alert-script` • `config system alert-webhook` • `config system alert-fortigate-ip-ban` • `config system alert-syslog` `config system alert-policy` configurations are often composed of multiple `config system alert` entries, making the `config system alert` most likely to exceed the entry capacity. Please use `show full-configuration system alert` for details in the CLI. **Workaround**: After figuring out which alert type has exceeded the 256 entry capacity from the backend CLI, remove any unused automation alerts from the GUI.
0816798	In an HA environment, if you are using a predefined automation configuration, resetting the configuration through the GUI (using the reset button) or unsetting comments through CLI will cause the HA synchronization to fail whenever a device reboots and rejoins the cluster. Using the GUI reset button resets the predefined configuration values to the predefined default values, all except the comments value which is set to the default value on the backend. For example, if using the HA predefined configuration, the reset will result in `set comments HA` → `set comments comments`. When a new device (or a rebooted device) joins the HA cluster, the synchronization will fail due to the mismatched `set comments` value between the device that has the predefined default value (`set comments HA`) and the reset device that has the default value (`set comments comments`).

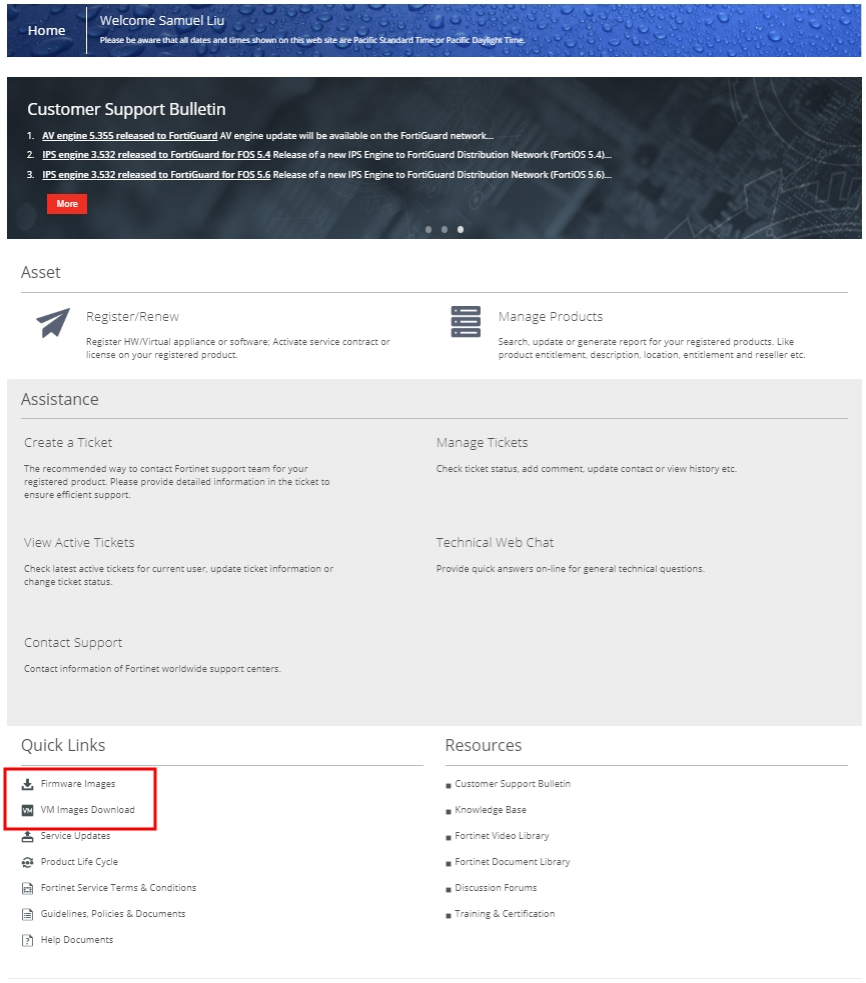
Bug ID	Description
	In the CLI, if `set comments` in the predefined configuration has been `unset` and is the default value `set comments comments`, then the same HA synchronization issue will occur. **Workaround**: In the CLI, edit `set comments` to ensure it is **not** the default value (`set comments comments`) and it matches the value of the predefined configuration (for example, `set comments HA`).

