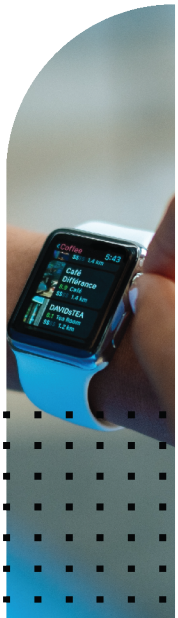
Offline Upgrade Guide

FortiSIEM 6.4.1



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

05/23/2022
FortiSIEM 6.4.1 Offline Upgrade Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-09-24	Initial version of FortiSIEM - Offline Upgrade Guide.
2018-10-08	Revision 1: modifications to the Section: 'Upgrading FortiSIEM' - Step 1.
2019-08-19	Revision 2: Updated the location of the image download site.
2021-03-30	Revision 3: Released for 6.2.0.
2021-04-06	Revision 4: Updated "6.1.x to 6.2.0 Upgrade" and "Syncing the Local Repository Mirror".
2021-05-07	Revision 5: Released for 6.2.1.
2021-06-22	Revision 6: Disk size for deployment updated.
2021-07-06	Revision 7: Released for 6.3.0.
2021-07-21	Revision 8: Added "Upgrading Multiple Collector Nodes in an Online and/or Offline Environment".
2021-08-26	Revision 9: Released for 6.3.1.
2021-10-15	Revision 10: Released for 6.3.2.
2021-12-22	Revision 11: Released for 6.3.3.
2022-01-18	Revision 12: Released for 6.4.0.
2022-01-27	Revision 13: Supervisor/Worker Upgrade section updated for 6.4.0 release.
2022-03-09	Revision 14: Supervisor/Worker Upgrade section updated for 6.4.0 release.
2022-05-23	Revision 15: Released for 6.4.1.

Offline Install and Upgrade

This document describes the steps needed to install and upgrade FortiSIEM in a closed environment without internet access. In some cases, FortiSIEM communicates with a repository to download the latest updates. This can be eliminated by setting up a local repository.

Fresh Installation

There are two options for fresh installation, FIPS disabled, or FIPS enabled.

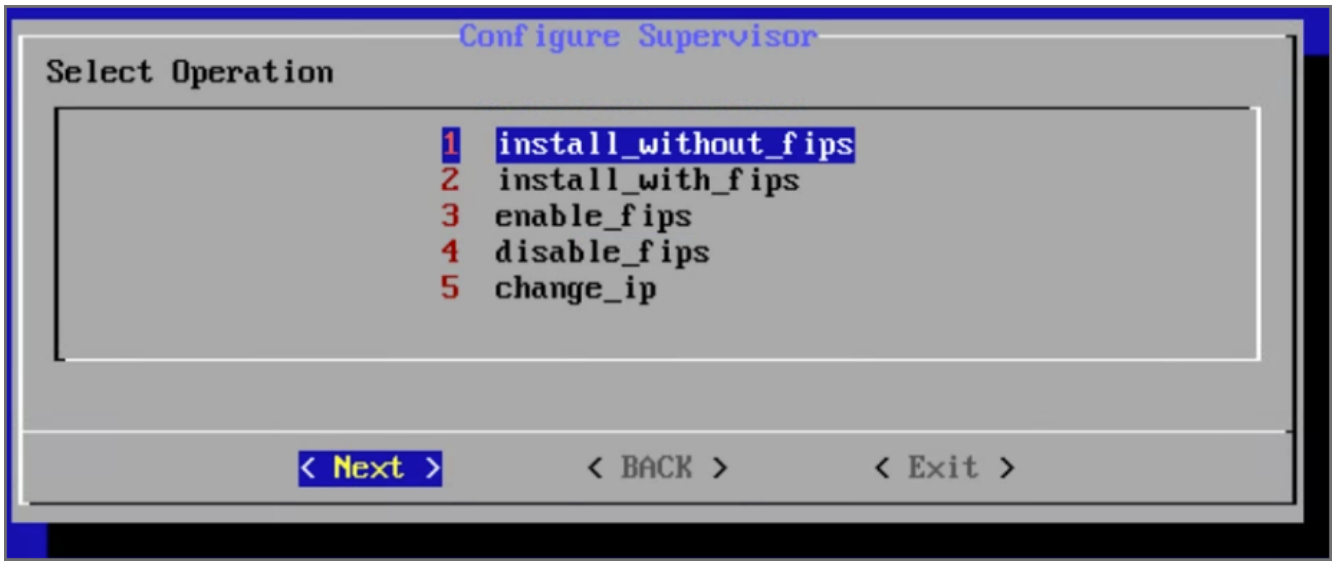
- FIPS Disabled Installation
- FIPS Enabled Installation

FIPS Disabled Installation

With FIPS disabled, a fresh installation does not require internet access and can be performed in a closed environment. Run the following command:

```
# configFSM.sh
```

and select **1 install_without_fips**.



