Upgrade Guide

FortiSOAR 7.3.0

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

November, 2022
FortiSOAR 7.3.0 Upgrade Guide
00-400-000000-20210416

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-05-05	Updated the path of the `leapp_upgrade.log` and updated the “Performing pre-checks on the FortiSOAR appliance" topic in the Upgrading FortiSOAR chapter.
2023-05-05	Updated the Upgrading FortiSOAR chapter as follows: - Updated the Preparing the system topic in the 'Upgrading FortiSOAR using the in-place upgrade method' topic. - Updated the 'Manual steps for reconfiguring FortiSOAR after the OS Upgrade when the 'leapp' service fails to resume in Enterprise or MSSP configurations' topic. - Added the 'Pre-upgrade check for in-place upgrade fails with a 'synchronization error for the fsr repositories' error' topic.
2023-05-03	Added the "Upgrading FortiSOAR with an externalized database" topic in the Upgrading FortiSOAR chapter.
2023-01-16	Added the "Manual steps for reconfiguring FortiSOAR after the OS Upgrade when the 'leapp' service fails to resume in Enterprise or MSSP configurations" topic in the Upgrading FortiSOAR chapter.
2022-12-19	Added the "In-place upgrades fail on setups that have their proxy configured" topic in the Upgrading FortiSOAR chapter.
2022-11-24	Replacing the 'screen' command with the 'tmux' command to handle session timeouts while running the FortiSOAR upgrade for 7.3.0 and later releases.
2022-11-21	Updated the Upgrading FortiSOAR chapter.
2022-11-04	Initial release of 7.3.0

Introduction

This guide covers upgrading a FortiSOAR™ enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration.

FortiSOAR release 7.3.0 supports Rocky Linux release 8.6 or RHEL 8.6 systems and support for the CentOS operating system has been discontinued.

As there is a change in the supported OS, there is a need to migrate the content from a pre-7.3.0 version to the 7.3.0 version. To migrate the content there are two methods:

- Using the FortiSOAR content export and restore method
- Using the in-place upgrade method

FortiSOAR Upgrade - Choosing between the content export and restore method and the in-place upgrade method

This topic lists some data points that should help you decide which upgrade method is better suited for your environment:

Prerequisite	FortiSOAR Content Export and Restore	In-place Upgrade
VM	Require to provision a new VM with FortiSOAR7.3.0.	New VM not required. Your existing FortiSOAR VM is upgraded.
Disk	Require to add a new disk if the database size is more than free space available on FortiSOAR appliance.	New disks are not required as this method does not take a backup of the database.

Time	Both methods take roughly the same amount of time. **Note**: The time taken varies as per your database size, as described in the following database comparison table.	Both methods take roughly the same amount of time. **Note**: The time taken varies as per your database size, as described in the following database comparison table.

The following tables present some additional data points to help you make your choice:

FortiSOAR system with 127 GB database size - Number of files/attachments is more		
Process	**FortiSOAR Content Export and Restore -Time or Storage Requirement**	**In-place Upgrade- Time or Storage Requirement**
Backup DB	30 minutes	2 minutes (DB backup process is skipped)
Requirement of extra disk space	320 GB - New disk was added to the VM	N/A
Compressed DB backup file size	91 GB	N/A
Configure the VM to add disk and update LVM	7 minutes	N/A
Provision new VM	10 minutes	N/A
Copy backup file to new VM	14 minutes	N/A
OS Upgrade	N/A	20 minutes
Install and configure FortiSOAR 7.3.0	N/A	20 minutes
Restore DB	51 minutes	10 minutes
Total Process Duration	Approximately 90 minutes	Approximately 58 minutes

FortiSOAR system with 18 GB database size - Number of files/attachments is less		
Process	**FortiSOAR Content Export and Restore - Time or Storage Requirement**	**In-place Upgrade- Time or Storage Requirement**

Backup DB	5 minutes	1 minutes (DB backup process is skipped)
Requirement of extra disk space	40 GB - New disk was added to the VM	N/A
Compressed DB backup file size	13 GB	N/A
Configure the VM to add disk and update LVM	7 minutes	N/A
Provision new VM	10 minutes	N/A
Copy backup file to new VM	5 minutes	N/A
OS Upgrade	N/A	20 minutes
Install and configure FortiSOAR 7.3.0	N/A	20 minutes
Restore DB	15 minutes	6 minutes
Total Process Duration	Approximately 42 minutes	Approximately 47 minutes

FortiSOAR Upgrade Notes

This document describes how to upgrade FortiSOAR to 7.3.0 using both the methods. This guide is intended to supplement the FortiSOAR Release Notes, and it includes the following chapters:

- Preparing to Upgrade FortiSOAR
- Upgrading FortiSOAR both the methods of upgrade, i.e., using the FortiSOAR content export and restore method and using the in-place upgrade script are described in this chapter.
- Upgrading a FortiSOAR High Availability Cluster
- Upgrading a FortiSOAR Distributed Multi-Tenancy Configuration
- Post-Upgrade Tasks

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant instance to version 7.3.0 from version 7.2.1 and 7.2.2 only. Also, once you have upgraded your instance, you must log out from the FortiSOAR UI and log back into FortiSOAR.