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



Upgrade notes

This section includes upgrade information about FortiADC 7.0.3.

Supported upgrade paths

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

Note:

If you are upgrading to a version that is in a higher version level, you will need to upgrade to the nearest branch of the major level incrementally until you reach the desired version. For example, to upgrade from 5.3.5 to 6.1.5, you will follow the upgrade path below:

5.3.5 → 5.4.x → 6.0.x → 6.1.5

(wherein "x" refers to the latest version of the branch)

6.2.x to 7.0.x

Direct upgrade via the web GUI or the Console.

6.1.x to 6.2.x

Direct upgrade via the web GUI or the Console.

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

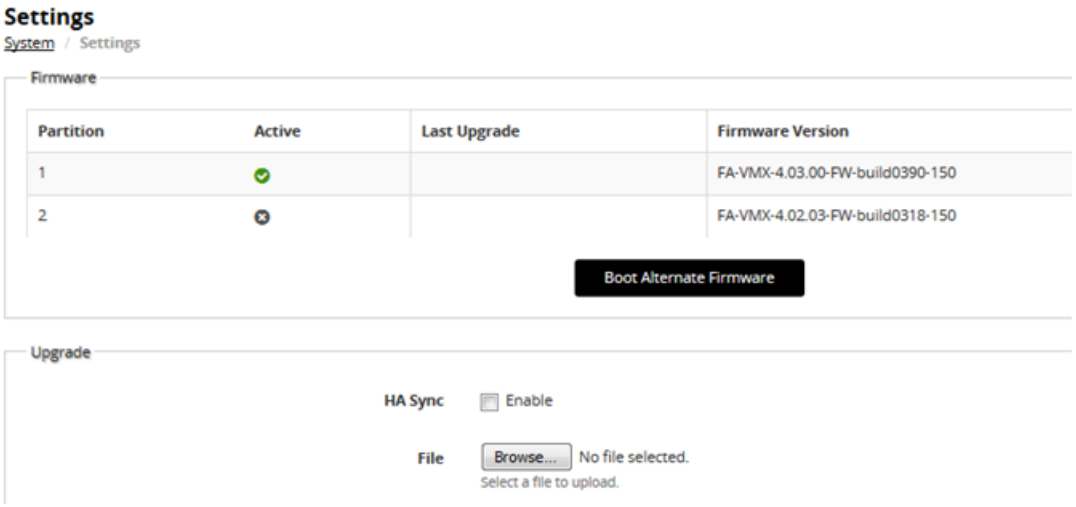
The following figure shows the user interface for managing firmware (either upgrades or downgrades). Firmware can be loaded on two disk partitions: the active partition and the alternate partition. The upgrade procedure:

- 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

- After upgrading to 7.0.3, in Virtual Machine HA environments where both nodes have been installed with certificate embedded licenses you must reinstall those licenses. As some backend certificate files would have been synchronized and overwritten by the HA Peer (due to an existing bug), the certificate file would not be recoverable. Reinstalling the certificate embedded licenses is required to ensure they would work properly where they are needed, such as in ZTNA or FortiSandbox Cloud.
- 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 7.0.3, please discard the old 5.2.x/5.3.x config file and back up the config file in 7.0.3 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-priotity` 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.
- To use the SRIOV feature, users must deploy a new VM.
- Before downgrading from 7.0.3, ensure the new L7 TCP or L7 UDP application profiles are deleted or changed to a profile type that is supported in the downgrade version. Otherwise, this will cause the cmdb to crash.
- When deploying the new GSLB based on FortiADC 7.0.0, the verify-CA function will be enabled by default.