OS Update Procedure

FortiSIEM 6.7.1

02/06/2024
FortiSIEM 6.7.1 OS Update Procedure

Change Log

Date	Change Description
01/25/2019	Initial version of the guide.
11/20/2019	CentOS Upgrade Guide released for 5.2.6.
03/30/2020	CentOS Upgrade Guide released for 5.3.0.
11/30/2020	Upgrade to CentOS 8.
03/31/2021	Updated for 6.1.x and 6.2.0.
05/06/2021	CentOS Upgrade Guide released for 6.2.1.
07/06/2021	CentOS Upgrade Guide released for 6.3.0.
08/10/2021	Updated FortiSIEM OS updates for 6.3.0.
08/26/2021	CentOS Upgrade Guide released for 6.3.1.
10/15/2021	CentOS Upgrade Guide released for 6.3.2.
12/22/2021	CentOS Upgrade Guide released for 6.3.3.
01/18/2022	Rocky Linux Upgrade Guide released for 6.4.0.
05/09/2022	Rocky Linux Upgrade Guide released for 6.5.0.
07/26/2022	Rocky Linux Upgrade Guide released for 6.6.0.
09/12/2022	Rocky Linux Upgrade Guide released for 6.5.1.
09/14/2022	Rocky Linux Upgrade Guide released for 6.6.1.
09/19/2022	Rocky Linux Upgrade Guide released for 6.6.2.
01/03/2023	Rocky Linux Upgrade Guide released for 6.7.0.
01/13/2023	"FortiSIEM - OS Update Lifecycle" renamed to "FortiSIEM - OS Update Procedure" and updated for 6.4.0 and later.
02/13/2023	FortiSIEM - OS Update Procedure Guide released for 6.7.1.
03/07/2023	FortiSIEM - OS Update Procedure Guide released for 6.7.2.
03/28/2023	FortiSIEM - OS Update Procedure Guide released for 6.7.3.
04/11/2023	FortiSIEM - OS Update Procedure Guide released for 6.7.4.
05/22/2023	FortiSIEM - OS Update Procedure Guide released for 6.7.5.
06/16/2023	FortiSIEM - OS Update Procedure Guide released for 6.7.6.

Date	Change Description
07/13/2023	FortiSIEM - OS Update Procedure Guide released for 6.7.7.
09/12/2023	FortiSIEM - OS Update Procedure Guide released for 6.7.8.
02/05/2024	FortiSIEM - OS Update Procedure Guide released for 6.7.9.
02/07/2024	FortiSIEM OS Update Procedure explanation of process updated.

FortiSIEM OS Update Procedure

FortiSIEM runs on Rocky Linux. This document provides steps for customers to upgrade their version of Rocky Linux, without upgrading FortiSIEM.

FortiSIEM maintains its own Rocky Linux repository.

- os-pkgs-cdn.fortisiem.fortinet.com
- os-pkgs-r8.fortisiem.fortinet.com

When Rocky Linux publishes an OS update, an announcement is made via Rocky Linux 8 Changelog. The FortiSIEM engineering team review the Rocky Linux 8 Changelog on a weekly basis.

Once a new update is available, the FortiSIEM engineering team first tests these updates for stability and upgradability from older OS versions. After confirming that the update is safe to deploy, FortiSIEM updates its Rocky Linux repository from official Rocky Linux 8 mirror servers.

Upon notification of a critical Rocky Linux vulnerability, the FortiSIEM engineering team review the update out of band of the weekly Changelog review. If deemed necessary, the FortiSIEM team will update the FortiSIEM Rocky Linux repositories.

Customers can then upgrade their FortiSIEM OS without necessarily upgrading the FortiSIEM application.

To upgrade FortiSIEM OS without going to the latest FortiSIEM release, take follow the steps.

Notes:

1. For FortiSIEM OS upgrade, you will need port 443 access to:
   - os-pkgs-cdn.fortisiem.fortinet.com
   - os-pkgs-r8.fortisiem.fortinet.com
2. You can upgrade from FortiSIEM 6.4.1, 6.4.2, 6.5.0, 6.5.1, 6.6.0, 6.6.1, 6.6.2, 6.6.3 and 6.7.0+. If you are running versions older than 6.4.1, then first upgrade FortiSIEM to 6.4.1 and then perform OS upgrade.
3. If you are running FortiSIEM in an offline mode without internet connection, then you need to set up an offline repository server instead of directly using the Fortinet OS repo. Check the latest Offline Upgrade guide in the FortiSIEM Documents Library for more information.

The following OS upgrade steps apply to all FortiSIEM nodes – Supervisor, Worker, Collector and FortiSIEM Manager.