Also, note that the upgrade procedure temporarily takes the FortiSOAR application offline while the upgrade operations are taking place. We recommend that you send a prior notification to all users of a scheduled upgrade as users are unable to log in to the FortiSOAR Platform during the upgrade.

From version 7.0.0 onwards, the FortiSOAR UI displays a notification when a new release (always the latest) is available. The notification also contains a link to that version's release notes so that you can get details about the latest available release. This keeps FortiSOAR users informed about the latest releases and then users can make informed decisions about upgrading to the latest available FortiSOAR version.

Before you upgrade your FortiSOAR instance, it is highly recommended that you review the *Special Notices* chapter in the "Release Notes", so that you are aware of operational and breaking changes made in version 7.3.0.

To solve common issues that occur during the upgrade process, see the *Troubleshooting FortiSOAR* chapter in the “Deployment Guide.”

Preparing to Upgrade FortiSOAR

We recommend performing the following tasks to prepare for a successful FortiSOAR upgrade:

To prepare for upgrading FortiSOAR (summary):

- Ensure that all data ingestion playbooks and schedules are stopped and wait for all existing active playbooks to complete before starting the upgrade process.
- Take a VM snapshot of your current system. Only after you have taken a VM snapshot of your system should you attempt to upgrade FortiSOAR. In case of any failures, these VM snapshots will allow you to revert to the latest working state. Follow the steps mentioned in the documentation of your platform for taking a snapshot and reverting to the current snapshot.
- Ensure that the playbook appliance has '`Create`' and '`Read`' permissions on the `Widgets` module. Playbook appliance is used to install the widgets required by the war room, and if the permissions to the Widgets are not assigned; the required war room widgets will fail to install.
- Execute the `screen` command to ensure that your `ssh` session does not timeout. For more information on how to handle session timeouts, see the Handle session timeouts while running the FortiSOAR upgrade article present in the Fortinet Knowledge Base.
- Ensure that repo.fortisoar.fortinet.com is reachable from your VM. If you are connecting using a proxy, then ensure that proxy details set are correct using the `csadm network list-proxy` command and also ensure that `repo.fortisoar.fortinet.com` is allowed in your proxy. For more information on `csadm` CLI, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."
- Ensure that you have reviewed the *Special Notices* chapter in the "Release Notes", so that you are aware of operational and breaking changes made in version 7.3.0.

Upgrading FortiSOAR

You must migrate the content from a pre-7.3.0 version to the 7.3.0 version as, there is a change in the supported OS. To migrate the content there are two methods:

- Using the FortiSOAR content export and restore method
- Using the in-place upgrade method

Upgrading FortiSOAR using the FortiSOAR content export and restore method

This topic covers the upgrade process that requires you to export your database from the FortiSOAR 7.2.1 or 7.2.2 CentOS or RHEL system and import the into the newly setup Rocky Linux or RHEL system. For the FortiSOAR content export and restore method, use the migration script (`migrate-fortisoar-7.3.0.bin`).

Supported Migrations

- FortiSOAR 7.2.1 or 7.2.2 CentOS 7.9 system to FortiSOAR 7.3.0 Rocky Linux or RHEL 8.6 system.
- FortiSOAR 7.2.1 or 7.2.2 RHEL 7.0 system to FortiSOAR 7.3.0 Rocky Linux or RHEL 8.6 system.

Prerequisites

- Setup a system with either Rocky Linux version 8.6 or RHEL version 8.6.
- Users who have `root` access must run the migration script (`migrate-fortisoar-7.3.0.bin`), i.e., perform the FortiSOAR content export and restore operations.
- Ensure that you have checked all the points mentioned in the Preparing to Upgrade FortiSOAR chapter.
- Take a VM snapshot of your current system. Only after you have taken a VM snapshot of your system should you attempt to upgrade FortiSOAR. In case of any failures, these VM snapshots will allow you to revert to the latest working state. Follow the steps mentioned in the documentation of your platform for taking a snapshot and reverting to the current snapshot.
- Review the list of failed notifications on FortiSOAR (**Settings** > **Notifications** > **Failure Notifications Logs** tab) before you upgrading your FortiSOAR instance.
- Ensure that the ssh session does not timeout by entering into the `screen` mode. For more information on how to handle session timeouts, see the Handle session timeouts while running the FortiSOAR upgrade article present in the Fortinet Knowledge Base.

