FortiNAC

CentOS Updates

Firmware: 6.x (CentOS 7)

Date: March 22, 2021

Rev: L

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
http://kb.fortinet.com

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

Contents

Overview

Introduction

Fortinet's appliances are based on CentOS Linux distribution. CentOS is a Linux distribution that is based on a commercial offering of Linux called Red Hat Enterprise Linux (RHEL). The CentOS organization repackages software released by Red Hat and makes it available for commercial use. RHEL and CentOS are designed to be stable, long-term Linux distributions. These distributions have a clear timeline, and maintenance work is regularly made available for these distributions. New functionality is not really a goal in the management of these distributions -- stability is.

The CentOS organization publishes periodic bugfix and security updates for the CentOS Distribution. Tens-of- thousands of organizations already use these updates. The CentOS distribution is grouped into "packages".

The packages are transported in specially formatted data files. Fortinet uses "Red Hat Package Manager" (RPM) as the package format. There are hundreds of packages installed on a typical Fortinet appliance. For example, the Apache HTTP server might comprise one package, and the library that implements SSL services might exist inside another package.

Sometimes the CentOS organization publishes many updates in a given day and sometimes days go by without an update. To get an idea for how often the CentOS organization releases software updates, and the variety of issues which are included, refer to the centos-announce mailing list, here:
http://lists.centos.org/pipermail/centos-announce/

CentOS Application Versions

FortiNAC software is dependent upon certain applications embedded within the CentOS 7 operating system. Fortinet relies on CentOS/Red Hat to update and maintain these applications. They are not maintained separately.

Tomcat
Currently FortiNAC uses Tomcat v7 (included with CentOS 7). There are no plans to upgrade unless CentOS 7 upgrades Tomcat.

Fortinet Update Policy

The CentOS organization makes updates available in repositories (web/ftp servers on their site.) Fortinet retrieves the updates from the CentOS site periodically, prepares its own repository and validates that the resulting set of packages is complete and compatible with FortiNAC. Fortinet follows the CentOS organization's update policy, in that the decision to correct any reported error is dependent on CentOS.

If the CentOS organization identifies the severity rating as CRITICAL, Fortinet will incorporate the changes into the repository as soon as is reasonable. If the CentOS organization does not provide changes to address the reported error, Fortinet will not provide a fix.

The below severity rating information was taken from the following URL:
https://access.redhat.com/security/updates/classification

Severity Rating Definitions

Critical impact	This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. These are the types of vulnerabilities that can be exploited by worms. Flaws that require an authenticated remote user, a local user, or an unlikely configuration are not classed as Critical impact.
Important impact	This rating is given to flaws that can easily compromise the confidentiality, integrity, or availability of resources. These are the types of vulnerabilities that allow local users to gain privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow remote users to cause a denial of service.
Moderate impact	This rating is given to flaws that may be more difficult to exploit but could still lead to some compromise of the confidentiality, integrity, or availability of resources, under certain circumstances. These are the types of vulnerabilities that could have had a Critical impact or Important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations.
Low impact	This rating is given to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences.

All available changes from CentOS are incorporated into Fortinet's repository for a "maintenance update", released once each quarter.

For a complete list of packages currently available browse to:
http://downloads.bradfordnetworks.com/pub/centos-repos/STABLE/7/updates/x86_64/

Some vulnerability reports list services that can be exploited if the default configuration is used. We do not use default configurations, which are often described in the reports.

In addition to mirroring CentOS, Fortinet regularly runs scans against the appliance and contracts an outside security firm to perform security assessments on the appliance.

Update Process

To configure CentOS on a system, Fortinet uses "yum" - a tool that retrieves packages from the Internet and takes into consideration any dependencies. For example, it is possible to invoke the "yum" program to (loosely speaking) "install package ABC"....whereupon "yum" goes to the Internet to obtain package ABC....as well as the 30 other packages that ABC depends on.

Every CentOS update which Fortinet provides in its repository is included in Fortinet's Release Matrix. The Release Matrix contains a link to the list of packages that are relevant to FortiNAC. The same information can be obtained with the **sysinfo -v** command in the Command Line Interface of FortiNAC.

Servers which can access the internet use "yum", which already exists on CentOS systems. Updates can be initiated from the Admin UI or from the system's CLI. Servers which cannot access the internet will need to download the packages and then build their own ftp update server to provide the updates and necessary keys for validating the packages.