FIPS Enabled Installation

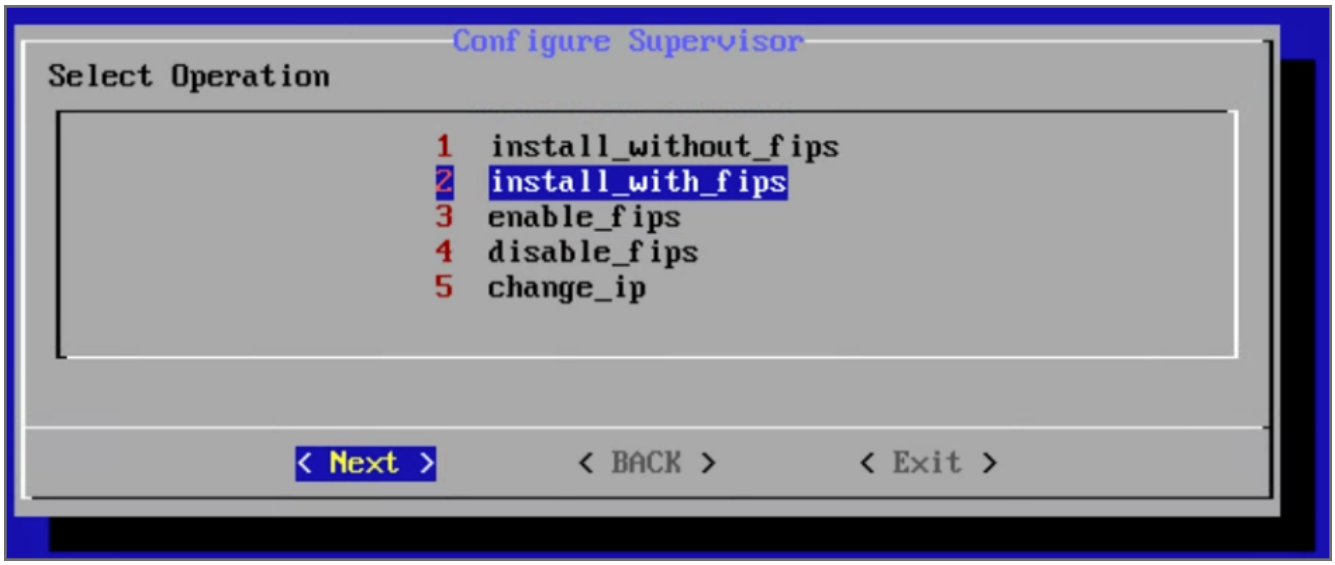
A FIPS enabled fresh installation requires internet access to Fortinet's RockyLinux repository. This can be re-routed to an offline repository by taking the following steps.

Note: For hardware appliance users, make sure to skip step 2.

1. Complete the Local RockyLinux Repository Mirror Installation.
2. Deploy your FortiSIEM VA onto your hypervisor.
3. Log into the FortiSIEM local console through your hypervisor.
   Default login:
   User = `root`
   Password = `ProspectHills`
4. Immediately change the `root` password.
5. Modify the Yum Repository Files to use the local repository by running the following commands.

```
# cd /etc/yum.repos.d
# sed -i 's/baseurl=https\:\/\/os-pkgs-
cdn.fortisiem.fortinet.com\/rockylinux8/baseurl=https\:\/\/<REPOSITORY MIRROR
IP>\/repos\/rockylinux8/g' *.repo
# sed -i 's/https\:\/\/os-pkgs-r8.fortisiem.fortinet.com.*//g' *.repo
# sed -i 's/enabled=1/enabled=1\nsslverify=false/g' *.repo
# dnf clean all
```