Migration Process

Exporting Data

1. ssh to the FortiSOAR VM (CentOS 7.0 or RHEL 7.0) from which you want to export your data.
2. Run the following command to download the migration script:
   ```
   # wget https://repo.fortisoar.fortinet.com/7.3.0/migrate-fortisoar-7.3.0.bin
   ```
   Note: If your instance can connect to "repo.fortisoar.fortinet.com" only by using a proxy, then ensure that the proxy is set in the `/etc/wgetrc` file. For example,
   ```
   use_proxy=yes
   http_proxy=<proxy_server_ip:port>
   https_proxy=<proxy_server_ip:port>
   ```
   You can also update the proxy setup using the `csadm network` command.
3. Run the migrate script using the following command:
   ```
   # sh migrate-fortisoar-7.3.0.bin --export [<backup_dir_path>]
   ```
   OR
   ```
   # chmod +x migrate-fortisoar-7.3.0.bin]
   # ./migrate-fortisoar-7.3.0.bin --export [<backup_dir_path>
   ```
   `[<backup_dir_path>]` is the directory file to which the data [`.tgz` file] is exported. If you do not specify any path, then the migration script throws an appropriate error.
   Notes: The migration script checks for the following:
   - Free space available in the directory to which you are exporting the data. If there is insufficient space, then the script displays an appropriate error. You can refer to 'Issues occurring in FortiSOAR due to insufficient space' section in the *Deployment Troubleshooting* chapter in the "Deployment Guide" for more information. Once you increase the disk space rerun the migrate script to continue the process of exporting the data.
   - FortiSOAR version from which data is being exported. Export of data is supported only from FortiSOAR release 7.2.1 onwards.
   - OS from which data is being exported. Export of data is supported from only CentOS and RHEL.
4. As a best practice move the database file to a different location as the VM from where the database file was exported is powered off.
5. Once your data is exported, check the 'Summary' message, and note the following information:
   - Name of the file (`.tgz`) that contains the exported data.
   - Free disk space required for the database import process.
   - Disk space that must be available on the directory to which you want to import the data.

Importing Data

Before you begin importing the data, ensure that you do following:

- Update the DNS as follows:
  a. Power off the system from where the data is exported.
  b. Update the DNS with the IP address of system where the data will be imported.
- Disk space on the target system in which you want import the data is meets the requirements as mentioned in the 'Summary' of the export operation.

To import data to restore your database, do the following:

1. ssh to the VM (RHEL or Rocky Linux) to which you want to import the data.
2. Run the following command to copy the exported data (`.tgz` file) to the system on which you want to import the data:
   ```
   # scp <file_name.tgz> csadmin@targetipaddress:directory_path
   ```

The `targetipadress` must be the IP address of the Rocky Linux or RHEL base OS.
Note: The copy operation might take a longer time depending on the size of the database file.
If the copy operation fails, then do the following:

a. Check if the 'openssh-clients' is present on the target machine. If it is not present, then download and install openssh-clients using the following command:
```
yum -y install openssh-clients
```
b. Once openssh-clients is installed, re-run the **scp** command with the required parameters.

3. Ensure that you are connected to a `screen` session.
4. Run the following command to import the data to this system:
```
# sh migrate-fortisoar-7.3.0.bin --import [<backup_file_path>]
```
OR
```
# chmod +x migrate-fortisoar-7.3.0.bin]
# ./migrate-fortisoar-7.3.0.bin --import [<backup_file_path>
```
`[<backup_file_path>]` is the name of the `.tgz` file that you want to import. If you do not specify the filename, then the migration script throws an appropriate error.
Notes: The migration script checks for the following:
   - Free space available in the directory to which you are importing the data. If there is insufficient space, then the script displays an appropriate error. You can refer to 'Issues occurring in FortiSOAR due to insufficient space' section in the *Deployment Troubleshooting* chapter in the "Deployment Guide" for more information. Once you increase the disk space re-run the migrate script to continue the process of importing the data.
   - FortiSOAR version to which databases are being imported. Import of databases is supported only from FortiSOAR release 7.3.0 onwards.
   - OS to which data is being imported. Import of data is supported only to RHEL and Rocky Linux systems.
5. The migration script imports the database and restores the hostname. Once the data is imported successfully, you can log into FortiSOAR and start using FortiSOAR.

Upgrading FortiSOAR using the in-place upgrade method

This topic covers the upgrade process using the in-place upgrade method. Upgrade of FortiSOAR using this method consists of the following phases:

1. Preparing the FortiSOAR appliance
2. Performing pre-checks on the FortiSOAR appliance
3. Downloading and installing the required packages, and reconfiguring FortiSOAR

In-place upgrade paths

- FortiSOAR 7.2.1 or 7.2.2 CentOS 7.9 system to FortiSOAR 7.3.0 Rocky Linux 8.6
- FortiSOAR 7.2.1 or 7.2.2 RHEL 7.0 system to FortiSOAR 7.3.0 RHEL 8.6 system