Step 1: Find the Rocky Linux Version in your FortiSIEM

1. SSH to FortiSIEM node as root.
2. Run the following command to get the Rocky Linux version information.

   ```
   cat /etc/redhat-release
   ```

   Example command and output:

   ```
   [root@Autosuper111 ~]# cat /etc/redhat-release
   Rocky Linux release 8.6 (Green Obsidian)
   ```

Step 2: Find the Rocky Linux Version in the FortiSIEM Rocky Linux Repo

Follow one of the following two options:

Option 1:

Run the following command.

```
yum check-update
```

Example Command and Output (Output shortened for brevity):

```
# yum check-update
Last metadata expiration check: 2:57:08 ago on Fri 13 Jan 2023 04:26:09 PM PST.

NetworkManager.x86_64
1:1.40.0-2.el8_7
     baseos
NetworkManager-initscripts-updown.noarch
1:1.40.0-2.el8_7
     baseos
NetworkManager-libnm.x86_64
1:1.40.0-2.el8_7
     baseos
NetworkManager-team.x86_64
1:1.40.0-2.el8_7
     baseos
NetworkManager-tui.x86_64
1:1.40.0-2.el8_7
     baseos
...

xinetd.x86_64
2:2.3.15-25.el8
     appstream
yum.noarch
4.7.0-11.el8
     baseos
zlib.i686
1.2.11-20.el8
     baseos
zlib.x86_64
1.2.11-20.el8
     baseos
Obsoleting Packages
gdb.x86_64                                                                                8.2-
19.el8
 appstream
    gdb.x86_64                                                                            8.2-
18.el8
 @appstream
gdb-headless.x86_64                                                                       8.2-
19.el8
 appstream
    gdb-headless.x86_64                                                                   8.2-
18.el8
 @appstream
```

```
grub2-tools.x86_64
1:2.02-142.el8.rocky.0.2
     baseos
    grub2-tools.x86_64
1:2.02-123.el8_6.8.rocky.0.2
     @baseos
grub2-tools-efi.x86_64
1:2.02-142.el8.rocky.0.2
     baseos
    grub2-tools.x86_64
1:2.02-123.el8_6.8.rocky.0.2
     @baseos
grub2-tools-extra.x86_64
1:2.02-142.el8.rocky.0.2
     baseos
    grub2-tools.x86_64
1:2.02-123.el8_6.8.rocky.0.2
     @baseos
grub2-tools-minimal.x86_64
1:2.02-142.el8.rocky.0.2
     baseos
    grub2-tools.x86_64
1:2.02-123.el8_6.8.rocky.0.2
     @baseos
kernel-headers.x86_64
4.18.0-425.3.1.el8
     baseos
    kernel-headers.x86_64
4.18.0-372.26.1.el8_6
     @baseos
```

Option 2:

Run the following command.

```
yum list updates
```

Example Command and Output (Output shortened for brevity):

```
# yum list updates
Last metadata expiration check: 2:58:10 ago on Fri 13 Jan 2023 04:26:09 PM PST.
Available Upgrades
NetworkManager.x86_64
1:1.40.0-2.el8_7
      baseos
NetworkManager-initscripts-updown.noarch
1:1.40.0-2.el8_7
      baseos
NetworkManager-libnm.x86_64
1:1.40.0-2.el8_7
      baseos
NetworkManager-team.x86_64
1:1.40.0-2.el8_7
      baseos
NetworkManager-tui.x86_64
1:1.40.0-2.el8_7
      baseos
```

```
...

wireshark-cli.x86_64
1:2.6.2-15.el8
      appstream
xinetd.x86_64
2:2.3.15-25.el8
      appstream
yum.noarch
4.7.0-11.el8
      baseos
zlib.i686
1.2.11-20.el8
      baseos
zlib.x86_64
1.2.11-20.el8
      baseos
```

Step 3: Upgrade your FortiSIEM OS

If you decide to upgrade, then take the following steps.

1. Run the following command.

   ```
   yum upgrade -y
   ```

2. After the upgrade is done, follow Step 1 to verify the new version. This ensures that the upgrade has completed successfully.
3. Check if reboot is required by running the following command.

   ```
   yum install -y yum-utils &> /dev/null && needs-restarting -r
   ```

   Example command and output:

   ```
   [root@Autoworker111 ~]# yum install -y yum-utils &> /dev/null && needs-restarting -
   r
   Core libraries or services have been updated since boot-up:
   * dbus
   * dbus-daemon
   * glibc
   * kernel
   * linux-firmware
   * systemd
   Reboot is required to fully utilize these updates.
   More information: https://access.redhat.com/solutions/27943
   [root@Autoworker111 ~]#
   ```

4. If reboot is required, then run the following command.

   ```
   reboot
   ```

5. Make sure all FortiSIEM processes are up.

FORTINET®

www.fortinet.com