Note: Each FortiNAC appliance or virtual machine must be updated individually. This applies to all of the following environments:

- FortiNAC Control Server and Application Server pairs
- FortiNAC Control Manager (NCM) managing multiple appliances
- High Availability configuration with redundant servers

General Requirements

- FortiNAC Version 8.0 or higher.
- FortiNAC firmware versions 6.x and higher. This firmware version runs on CentOS 7. Updates for CentOS 5 are no longer available.
- Root access to each appliance or virtual machine.
- Access to **updates.bradfordnetworks.com** from each appliance or virtual machine (FTP, HTTP or HTTPS).
    - Default transfer protocol
        - Versions 8.8.1 and lower: FTP
        - Versions 8.8.2 and above: HTTP
    - To change the transfer protocol used, see Appendix.

- HTTP access to **centos.org** from each appliance or virtual machine.
- Maintenance window to reboot the appliance or virtual machine after installing the updates.
- Hardware appliances: Dell hardware with one of these SKUs:
  FNC-CA-XXXC
  FNC-C-XXXXC
  FNC-A-XXXXC
  FNC-M-550C

  Legacy models:
  FNC-R-650C
  SYS-BFN330-XXXX, SYS-BFN630-XXXX, SYS-BFN630XL-XXXX, SYS-G-BFN630-XXXX
  SYC-FNT440-XXX, SYC-FNT440XL-XXX, SYC-FNT330-000

Considerations

- The UI will *not* record and display dates of Operating System updates that are run using the CLI method. If it is desired to keep record of the last OS update, update using the Administrative UI.
- OS Updates replace all prior OS Updates and do not require that prior updates be installed first.
- If you are experiencing any issues with the Operating System, you are required to install the most recent release of OS Updates before Support can troubleshoot the problem.
- Update packages are signed and will not install if keys do not match those on the appliance.
- The file bradford-build-pgp-pubkey.txt contains the public half of a keypair that is used to secure the rpms that are contained in Fortinet's repositories. This allows the OS Update packages to be downloaded over unsecure FTP connections with confidence that they have come from Fortinet and they have not been tampered with.

Procedure

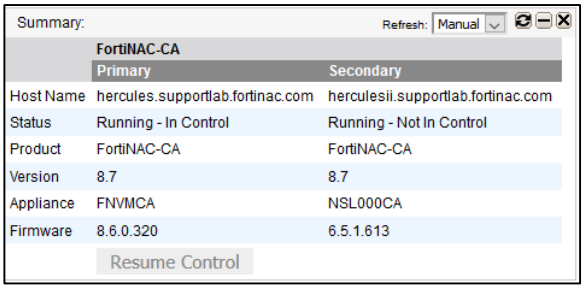
The updates can be performed either using the Administration UI or the appliance CLI.

Preparation

1. If updating virtual machines, take a snapshot of the VM before performing the update.
2. Verify the firmware version is 6.x or higher. **Important:** Do not install the updates if the firmware version is not correct or the Linux Distribution is not CentOS.

   UI Method: Firmware is listed in the **Summary** panel of the Dashboard.

   Example:



   CLI Method: Open an SSH session to the first appliance or virtual machine to be updated using PuTTy or some other SSH tool. Log in as **root**.

   Verify the appliance has firmware version 6.x or higher using the following command:
   `sysinfo`

Example:

```
> sysinfo
      ************************************************************************
         Recognized platform: Linux
                 Distribution: CentOS Linux release 7.7.1908 (Core)
                    OS Kernel: 3.10.0-1062.9.1.el7.x86_64
               Home directory: /root
                Terminal type: xterm

                 Product Type: NetworkControlApplicationServer
               Product Family: NetworkSentry
               Appliance Type: FortiNAC FNVMCA
               Engine Version: 8.7.2.640
                   Build Date: Fri 06-Mar-2020
            Firmware Version: 8.6.0.320
                Firmware Date: 2019-07-29
      ************************************************************************
```

Download and Install Updates

Update least impactful appliance first: If multiple appliances are being updated, it is suggested to update the least impactful appliance first (e.g. secondary server in High Availability configuration). Once appliance has come up successfully, proceed with other appliances. This is especially recommended for physical appliances in the rare event the appliance does not complete boot up. Should a virtual appliance not come up after reboot, a snapshot can be used to restore.

UI Method

1. Navigate to **System > Settings > Updates > Operating System**.
2. Click **Check for Updates** to check the FTP server for updates and assess whether the FortiNAC servers are up to date or not.
3. Click **Update All** to begin downloading and installing the operating system updates.
4. A warning is displayed indicating that this is a long process and that you must reboot the server after the update. Click **Yes** to continue.
5. Use **Show Log** at the bottom of the table to view a log of the update process.
6. When the update process is complete, shut down the FortiNAC process and reboot the appliance or virtual machine. This can be done via the Administration UI or the CLI.