In-place upgrade process

Preparing the system

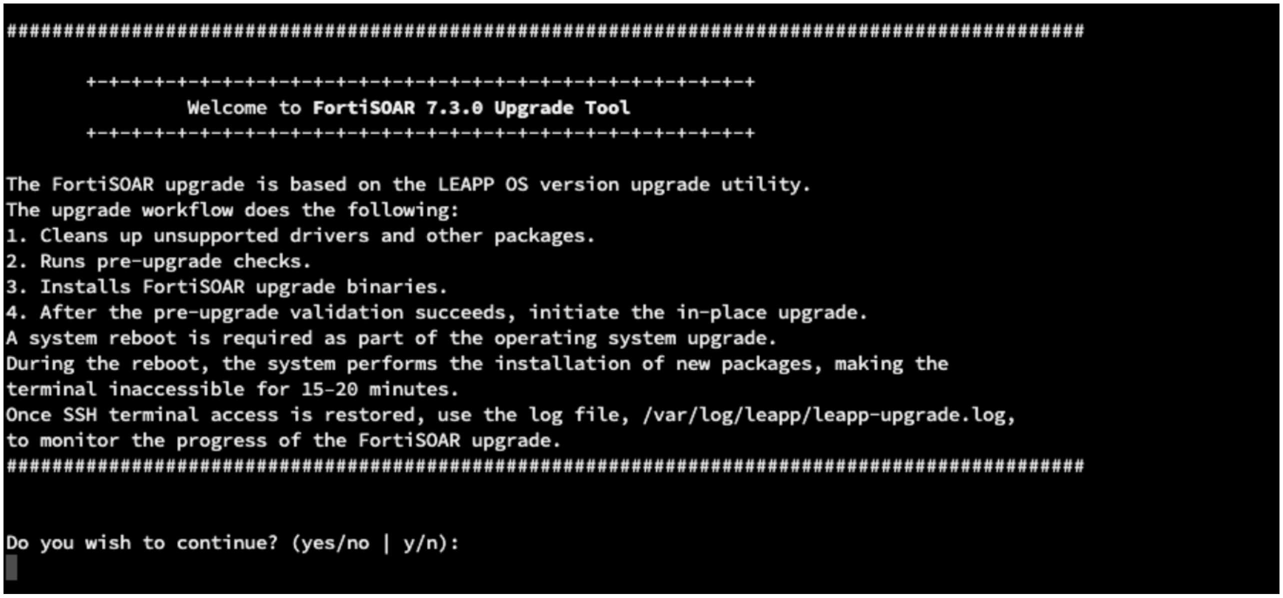
To prepare the FortiSOAR appliance for running the in-place upgrade, do the following:

1. Ensure that your FortiSOAR instance has the following minimum available space:
   - 2 GB free disk space in `/opt`
   - 2 GB free disk space in `/var`
2. Ensure that repo.fortisoar.fortinet.com is reachable from your FortiSOAR appliance. OR, if you are in an air-gapped environment, then ensure that the offline repository is synced with release 7.2.1 or 7.2.2, whichever is the current release of FortiSOAR since, some of the upgrade packages are present on 7.2.1 and 7.2.2 repositories.
3. In the case of an AWS instance, execute the following command to preserve `/etc/resolv.conf`:
   `chattr +i /etc/resolv.conf`
4. Ensure that you temporarily unmount any NFS mounts before upgrading your system.
5. If your system has more than one NIC, especially if the interface starts with eth, they must be temporarily disabled before the upgrad, i.e., ensure that there is only one NIC present before upgrading your system.

Performing pre-checks on the FortiSOAR appliance

This phase checks if your FortiSOAR appliance is ready for migration. If the pre-check displays warnings, the process stops, and the you are prompted to review the report and make changes, if necessary. No changes have been made to the system at this point.

1. Connect to the FortiSOAR appliance terminal.
2. Once ready, download the `fortisoar-inplace-upgrade-7.3.0.bin` utility, using `wget` or `curl`, to your FortiSOAR appliance from the following URL:
   `https://repo.fortisoar.fortinet.com/7.3.0/fortisoar-inplace-upgrade-7.3.0.bin`
3. Enter into the `screen` mode. This allows to re-connect terminal session and keeps in-place upgrade process execution uninterrupted.
4. Run the following command to launch the migration tool:
   `sh fortisoar-inplace-upgrade-7.3.0.bin`
   The migration utility gets launched and displays the following screen with informational message:



```
###############################################################################################

       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                Welcome to FortiSOAR 7.3.0 Upgrade Tool
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

The FortiSOAR upgrade is based on the LEAPP OS version upgrade utility.
The upgrade workflow does the following:
1. Cleans up unsupported drivers and other packages.
2. Runs pre-upgrade checks.
3. Installs FortiSOAR upgrade binaries.
4. After the pre-upgrade validation succeeds, initiate the in-place upgrade.
A system reboot is required as part of the operating system upgrade.
During the reboot, the system performs the installation of new packages, making the
terminal inaccessible for 15-20 minutes.
Once SSH terminal access is restored, use the log file, /var/log/leapp/leapp-upgrade.log,
to monitor the progress of the FortiSOAR upgrade.
###############################################################################################


Do you wish to continue? (yes/no | y/n):
```

5. On the first prompt of the migration utility, type yes or y to continue with the pre-checks.
   If the pre-checks report some inhibitors for migration, the process stops, and a report file path is presented for review.
   You can make changes as per the report and re-execute the utility to continue with the pre-checks.
   Note: If the changes require time, then you can re-plan the migration activity to a time after the changes are made. At this point, no changes are done to the system.

6. Once the pre-check process is clean, the migration utility asks for user confirmation to continue the migration process.

Downloading and installing the required packages, and reconfiguring FortiSOAR

1. Once the user confirmation is received for the continuation of the migration process once the pre-check process is clean, the migration utility performs the following steps:
   a. Cleans up unsupported drivers and other packages.
   b. Downloads FortiSOAR and OS packages.
   c. Once all packages are downloaded, the migration utility displays a message asking the user to reboot the system. A manual system reboot is required.
      During system reboot, FortiSOAR and the required packages are installed and due to this terminal access will be blocked for 15-20 min.
2. Once the system gets rebooted and the terminal access is restored , the migration utility continues with the FortiSOAR migration.
   You can monitor the migration process by checking `/var/log/leapp/leapp-upgrade.log`.
   Once the migration process is completed successfully the utility displays a completion message.
   Note: This process takes approximately one hour to complete.