6. Use the appropriate Installation Guide from 6.4 Installation Guides to continue.
   You will need to run the following command, and then select **2 install_with_fips**.
   `# configFSM.sh`



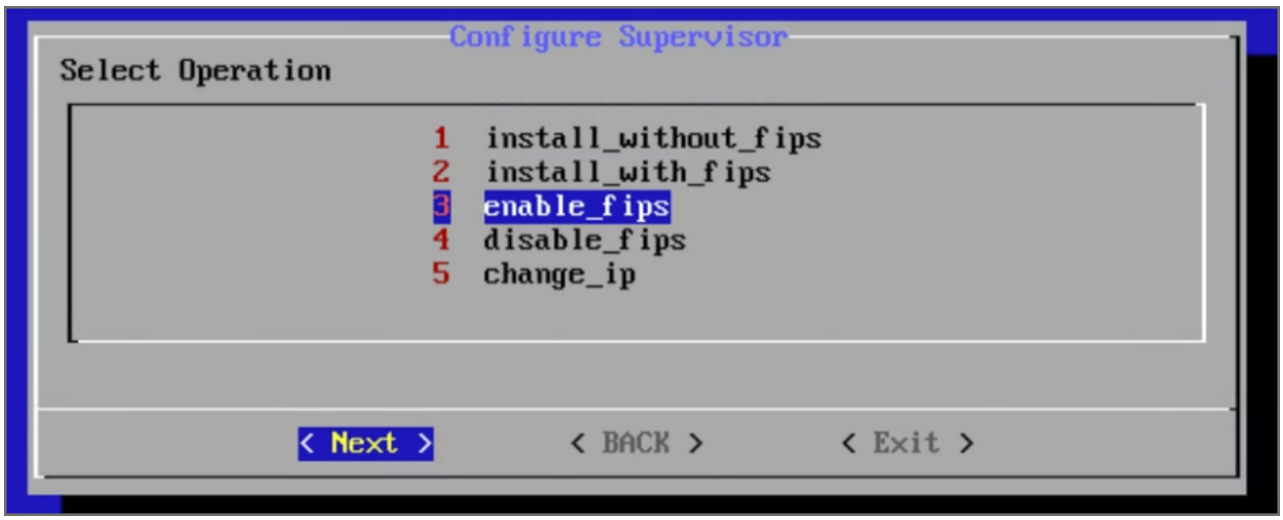
5.3.x or 5.4.0 to 6.1.x Migration

FortiSIEM Migration does not require internet access and can be performed in a closed environment. However, if you want to enable FIPS after migrating to 6.1.x, then internet access is required. Follow the steps below to enable FIPS without requiring Internet access.

Enabling FIPS After Migration

Take the following steps to enable FIPS after migration.

1. Complete the 6.1.x Upgrade and below Local CentOS Repository Mirror Installation.
2. Log into FortiSIEM via SSH.
   ```
   # ssh root@<FortISIEM Super/Worker/Collector>
   ```
3. Modify the Yum Repository Files to use the Local Repository by running the following commands.
   ```
   # cd /etc/yum.repos.d
   # sed -i 's/baseurl=https\:\/\/os-pkgs-cdn.fortisiem.fortinet.com\/centos8/baseurl=https\:\/\/<REPOSITORY MIRROR IP>\/repos\/centos\/84/g' *.repo
   # sed -i 's/https\:\/\/os-pkgs-c8.fortisiem.fortinet.com.*//g' *.repo
   # sed -i 's/enabled=1/enabled=1\nsslverify=false/g' *.repo
   # dnf clean all
   ```
4. Run the following command and select **3 enable_fips**.
   ```
   # configFSM.sh
   ```



6.4.1 Upgrade

The 6.4.1 upgrade is comprised of two parts, the supervisor/worker upgrade and collector upgrade.

Supervisor/Worker Upgrade

Take the following steps to prepare an offline upgrade from 6..x to 6.4.1 for your supervisor and worker(s).