Important: Reboot the appliance as soon as the update process is complete. Otherwise, if a service were to be stopped and restarted, there could be a component mismatch and the server will not run correctly.

CLI Method

Perform the following steps on **all** appliances.

1. Login to the appliance CLI as root.
2. Verify appliance can reach the repositories. Type

   ```
   yum check-update
   ```

   Example of a successful check

```
> yum check-update
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
bradford-stable                                | 2.9 kB     00:00
bradford-updates-stable                        | 2.9 kB     00:00
networkradius-stable                           | 2.9 kB     00:00
```

3. Download and install the updates from the repositories enabled in **bradford.repo**, type the following:

   ```
   yum -y update
   ```

Note: Depending upon when the last update was run, this process can take several minutes. To stop any updates already in progress, see Appendix.

4. When the update process is complete, shut down the FortiNAC process and reboot the appliance or virtual machine. This can be done via the Administration UI or the CLI.

Important: Reboot the appliance as soon as the update process is complete. Otherwise, if a service were to be stopped and restarted, there could be a component mismatch and the server will not run correctly.

Reboot Servers

UI Method

Use the applicable procedure:
Single Appliance
Single Appliance (High Availability)
Control and Application Server pair
Control and Application Server pair (High Availability)

Single Appliance

1. Navigate to **System > Settings > System Management > Power Management**
2. Select a server from the list.
3. Click **Reboot**.
4. After 4-5 minutes, confirm that the Admin UI the server is up.
5. Proceed to Validate.

Single Appliance (High Availability)

1. Navigate to **System > Settings > System Management > Power Management**
2. Select the Secondary Server from the list.
3. Click **Reboot**.
4. Select the Primary Server from the list.
5. Click **Reboot**.
6. After 4-5 minutes, confirm that the Admin UI dashboard shows both servers up.
7. Proceed to Validate.

Control and Application Server pair

1. Navigate to **System > Settings > System Management > Power Management**
2. Select the Application Server from the list.
3. Click **Reboot**.
4. Select the Control Server from the list.
5. Click **Reboot**.
6. After 4-5 minutes, confirm that the Admin UI dashboard shows both servers up.
7. Proceed to Validate.

Control and Application Server pair (High Availability)

1. Navigate to **System > Settings > System Management > Power Management**
2. Select the Secondary Application Server from the list.
3. Click **Reboot**.

4. Select the Secondary Control Server from the list.
5. Click **Reboot**.
6. Select the Primary Application Server from the list.
7. Click **Reboot**.
8. Select the Primary Control Server from the list.
9. Click **Reboot**.
10. After 4-5 minutes, confirm that the Admin UI dashboard shows all servers up.
11. Proceed to Validate.

CLI Method

Use the applicable procedure:
Single Appliance
Single Appliance (High Availability)
Analytics Reporter (FNC-R-VM)
Control and Application Server pair
Control and Application Server pair (High Availability)

Control Manager (NCM) or a Single Control Application Server

1. On the server, run
   `shutdownCampusMgr`

2. Wait 30 seconds and run
   `shutdownCampusMgr -kill`
   `reboot`

3. After 4-5 minutes, confirm that the Admin UI dashboard shows all servers up.

4. Proceed to Validate.

Control Manager (NCM) or a Single Control Application Server (High Availability)

1. On Primary server run
   `shutdownCampusMgr`

2. Wait 30 seconds.

3. On both servers run
   `shutdownCampusMgr -kill`

4. On Primary Server, run
   `reboot`

5. Wait until the Primary Server is up and running (confirm SSH and Admin UI access).

6. On Secondary Server, run
   `reboot`

7. After 4-5 minutes, confirm that the Admin UI dashboard shows all servers up.

8. Proceed to Validate.

Analytics Server

1. On the server, run
   ```
   service bsc-wildfly stop
   ```
2. Wait 30 seconds and run
   ```
   reboot
   ```
3. Proceed to Validate.

Control Server and Application Server Pair (Non-HA Configuration)

1. On the Control Server, run
   ```
   shutdownCampusMgr
   ```
2. Wait 30 seconds and run
   ```
   shutdownCampusMgr –kill
   ```
3. On the Application Server, run
   ```
   shutdownCampusMgr -kill
   reboot
   ```
4. Wait 30 seconds.
5. On the Control Server, run
   ```
   reboot
   ```
6. After 4-5 minutes, confirm the Admin UI is accessible.
7. Proceed to Validate.

Control and Application Server Pair (HA Configuration)

This procedure reboots appliances without causing a failover.