Manual steps for reconfiguring FortiSOAR after the OS Upgrade when the 'leapp' service fails to resume in Enterprise or MSSP configurations

As explained, the in-place upgrade has two phases: a pre-OS upgrade and a post-OS upgrade. During the pre-OS upgrade phase, a FortiSOAR backup is taken and the system is prepared for the OS upgrade. The system requires to be rebooted after the pre-OS upgrade phase. Once the system is rebooted, the leapp framework attempts to initiate the second phase. In the second phase, FortiSOAR is reconfigured with the latest version and the backed up configurations are restored as mentioned in the Downloading and installing the required packages, and reconfiguring FortiSOAR topic. In the rare cases where the leapp service does not work or fails to resume, you can manually reconfigure FortiSOAR with the latest version and restore the backed-up configurations, as described in the following topics.

Pre-Checks

1. Check `/var/log/leapp/leapp-upgrade.log`:
   a. Search for the term '`fortisoarupgrade`' to see if there was any error.
   b. If the error has occurred post installation of FortiSOAR, consult Support. If FortiSOAR was not installed, then proceed with the steps.
2. Check for the existence of the backup file. The filename of the backup file starts with `DR_XYS.tar`
3. After the OS is rebooted, check if FortiSOAR version 7.3.0 is installed.
4. Check for the existence of the `/var/lib/pgsql/12_bkp` directory.
5. Install `tmux`.
6. If your system uses a proxy, update the proxy configuration for `yum` and in the `/etc/environment` file.

Manual Steps

1. Launch `tmux`.
2. For performing the manual steps on a FortiSOAR MSSP or Enterprise setup, set the following environmental variable using the following command:
   ```
   export fsr_edition=enterprise
   ```

3. Set the following OS environment variable using the following command:
   `export is_inplace_upgrade=true`
4. If FortiSOAR version 7.3.0 is not installed, then download and install FortiSOAR 7.3.0. **If FortiSOAR is already installed, then skip this step**.
   a. `wget https://repo.fortisoar.fortinet.com/7.3.0/install-fortisoar-7.3.0.bin`
   b. Start the installation by executing the following command:
      `sh install-fortisoar-7.3.0.bin`
   c. Follow the on-screen instructions and complete the installation.
5. Rename the database backup directory:
   `mv /var/lib/pgsql/12_bkp /var/lib/pgsql/12`
6. Once FortiSOAR is installed, begin reconfiguring FortiSOAR:
   a. Download the migration script using the following command:
      `# wget https://repo.fortisoar.fortinet.com/7.3.0/migrate-fortisoar-7.3.0.bin`
   b. Initiate the restoration of your FortiSOAR configurations using the following command:
      `# sh migrate-fortisoar-7.3.0.bin --import [<backup_dir_path>]`
   c. Follow the on-screen instructions and complete the restoration of your FortiSOAR configurations.
7. Once your FortiSOAR configurations are restored, run the following command:
   `sed -i 's/trust/md5/g' /var/lib/pgsql/14/data/pg_hba.conf`
8. Install '`Ansible`' using the following command:
   ```
   /bin/sudo -u nginx /opt/cyops-workflow/.env/bin/pip install ansible==2.8.2 --extra-index-url https://repo.fortisoar.fortinet.com/prod/connectors/deps/simple/
   ```
9. Restart the FortiSOAR services using the following command:
   `csadm services -restart`
10. Update the login banner as follows:
    Edit the `/etc/motd` file to change the '`CentOS Version: 7.9.2009`' string to '`Rocky Linux Version: 8.6`'
11. Update the attributes in the `resolv.conf` file using the following command:
    `/bin/chattr -i filepath`
    This completes the FortiSOAR upgrade to release 7.3.0.

Upgrading FortiSOAR with an externalized database

1. Use in place upgrade script to upgrade to 7.3.0, see the Upgrading FortiSOAR using the in-place upgrade method topic.
2. Once FortiSOAR is successfully upgraded, upgrade your PostGreSQL version to 14, if you are using self-deployed PostGreSQL.
   If you are using Cloud, then use the cloud service to migrate to PostGreSQL14

Upgrade considerations for varied types of FortiSOAR configurations

You can upgrade the following FortiSOAR configuration:

- FortiSOAR Enterprise Edition - Standalone and HA.
  Notes:
  All nodes within an HA cluster must be upgraded to the same release of FortiSOAR.
  Post-upgrade, you will need to reconfigure the HA cluster.
  For more information, see the Upgrading a FortiSOAR High Availability Cluster chapter.

- FortiSOAR MSSP Edition - Standalone and HA
  Notes:
  In the case of an MSSP setup, the master, tenant, and secure exchange message nodes must be upgraded to the same release of FortiSOAR.
  For more information, see the Upgrading a FortiSOAR Distributed Multi-Tenancy Configuration chapter.
- FortiSOAR on FortiCloud. For more information, see the *Upgrade Information* chapter in the "FortiSOAR Cloud 7.3.0 Release Notes".