1. Upload the `FSM_Upgrade_All_6.4.1_build1415.zip` onto the 6.x Supervisor/Worker under the `/tmp/` folder.
2. Log in and unzip the upgrade package by running the following commands.

```
# ssh root@<Super/Worker>
# mkdir -p /opt/upgrade/
# mv /tmp/FSM_Upgrade_All_6.4.1_build1415.zip /opt/upgrade/
# unzip FSM_Upgrade_All_6.4.1_build1415.zip
```

3. Update the migration script migrate_centos_to_rocky.sh:

```
# cd /opt/upgrade/FSM_Upgrade_All_6.4.1_build1415/install/files/

# sed -i 's/https\:\/\/os-pkgs-
r8.fortisiem.fortinet.com\/rockylinux8/https\:\/\/<REPOSITORY MIRROR
IP>\/repos\/rockylinux8/g' migrate_centos_to_rocky.sh

# sed -i 's/https\:\/\/os-pkgs-
cdn.fortisiem.fortinet.com\/rockylinux8/https\:\/\/<REPOSITORY MIRROR
IP>\/repos\/rockylinux8/g' migrate_centos_to_rocky.sh

# sed -i 's/curl \-o \/etc\/pki\/rpm\-gpg\/RPM\-GPG\-KEY\-PGDG /curl \-k \-o
\/etc\/pki\/rpm\-gpg\/RPM\-GPG\-KEY\-PGDG /g' migrate_centos_to_rocky.sh

# sed -i 's/curl \-o \/etc\/pki\/rpm\-gpg\/RPM\-GPG\-KEY\-rockyofficial /curl \-k \-o
\/etc\/pki\/rpm\-gpg\/RPM\-GPG\-KEY\-rockyofficial /g' migrate_centos_to_rocky.sh

# sed -i 's/curl \-o /curl \-k \-o /g' migrate_centos_to_rocky.sh
```

4. Modify the necessary repository files by running the following set of commands.

Update the Repos Files

```
# cd /opt/upgrade/FSM_Upgrade_All_6.4.1_build1415/install/files/repos/
# sed -i 's/baseurl=https\:\/\/os-pkgs-
cdn.fortisiem.fortinet.com\/rockylinux8/baseurl=https\:\/\/<REPOSITORY MIRROR
IP>\/repos\/rockylinux8/g' *.repo
# sed -i 's/https\:\/\/os-pkgs-r8.fortisiem.fortinet.com.*//g' *.repo
# sed -i 's/enabled=1/enabled=1\nsslverify=false/g' *.repo
```

Update PSQL DB Repo

```
# cd /opt/upgrade/FSM_Upgrade_All_6.4.1_build1415/install/roles/upgrade-db-server/files
# sed -i 's/baseurl=https\:\/\/os-pkgs-cdn.fortisiem.fortinet.com\/rockylinux8/baseurl=https\:\/\/<REPOSITORY MIRROR IP>\/repos\/rockylinux8/g' *.repo
# sed -i 's/https\:\/\/os-pkgs-r8.fortisiem.fortinet.com.*//g' *.repo
# sed -i 's/enabled=1/enabled=1\nsslverify=false/g' *.repo
```

Update Files that Pick Up the GPG Key for PSQL

```
# cd /opt/upgrade/FSM_Upgrade_All_6.4.1_build1415/install/roles/upgrade/tasks/
# sed -i 's/https\:\/\/os-pkgs-cdn.fortisiem.fortinet.com\/rockylinux8/https\:\/\/<REPOSITORY MIRROR IP>\/repos\/rockylinux8/g' main.yml
# sed -i 's/curl \-o /curl \-k \-o /g' main.yml
# cd /opt/upgrade/FSM_Upgrade_All_6.4.1_build1415/install/roles/upgrade-db-server/tasks/
# sed -i 's/https\:\/\/os-pkgs-cdn.fortisiem.fortinet.com\/rockylinux8/https\:\/\/<REPOSITORY MIRROR IP>\/repos\/rockylinux8/g' main.yml
# sed -i 's/curl \-o /curl \-k \-o /g' main.yml
```

Perform Clean Up

```
# dnf clean all
```

Prepare yum.conf to Ignore SSL Verification

```
# echo sslverify=false >> /etc/yum.conf
```

5. Use the Upgrade Guide located in 6.4 Reference Manuals to continue with your upgrade for the supervisor and worker(s).

Collector Upgrade

For FortiSIEM version 6.4.0, the collector offline upgrade is unsupported at this time. Please reference Known Issues in the 6.4.0 Release Notes.

Configuring Existing FSM on RockyLinux Install to use Local Repository Mirror

Sometimes you may want to run a "yum update" on an existing FortiSIEM installation to get the latest patches. Follow these steps to avoid internet access during this step.