1. On all servers run
   `shutdownCampusMgr`
2. Wait 30 seconds.
3. On all servers run
   `shutdownCampusMgr -kill`
4. On Primary Application Server, run
   `reboot`
5. Wait 30 seconds.
6. On Primary Control Server, run
   `reboot`
7. Wait until the Primary Control and Application Servers are up and running (confirm SSH and Admin UI access).
8. On Secondary Application Server, run
   `reboot`
9. On Secondary Control Server, run
   `reboot`
10. After 4-5 minutes, confirm that the Admin UI dashboard shows all servers up.
11. Proceed to Validate.

Validate

After installing the Operating System Updates, refer to the Product Bulletin for information about the package versions you should expect to have after the update. Some version numbers will remain the same from one update to the next if no update was required by CentOS to a particular package.

1. Open an SSH session to the appliance or virtual machine that was updated.

2. Log in as **root**.

3. Most package versions can be verified by typing

   ```
   sysinfo -v
   ```

   Packages that do not display using `sysinfo` can be verified individually using an rpm command. The following example lists current sudo version:

   ```
   rpm -qa | grep -i sudo
   ```

4. The CVE's addressed in an update can also be verified. Example listing CVE's fixed in sudo update:

   ```
   rpm -q sudo --changelog | grep CVE
   ```

   For more information, refer to the following URL:
   https://wiki.centos.org/FAQ/General#A_PCI_audit_says_I_am_running_a_version_which_has_CVE_exploits_in_it

Contact Support for assistance.

Troubleshooting

Issue: Update fails to start and displayed the message "There are no enabled repos."
Solution: Enable the appropriate repos. See Appendix topic **Enable CentOS Update**.

Related KB Articles

Upgrade aborts with error detecting CentOS 5
https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD49641

Operating system updates fail with errors
https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD49892

Error when restarting an inturrupted operating system update
https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD44569

Appendix

Stopping Updates in Progress

Type the following series of commands:

Note: You may see FAILED after the stop command is run because typically this service is not running.

```
service yum-updatesd stop
chkconfig yum-updatesd off
killall yum-updatesd
yum clean all
```

Enable CentOS Update

The file **bradford.repo** contains file transfer protocol settings and information to enable and disable access to different repositories.

Important: This procedure enables the "stable" repositories. Do not enable the "beta" repositories as these are for testing purposes.

1. Using vi or another text editor, modify the **bradford.repo** file:

   `/etc/yum.repos.d/bradford.repo`

2. Scroll to the bradford-stable section shown in the file and set enabled= to 1 if it is not already set. Save your changes.

   For example:

   ```
   [bradford-stable]
   name=bradford CentOS-$releasever - Stable Repository of CentOS repos
   baseurl=ftp://downloads.bradfordnetworks.com/pub/centos-
   repos/STABLE/$releasever/updates/
   $basearch/
   gpgcheck=1
   gpgkey=http://mirror.centos.org/centos/RPM-GPG-KEY-CentOS-5
   enabled=1
   ```

3. Enable the **httpd/apache** update from the **bradford-updates-stable** repository.
    a. Scroll to the bradford-updates-stable section shown in the file and set enabled= to 1 if it is not set already. Save your changes. For example:

    ```
    [bradford-updates-stable]
    name=bradford CentOS-$releasever - Stable Repository of Updates to CentOS packages
    baseurl=ftp://downloads.bradfordnetworks.com/pub/bradford-updates/STABLE/$releasever/ updates/$basearch/
    gpgcheck=1
    gpgkey=file:/bsc/campusMgr/bin/install/bradford-build-pgp-pubkey.txt
    enabled=1
    ```

    Note: Appliances and VMs that are running firmware version 4.0.4.140 or higher or software version 6.0.4.140 already include the following file change, so this step can be skipped.

    b. Scroll to the **bradford-updates-stable** repository section. Remove one of the two backslash (/) characters after the colon in this line:

    ```
    gpgkey=file://bsc/campusMgr/bin/install/bradford-build-pgp-pubkey.txt
    ```

    It should look like this:

    ```
    gpgkey=file:/bsc/campusMgr/bin/install/bradford-build-pgp-pubkey.txt
    ```

4. Save the changes you have made and exit the editor.
5. **Versions 8.8.0 and above: networkradius.repo** must also be modified with similar changes, otherwise, the centOS update will not complete. This is file used for downloading the centOS files for the Local RADIUS Server feature.

    ```
    /etc/yum.repos.d/networkradius.repo
    ```

    Note: The .repo files are not overwritten during upgrades, so changes will be permanent.