Upgrade Notes

- The postfix version bundled with FortiSOAR 7.3.0 has multiple "Safety Net" improvements. So that customer workflows built with the SMTP connector and using the local postfix configuration are not blocked, the postfix configuration is updated to the `compatibility_level` of '2'. However, it is strongly recommended that you apply the new settings such as `smtpd_relay_restriction` to have good relay restrictions, etc. For more information, see the Postfix Backwards-Compatibility Safety Net article.

Troubleshooting in-place upgrade failures

The in-place upgrade can fail for various reasons, and you can resolve them by checking the reason of the failure by reviewing the `leapp-report.txt` file located at `/var/log/leapp/leapp-report.txt`. The `leapp-report.txt` details the risk factor's level of severity, the title and summary of the failure reason, and the issue's solution. You can restart the upgrade after fixing the problem as advised in the `leapp-report.txt` file. A copy of the `leapp-report.txt` file is also saved in location from where the upgrade script is executed.

In-place upgrades fail on setups that have their proxy configured

If you have a system that has its proxy configured, then the in-place upgrade fails with the following error:

```
Failed to synchronize cache for repo
```

Resolution

On your appliance terminal, run the following command:

```
export LEAPP_PROXY_HOST=http://<ADDRESS>:<PORT>
```

Replace `<address>` and `<port>` with your actual proxy.

If this solution does not work, then do the following:

1. Run the following command:
   ```
   sed -i '/^enabled=.*/a proxy=<proxy server>' /etc/leapp/files/leapp_upgrade_repositories.repo
   ```
   Replace `<proxy server>` with the actual proxy server.
2. Run the following command:
   ```
   execute truncate -s -1 fortisoar-inplace-upgrade-7.3.0.bin
   ```
3. Restart the upgrade procedure by running the following command to re-launch the migration tool:
   ```
   sh fortisoar-inplace-upgrade-7.3.0.bin
   ```

In-place upgrades fail with the 'Possible problems with remote login using root account' error

This issue occurs when you have deployed a Centos VM where `root` is allowed to login. However, as per RHEL8 policy `root` is not allowed for "ssh" access and requires to blocked, leading to pre-upgrade checks failing with the `Possible problems with remote login using root account` error.

Resolution

1. Add a "non-root" user with 'admin' privileges and disable `ssh` login for the `root` user.
   For additional information, you can also check the `leapp-report.txt` file.
2. Restart the upgrade procedure by running the following command to re-launch the migration tool:
   ```
   sh fortisoar-inplace-upgrade-7.3.0.bin
   ```

Pre-upgrade check for in-place upgrade fails with 'kernel' issues

The the pre-upgrade check fails with the following errors when you have updated a system that causes the kernel to upgrade, but you have forgotten to reboot the system after the upgrade:

```
###################
Upgrade has been inhibited due to the following problems:

    1. Inhibitor: Multiple devel kernels installed

    2. Inhibitor: Newest installed kernel not in use

Consult the pre-upgrade report for details and possible remediation.
######################
```

Resolution

1. Reboot your system.
2. Restart the upgrade procedure by running the following command to re-launch the migration tool:
   ```
   sh fortisoar-inplace-upgrade-7.3.0.bin
   ```

Pre-upgrade check for in-place upgrade fails with a 'synchronization error for the fsr repositories' error

The pre-upgrade checks fail with a synchronization error for the fsr repositories, for example,
`"Failed to synchronize cache for repo 'fsr-rockylinux-baseos', ignoring this repo."`

This issue occurs when `yum` fails to recognize the proxy settings and therefore, the proxy settings need to be explicitly configured for each repository.

Resolution

1. Manually set the proxy for each repository using the following command:
   ```
   sed -i '/^enabled=.*/a proxy=<proxy>' fortisoar-inplace-upgrade-7.3.0.bin
   ```
   For example, `sed -i '/^enabled=.*/a proxy=http://user:password@10.10.10.10:808' fortisoar-inplace-upgrade-7.3.0.bin`
2. Refresh the binary to apply the proxy changes using the following command:
   ```
   truncate -s -1 fortisoar-inplace-upgrade-7.3.0.bin
   ```
3. Re-run the upgrade script using the following command:
   ```
   sh fortisoar-inplace-upgrade-7.3.0.bin
   ```

Troubleshooting upgrade issues

This topic provides you with troubleshooting tips, irrespective of the selected upgrade method.

Retrying of failed notifications might fail

Before you start upgrading FortiSOAR, you must review failed notifications. After the upgrade, you can retry a failed notification by clicking **Settings** > **Notifications** > **Failure Notifications Logs** tab, selecting the failed notification, and then clicking **Retry Notification**. This "Retry" process might still fail.

Resolution

If the "Retry" for failed notifications still fails after the upgrade, then restart the `fsr-workflow` (`systemctl restart celeryd celerybeatd fsr-workflow`) and `uwsgi` (`# systemctl restart uwsgi`) services.

Error messages displayed during the restore process

During the post-reboot phase in the case of an in-place upgrade or the database restore phase in the case of an upgrade using the export-import method errors such as the following is displayed:

```
Error: unable to perform an operation on node 'rabbit@qa-sme-720-sys1'. Please see
diagnostics information and suggestions below.
```

Resolution

You can ignore these errors because they show that your configurations are currently being restored.

Upgrading a FortiSOAR High Availability Cluster

This section describes the procedure to upgrade a FortiSOAR High Availability (HA) cluster.

