# FortiNAC

## CentOS Update CLI Instructions

Firmware: 6.x

(CentOS 7)

Date:

12/17/2018

Rev: D

## 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

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

## FORTINET COOKBOOK
http://cookbook.fortinet.com

## FORTINET TRAINING AND CERTIFICATION PROGRAM
http://www.fortinet.com/support-and-trainingt/training.html

## 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

Monday, December 17, 2018

# Contents


Overview ..... 4
Introduction ..... 4
Fortinet Update Policy ..... 4
Update Process ..... 5
General Requirements ..... 5
Notes ..... 6
Procedure ..... 6
Preparation ..... 6
Initiate the Update Process ..... 6
Reboot Servers ..... 7
Control Manager (NCM) or a Single Control Application Server ..... 7
Analytics Server ..... 7
Control Server and Application Server Pair (Non-HA Configuration) ..... 7
Control and Application Server Pair (HA Configuration) ..... 8
Validate ..... 9
Troubleshooting Tips ..... 9
Appendix ..... 10
Enable CentOS Update ..... 10
Change Transfer Protocol to HTTP/HTTPS ..... 11
Update Using a Proxy Server ..... 12
Update Procedure for Sites without External Access ..... 12

# 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/

## 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 error 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. 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.
- FTP access to **downloads.bradfordnetworks.com** from each appliance or virtual machine.
  **Note:** If this is not feasible, there is a workaround to use HTTP or HTTPS in CLI.
- 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:
  SYS-BFN330-XXXX
  SYS-BFN630-XXXX
  SYS-BFN630XL-XXXX
  SYS-G-BFN630-XXXX
  SYC-FNT440-XXX
  SYC-FNT440XL-XXX
  SYC-FNT330-000
- Root access to each appliance or virtual machine.

## Notes

- 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 Administration UI. For instructions, refer to the **Operating System Updates** topic in the Online Help or the Administration and Operation guide in the Document Library.
- OS Updates replace all prior OS Updates and do not require that prior updates be installed first.
- If experiencing any issues with the Operating System, it is required to install the most recent release of OS Updates before the problem can be troubleshot.
- 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.

# CLI Procedure

## Preparation

1. If updating virtual machines, take a snapshot of the VM before performing the update.

2. Open an SSH session to the first appliance or virtual machine to be updated using PuTTy or some other SSH tool.

3. Log in as **root**.

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

   **Important:** Do not install the updates if the firmware version is not correct or the Linux Distribution is not CentOS.

## Initiate the Update Process

The following steps must be done on all appliances.

1. To 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

2. When the update process is complete, shut down the FortiNAC process and reboot the appliance or virtual machine.

To stop any updates already 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
```

## Reboot Servers

**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.

### Control Manager (NCM) or a Single Control Application Server

1. On the server, run
   ```
   shutdowncampusMgr
   ```
2. Wait 30 seconds and run
   ```
   shutdowncampusMgr –kill
   ```
3. On the server, run
   ```
   reboot
   ```
4. If the NCM or Control Application Servers are in a HA configuration, on the Secondary server, run
   ```
   shutdowncampusMgr -kill
   reboot
   ```

### Analytics Server

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

### 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.

## 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 (by confirming you have ssh access 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.

## 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. For example, verify that the bash update is installed by typing the following command at the prompt:

   ```
   rpm -qa | grep -i bash
   ```

# Troubleshooting Tips

**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**.

# Appendix

## 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** respository 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.

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

## Change Transfer Protocol to HTTP/HTTPS

The default protocol in the bradford.repo file is FTP. 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.

## 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://<server FQDN or IP>:3128`

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 **/etc/yum.repos.d/bradford.repo** and change the baseurl to point to the area created in step 2, specifying the applicable protocol.

   **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.