Note: This configuration is needed to run Yum updates without needing to go to the internet.

1. Log into all FortiSIEM Supervisor/Worker(s)/Collector(s) that will pull from the new repository by running the following commands.

   ```
   # ssh root@<Super/Worker/Collector IP>
   # cd /etc/yum.repos.d
   ```

2. Modify necessary repository files by running the following commands.

   ```
   # sed -i 's/baseurl=https\:\/\/os-pkgs-
   cdn.fortisiem.fortinet.com\rockylinux8/baseurl=https\:\/\/<REPOSITORY MIRROR
   IP>\/repos\/rockylinux8/g' *.repo
   # sed -i 's/https\:\/\/os-pkgs-r8.fortisiem.fortinet.com.*//g' *.repo
   # sed -i 's/enabled=1/enabled=1\nsslverify=false/g' *.repo
   # dnf clean all
   ```

3. Connect and update from the local repository mirror by running the following the following command.

   ```
   # dnf update -y / # yum update -y
   Rocky Linux 8 - AppStream
                               90 MB/s | 9.5 MB     00:00
   Rocky Linux 8 - BaseOS
                              103 MB/s | 8.6 MB     00:00
   Rocky Linux 8 - Extras
                              289 kB/s |  12 kB     00:00
   Rocky Linux 8 - PowerTools
                               42 MB/s | 2.3 MB     00:00
   ELRepo.org Community Enterprise Linux Repository - el8
                              8.9 MB/s | 293 kB     00:00
   Extra Packages for Enterprise Linux 8 - x86_64
                               17 MB/s | 955 kB     00:00
   Extra Packages for Enterprise Linux 8 - x86_64
                               97 MB/s |  11 MB     00:00
   PostgreSQL common RPMs for RHEL/CentOS 8 - x86_64
                               17 MB/s | 545 kB     00:00
   PostgreSQL 13 for RHEL/CentOS 8 - x86_64
   ```

```
                            12 MB/s | 440 kB     00:00
Dependencies resolved.
Nothing to do.
Complete!
```

Local RockyLinux 8 Repository Mirror Installation

Follow these steps to setup a local RockyLinux repository mirror in your internal network. FortiSIEM will only communicate with this local RockyLinux repository mirror whenever needed, thereby avoiding internet access.

You will be going through these general steps:

1. Deploying the base VM to state and setup access to the repository
2. Replicating the remote repository into your new internal mirror
3. Testing the internal mirror for accessibility
4. A walk through for all the FSM nodes in order to reach the internal mirror

Instructions are broken down into the following sections.

Repository Mirror Deployment and Apache Staging

This server is required to have internet access and be able to resolve [`os-pkgs-cdn.fortisiem.fortinet.com`] or [`os-pkgs-r8.fortisiem.fortinet.com`] in order to prepare the repository mirror. Once the Repository Mirror is completed, the internet connection can then be cut off from this repository mirror until the next time the mirror needs to be updated.

When the above conditions are met, take the following steps:

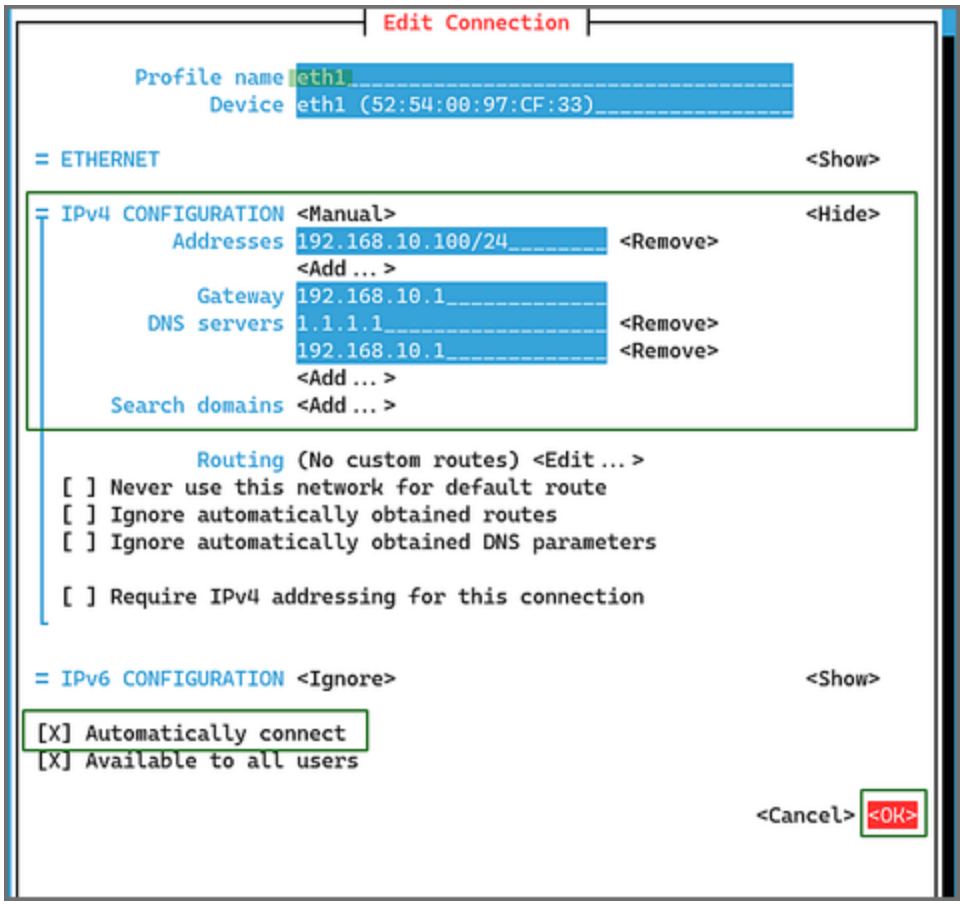
1. Download the 6.4.1.1415 FortiSIEM image and create a VM on your preferred hypervisor.
2. Add an 100GB disk to the FortiSIEM image that was deployed by taking the following steps:
   Note: Instructions to add a disk is based off of vSphere 6.7. Your hypervisor may differ in instructions, but the concept is the same.
   a. Right click the **FortiSIEM VM > Editing Settings**.
   b. In the pop-up, click "Add New Device".
   c. Find "Hard Disk" and select it.
   d. Configure it for 100GB.
   e. Click "OK" to save the configuration.
   f. Boot the FortiSIEM image.

Configuring the Network Adapter

To complete the configuration, take the following steps:

1. Log into the FortiSIEM console through your hypervisor.
   Default login:
   User = root
   Password = `ProspectHills`
2. Immediately change the root password.
3. Enter the IP address configuration utility by running the following command:
   `# nmtui-edit eth0`
4. Go to **IPv4 CONFIGURATION**, toggle **Automatic**, and select **Manual** from the menu.
5. Toggle **Show** to expand the configuraion.
6. In the **Addresses** field, add an IP address/netmask (CIDR).
   Example: `192.168.1.1/24`
   Note: Use the tool at this URL to convert netmask to CIDR.
   https://www.xarg.org/tools/subnet-calculator/
7. In the **Gateway** field, enter the Gateway IP address.
   Example: `192.168.1.254`
8. In the **DNS Servers** field, toggle Add, and select IP of DNS.
   Example: 1.1.1.1
9. In the **DNS Servers** field, Toggle Add, and add the IP of the second DNS.
   Example: 1.0.0.1
10. Toggle the **Automatically connect setting** to enable.
11. Toggle the **Available to all users setting** to enable.

12. Toggle to **OK**.



13. Restart the network adapter.
    ```
    # ifdown eth0
    # ifup eth0
    ```
14. Check if the IP address is assigned to the network adapter.
    ```
    # ifconfig eth0
    ```
    The IP address will be assigned to eth0.
15. Ping an external address to verify network connectivity.
    ```
    # ping <ip address>
    ```
    or
    ```
    # ping google.com
    ```

Installing the Yum-Utils Package

Take the following steps to install the yum-utils package.

1. Clean the current respository from the VM.
   ```
   # dnf clean all
   ```
2. Install the yum-utils package.
   ```
   # dnf install yum-utils -y
   ```

Preparing the Disk for the Local Repository Mirror

Take the following steps to prepare your disk for the local repository mirror.