To upgrade a high availability cluster in FortiSOAR, you require to upgrade each node individually, one after the other.

This section considers that the HA setup has a Reverse Proxy or Load Balancer such as "HAProxy" configured.

Refer to the Preparing to Upgrade FortiSOAR section and ensure that all the prerequisites mentioned in that section are met. The upgrade installer will handle all FortiSOAR services management.

Upgrading an Active-Active HA Cluster

For the purpose of the following procedure, *Node1* is considered as the Active Primary node, *Node2* is considered as the Active Secondary node. Both the nodes are fronted by a Reverse Proxy or Load Balancer such as "HAProxy".

Approximately 30 minutes of downtime is required for the upgrade.

To upgrade your active-active HA cluster to FortiSOAR 7.3.0, perform the following steps:

1. Configure the Reverse Proxy to pass requests only to *Node1*.
   This ensures that FortiSOAR requests are passed only to *Node1*, and *Node2* can be upgraded.
2. Use the `#csadm ha` command as a root user and run the `leave-cluster` command on *Node2*.
   This makes *Node2* a standalone system.
3. Upgrade *Node2* using the process mentioned in the Upgrading FortiSOAR chapter.
   Once the upgrade of *Node2* is completed successfully, you can now upgrade *Node1*.
   Important: Upgrade of *Node1* will incur downtime.
4. Once both the nodes are upgraded then run the `join-cluster` command from *Node2*.
5. Configure the Reverse Proxy again to handle requests from both *Node1* and *Node2*.

Upgrading an Active-Passive HA Cluster

For the purpose of the following procedure, *Node1* is considered as the Active Primary node, *Node2* is considered as the Passive Secondary node. Both the nodes are fronted by a Reverse Proxy or Load Balancer such as "HAProxy".

Approximately 30 minutes of downtime is required for the upgrade.

To upgrade your active-passive HA cluster to FortiSOAR 7.3.0, perform the following steps:

1. Reverse Proxy is configured to have *Node2* as backup system. Therefore, you require to comment out that part from Reverse Proxy configuration.
2. Use the `#csadm ha` command as a `root` user and run the `leave-cluster` command on *Node2*.
   This makes *Node2* a standalone system.
3. Upgrade *Node2* using the process mentioned in the Upgrading FortiSOAR chapter.
   Once the upgrade of *Node2* is completed successfully, you can now upgrade *Node1*.
   Important: Upgrade of *Node1* will incur downtime.
4. Once both the nodes are upgraded then run the `join-cluster` command from *Node2*.
5. Configure the Reverse Proxy again to set *Node2* as the backup server.

Upgrading a FortiSOAR Distributed Multi-Tenancy Configuration

This section describes the procedure to upgrade a FortiSOAR distributed multi-tenant configuration for managed security services providers (MSSPs) or Distributed SOC configuration.

You must first upgrade the master node of your FortiSOAR distributed multi-tenant configuration and only then upgrade the tenant nodes of your FortiSOAR multi-tenancy setup.

⚠ In case of a distributed deployment, both the master and the tenant nodes must be upgraded. A version mismatch will not work if either of them upgrades to 7.3.0.

Upgrading a FortiSOAR master node

Before you upgrade your FortiSOAR master node, ensure the following:

- All playbooks have completed their execution on the master.
- The tenant node(s) are deactivated from the master node before upgrading the master node, and tenant nodes have disabled communication to the master node from the "`Master Configuration`" page.

If the master node of your multi-tenant configuration is part of an HA setup, i.e., MSSP +HA, then follow the steps mentioned in the Upgrading a FortiSOAR High Availability Cluster chapter.

If the master node of your multi-tenant configuration is not part of an HA setup, then follow the steps mentioned in the Upgrading FortiSOAR chapter.

Upgrading a FortiSOAR Tenant node

Before you upgrade your FortiSOAR tenant node, ensure the following:

- Data replication from the tenant node to the master node is stopped. You can stop data replication by logging on to the tenant node and clicking **Settings** to open the `System` page, then in the `Multi Tenancy` section, click the **Master Configuration** menu item and then in the `Communication With Master Node` section, toggle the **Enabled** button to **NO**.
- All playbooks have completed their execution on the tenant.
- All schedule playbooks that fetch data from data sources to the tenant are stopped.
- Any application that pushes data from data sources to the tenant is stopped.

If the tenant node of your multi-tenant configuration is part of an HA setup, i.e., MSSP +HA, then follow the steps mentioned in the Upgrading a FortiSOAR High Availability Cluster chapter.

If the tenant node of your multi-tenant configuration is not part of an HA setup, then follow the steps mentioned in the Upgrading FortiSOAR chapter.

After the tenant node has been successfully upgraded, you must toggle the **Allow Module Management** setting to **NO** and then back to **YES**. This is needed only if you were already using the 'Allow Module Management' feature and is required to synchronize the tenant module metadata with the master instance. You can ignore this step, if your 'Allow Module Management' setting was already disabled before the upgrade.

Upgrading a FortiSOAR Secure Message Exchange

A secure message exchange establishes a secure channel that is used to relay information to the agents or tenant nodes. To create a dedicated secure channel, you are required to add the reference of the installed and configured secure message exchange, when you add agent or tenant nodes to your environment. For information on agents see the *Segmented Network support in FortiSOAR* chapter in the "Administration Guide," and for more information on secure message exchange and tenants, see the "Multi-Tenancy support in FortiSOAR Guide".