Change Transfer Protocol

The default transfer protocol in the repo files is dependent upon the code version:
Versions 8.8.1 and lower: FTP
Versions 8.8.2 and higher: HTTP

This setting can be changed to HTTPS or HTTP.

1. Using vi or another text editor, modify the **bradford.repo** file:

   `/etc/yum.repos.d/bradford.repo`

2. To change the file transfer protocol from FTP to HTTPS or HTTP, change all four instances of the baseurl in the bradford.repo file. For example:

   From:

   `baseurl=ftp://downloads.bradfordnetworks.com`

   To one of the following:

   `baseurl=https://downloads.bradfordnetworks.com`

   `baseurl=http://downloads.bradfordnetworks.com`

3. Save the changes and exit the editor.

   Note: The bradford.repo file is not overwritten during upgrades, so changes will be permanent.

4. Verify changes:

```
> grep -i baseurl /etc/yum.repos.d/bradford.repo
baseurl=http://downloads.bradfordnetworks.com/pub/centos-repos/BETA/$releasever/updates/$basearch/
baseurl=http://downloads.bradfordnetworks.com/pub/centos-repos/STABLE/$releasever/updates/$basearch/
baseurl=http://downloads.bradfordnetworks.com/pub/bradford-updates/BETA/$releasever/updates/$basearch/
baseurl=http://downloads.bradfordnetworks.com/pub/bradford-updates/STABLE/$releasever/updates/$basearch/
```

5. **Versions 8.8.0 and above: networkradius.repo** must also be modified. This is used for downloading the centOS files for the Local RADIUS Server feature. The baseurl entry must be modified regardless if the feature is being used. Otherwise, the centOS update will not complete.

   `/etc/yum.repos.d/networkradius.repo`

6. Change both instances of the baseurl in this file to reflect the same protocol and address as bradford.repo. For example:

   From:

   ```
   baseurl=ftp://fnac-updates.fortinet.net
   ```

   To:

   ```
   baseurl=http://downloads.bradfordnetworks.com
   ```

7. Save the changes and exit the editor.

   Note: The networkradius.repo file is not overwritten during upgrades, so changes will be permanent.

8. Verify changes:

```
> grep -i baseurl /etc/yum.repos.d/networkradius.repo
baseurl=http://downloads.bradfordnetworks.com/pub/networkradius/BETA/$releasever/updates/$basearch/
baseurl=http://downloads.bradfordnetworks.com/pub/networkradius/STABLE/$releasever/updates/$basearch/
```

Update Using a Proxy Server

The following steps must be performed on all appliances.

1. Using vi or another text editor, modify the yum.conf file
   `/etc/yum.conf`

2. Add lines:
   `proxy=http://<Proxy Server FQDN or IP>:<Proxy Port>`

3. If user name and password is required for proxy, add the following:
   `proxy_username=<username>`
   `proxy_password=<password>`

4. Save changes and exit the editor.

Update Procedure for Sites without External Access

1. Obtain RPMs found on
   http://downloads.bradfordnetworks.com/pub/centos-repos/STABLE/7/updates/x86_64/
   If downloading to a Linux platform type:

   ```
   wget -r -l1 --no-parent -A.rpm downloads.bradfordnetworks.com/pub/centos-repos/STABLE/7/updates/x86_64/
   ```

2. Copy all the RPMs to an accessible media form (FTP, Web server, etc) or local directory on the FortiNAC server.

3. On each FortiNAC server, edit the following files and change the baseurl to point to the area created in step 2, specifying the applicable protocol.

   Versions 8.7 and lower:
   `/etc/yum.repos.d/bradford.repo`

   Version 8.8.0 and higher:
   `/etc/yum.repos.d/bradford.repo`
   `/etc/yum.repos.d/networkradius.repo`

   Example
   From:

   ```
   baseurl=ftp://downloads.bradfordnetworks.com/pub/bradford-updates/STABLE/$releasever/updates/$basearch/
   ```

   To one of the following:

   FTP or HTTP to local server

   ```
   baseurl=ftp://yourupdateserver/pub/bradford-updates/
   ```

   ```
   baseurl=http://yourupdateserver/pub/Fortinet-updates/
   ```

   HTTP is allowed but not FTP to downloads.bradfordnetworks.com

   ```
   baseurl=http://downloads.bradfordnetworks.com/pub/bradford-updates/STABLE/$releasever/updates/$basearch/
   ```

   Local directory on the FortiNAC server

   ```
   baseurl=file:///yourupdate_local_directory
   ```

4. Run the update on each FortiNAC server. Type

   ```
   yum -y update
   ```

5. Once updates are applied, gracefully shut down FortiNAC services and reboot using the UI or CLI.