1. Look for the 100GB disk created when the ova was deployed.

```
# lsblk
NAME         MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda            8:0    0   25G  0 disk
├─sda1         8:1    0    1G  0 part /boot
└─sda2         8:2    0   24G  0 part
├─cl-swap 253:0    0  2.5G  0 lvm  [SWAP]
└─cl-root 253:1    0 21.5G  0 lvm  /
sdb            8:16   0   100G  0 disk                    << New disk
```

2. Format the disk using xfs file system.

```
# mkfs.xfs /dev/sdb
```

3. Create a new mount point for the new disk.

```
# mkdir /repos
```

4. Mount the disk.

```
# mount -t xfs /dev/sdb /repos
# chmod 755 /repos
```

5. Edit `/etc/fstab` and add the mount entry permanently.

```
# vi /etc/fstab
/dev/sdb /repos                    xfs     defaults        0 0
```

6. Test `/etc/fstab` to verify configuration.

```
# mount -a
```

Configuring Apache to Publish the Local Repository Mirror

Take the following steps to configure Apache to publish the local repository mirror.

1. Create the link to the repository path.

```
# cd /var/www/html/
# ln -sf /repos repos
# ls -l /var/www/html/
result: lrwxrwxrwx. 1 root root 6 Mar 26 16:18 repos -> /repos
```

2. Restart Apache.

```
# systemctl restart httpd
```

Verifying Remote Connectivity to the Local Repository Mirror

Take the following step to verify remote connectivity with the repository mirror.

1. From the local network workstation's browser, go to: `https://<Repository Mirror IP Address>/`

Syncing the Local Repository Mirror

Take the following steps to sync the local repository mirror.

1. Sync the FSM Mirror to the repository mirror.

```
# mkdir -p /repos/rockylinux8/gpg-keys
# cd /repos/rockylinux8/gpg-keys
# wget https://os-pkgs-cdn.fortisiem.fortinet.com/rockylinux8/gpg-keys/RPM-GPG-KEY-EPEL-8
# wget https://os-pkgs-cdn.fortisiem.fortinet.com/rockylinux8/gpg-keys/RPM-GPG-KEY-PGDG
# wget https://os-pkgs-cdn.fortisiem.fortinet.com/rockylinux8/gpg-keys/RPM-GPG-KEY-elrepo.org
# wget https://os-pkgs-cdn.fortisiem.fortinet.com/rockylinux8/gpg-keys/RPM-GPG-KEY-rockyofficial
# wget https://os-pkgs-cdn.fortisiem.fortinet.com/rockylinux8/gpg-keys/RPM-GPG-KEY-rockytesting
# cd /repos/rockylinux8
```

Note: Reposync will take a larger period of time as it's replicating the entire mirror.

```
# reposync --download-meta --downloadcomps
# reposync --repoid=epel-testing
# reposync --repoid=plus
```

2. Verify repository mirror's folder paths.

```
# ls -la
total 80
drwxrwxr-x. 14 root root 196 Dec 10 12:22 .
drwxrwxr-x. 3 root root 46 Oct 28 03:44 ..
drwxrwxr-x. 4 root root 55 Dec 16 01:20 appstream
drwxrwxr-x. 4 root root 55 Dec 16 01:20 baseos
```

```
drwxrwxr-x. 4 root root 34 Dec 16 01:20 elrepo
drwxrwxr-x. 4 root root 55 Dec 16 01:20 epel
drwxrwxr-x. 4 root root 38 Dec 16 01:20 epel-modular
drwxr-xr-x. 4 root root 75 Dec 14 18:38 epel-testing
drwxrwxr-x. 4 root root 38 Dec 16 01:20 extras
drwxrwxr-x. 2 root root 151 Dec 13 13:11 gpg-keys
drwxrwxr-x. 3 root root 28672 Dec 16 01:20 pgdg13
drwxrwxr-x. 3 root root 32768 Dec 16 01:20 pgdg-common
drwxr-xr-x. 4 root root 56 Dec 14 18:38 plus
drwxrwxr-x. 4 root root 73 Dec 16 01:20 powertools
```

3. Modify Permissions and Restart Apache on the repository mirror.
   ```
   # chmod -R 755 /repos
   # systemctl restart httpd
   ```
4. Check repository mirror.
   Locally, run the following command:
   ```
   # curl -k https://localhost/repos/rockylinux8/
   ```
   Remotely:
   Open a browser, and go to: `https://<Repository Mirror IP>/repos/rockylinux8/`

www.fortinet.com