1. Ensure that you stop data replication between the master and the tenant nodes. You can stop data replication by logging on to the tenant node and clicking **Settings** to open the `System` page, then in the `Multi Tenancy` section, click the **Master Configuration** menu item and then in the `Communication With Master Node` section, toggle the **Enabled** button to **NO**.
2. Upgrade Secure Message Exchange using the process mentioned in the Upgrading FortiSOAR chapter.
3. Once you have successfully upgraded the secure message exchange, start the data replication between the master and the tenant nodes again by toggling the **Data Replication** button to **ON**, and then verify the replication.

Upgrading a FortiSOAR Secure Message Exchange Cluster

RabbitMQ supports clustering, that in conjunction with Queue Mirroring can be used for an Active-Active configuration as explained in the Clustering Guide and in the Highly Available (Mirrored) Queues article, which includes steps on how to set up the clusters and monitor queues. The clustered instances should be fronted by a TCP Load Balancer such as HAProxy, and clients should connect to the cluster using the address of the proxy. For more information, see the *Multi-tenancy support in FortiSOAR* guide.

For the purpose of the following procedure, we are considering a two-node MQ mirrored queue clusters that are both added to the Reverse Proxy.

1. Configure the Reverse Proxy to pass requests only to *Node1*, which is the primary node of the MQ cluster. Therefore, now all requests will be handled by *Node1* and *Node2* will be available for maintenance.
2. Log on to the *Node2* terminal session as a `root` user, and upgrade *Node2* by following the steps mentioned in the Upgrading a FortiSOAR Secure Message Exchange topic.
3. Configure the Reverse Proxy to route requests through *Node2*. Therefore, now all requests will be handled by *Node2* and *Node1* will be available for maintenance.
4. Login to *Node1*, and upgrade *Node1* as per the procedure mentioned in **step 2**.
5. Reconfigure the Reverse Proxy to load balance both *Node1* and *Node2*.

Troubleshooting upgrade issues for MSSP setups

This topic provides you with troubleshooting tips for MSSP setups, irrespective of the selected upgrade method.

Replication from tenant to master stops once you upgrade an MSSP with an HA setup

If you have upgraded an MSSP+HA setup, then post-upgrade the replication from tenant nodes to the master node stopped.

Resolution

To resolve this issue, once you have upgraded your MSSP setup and created the HA cluster, you must restart all FortiSOAR services on the primary master node and the primary tenant node using the following command:

```
csadm services --restart
```

Post-Upgrade Tasks

Modify the 'Notify On Pending External Manual Input' Delivery Rule

From FortiSOAR 7.3.0 onwards, you can choose to run unauthenticated manual inputs in segmented networks using FSR agents. To achieve this, the 'Notify On Pending External Manual Input' delivery rule has been updated in the case of fresh installations of FortiSOAR 7.3.0. However, if you have upgraded your FortiSOAR instance to release 7.3.0 or later from a release prior to 7.3.0, you must modify the 'Notify On Pending External Manual Input' rule to allow the running of manual inputs on FSR agents. For the steps on how to achieve this, see the `Modifying the 'Notify On Pending External Manual Input' delivery rule post-upgrade to release 7.3.0 or later` topic in the *System Configuration* chapter of the "Administration Guide."

Disable the 'Notify On Pending Manual Input' Delivery Rule

Post-upgrade to release 7.3.0 or later from a release prior to 7.3.0, you can disable the `Notify On Pending Manual Input` rule, if you want to disable the manual input notification from the 'Notifications Panel'; else you will receive the manual input notification in both the 'Notifications Panel' and the 'Pending Tasks'. In the case of a fresh installation of FortiSOAR 7.3.0 (or later), notifications for manual input are visible on only the **Manual Input** tab in the 'Pending Tasks' panel. For the steps on how to achieve this, see the `Modifying the 'Disabling a Delivery Rule` topic in the *System Configuration* chapter of the "Administration Guide."

Install dependency for the SAP RFC connector

If you had the SAP RFC connector installed on your FortiSOAR instance before upgrading to release 7.3.0 or later from a release prior to 7.3.0, then on the upgraded instance, you will see that the "`Connector Dependencies Failed To Install`" message is displayed on the **Connector Configuration** popup of the SAP RFC connector. In this case you must manually install the dependencies, using the steps mentioned in the `Steps to install dependency python packages required by the SAP RFC connector` topic and the `install_dependencies.sh` script file attached with the SAP RFC Connector document.

Update IPv6 Settings in the case of in-place upgrade

If you have upgrade to FortiSOAR 7.3.0 using the in-place upgrade process and you have not configured IPv6, then you might see errors such as:
"`2022-09-22 11:55:05.957 DEBUG PID: 51248 leapp.workflow.FirstBoot.network_manager_update_connections: ModuleNotFoundError: No module named 'gi'`".
If you do not want to configure IPv6 and do not want there errors to fill up the logs, you require to set the `IPV6INIT` variable to "`no`" in the `/etc/sysconfig/network-scripts/ifcfg-ens160` file.

FORTINET®

www.fortinet.com