Install Unified Manager on Linux systems

Active IQ Unified Manager 9.13

NetApp
May 09, 2024

Table of Contents

Install Unified Manager on Linux systems 1
Introduction to Active IQ Unified Manager 1
Requirements for installing Unified Manager 2
Installing, upgrading, and removing Unified Manager software 10

Install Unified Manager on Linux systems

Introduction to Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) enables you to monitor and manage the health and performance of your ONTAP storage systems from a single interface. You can deploy Unified Manager on a Linux server, on a Windows server, or as a virtual appliance (vApp) on a VMware host.

After you have completed the installation and have added the clusters that you want to manage, Unified Manager provides a graphical interface that displays the capacity, availability, protection, and performance status of the monitored storage systems.

Related information

NetApp Interoperability Matrix Tool

What the Unified Manager server does

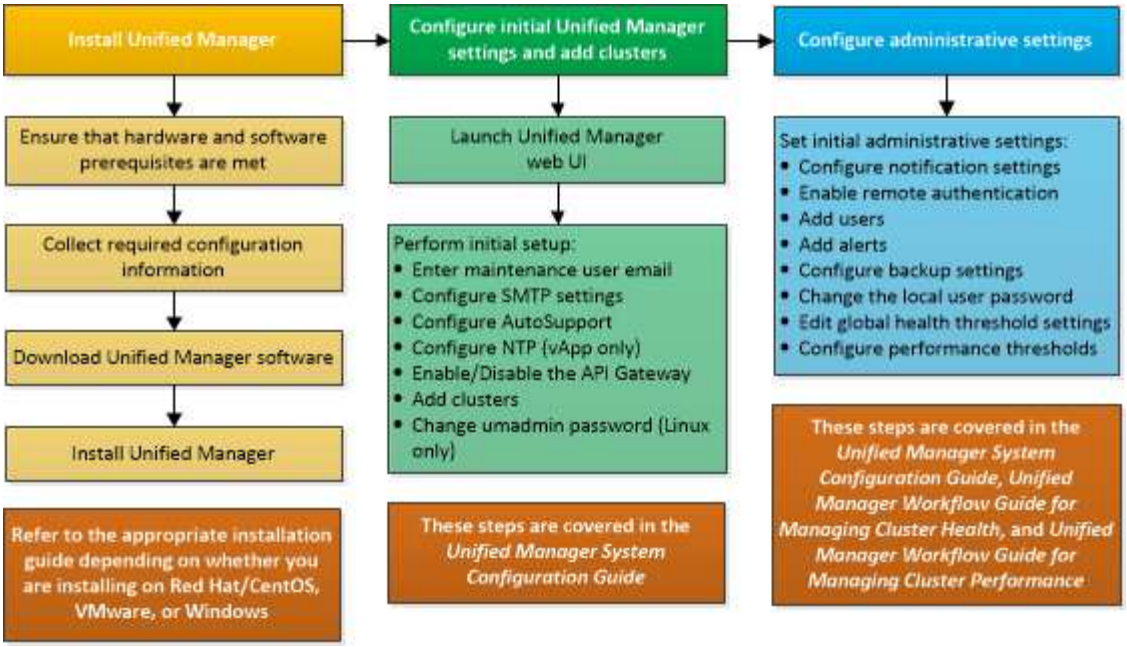
The Unified Manager server infrastructure consists of a data collection unit, a database, and an application server. It provides infrastructure services such as discovery, monitoring, role-based access control (RBAC), auditing, and logging.

Unified Manager collects cluster information, stores the data in the database, and analyzes the data to see if there are any cluster issues.

Overview of the installation sequence

The installation workflow describes the tasks that you must perform before you can use Unified Manager.

These sections describe each of the items shown in the workflow below.



Requirements for installing Unified Manager

Before you begin the installation process, ensure that the server on which you want to install Unified Manager meets the specific software, hardware, CPU, and memory requirements.

NetApp does not support any modification of the Unified Manager application code. If you need to apply any security measures to the Unified Manager server, you should make those changes to the operating system on which Unified Manager is installed.

For more details about applying security measures to the Unified Manager server, see the Knowledge Base article.

Supportability for Security Measures applied to Active IQ Unified Manager for Clustered Data ONTAP

Related information

NetApp Interoperability Matrix Tool

Virtual infrastructure and hardware system requirements

Installing Unified Manager on virtual infrastructure or a physical system should meet the minimum requirements for memory, CPU, and disk space.

The following table displays the values that are recommended for memory, CPU, and disk space resources. These values have been qualified so that Unified Manager meets acceptable performance levels.

Hardware configuration	Recommended settings
RAM	12 GB (minimum requirement 8 GB)
Processors	4 CPUs

Hardware configuration	Recommended settings
CPU cycle capacity	9572 MHz total (minimum requirement 9572 MHz)
Free disk space	150 GB, where the capacity is allocated as follows: • 50 GB allotted to the root partition • 100 GB of free disk space allotted to the `/opt/netapp/data` directory, which is mounted on an LVM drive or on a separate local disk attached to the target system For separately mounted `/opt` and `/var/log` directories, ensure that `/opt` has 15 GB and `/var/log` has 16 GB of free space. The `/tmp` directory should have at least 10 GB of free space.

Unified Manager can be installed on systems with a small amount of memory, but the recommended 12 GB of RAM ensures that enough memory is available for optimal performance, and so that the system can accommodate additional clusters and storage objects as your configuration grows. You should not set any memory limits on the VM where Unified Manager is deployed, and should not enable any features (for example, ballooning) that hinder the software from utilizing the allocated memory on the system.

Additionally, there is a limit to the number of nodes that a single instance of Unified Manager can monitor before you install a second instance of Unified Manager. For more information, see the *Best Practices Guide*.

Technical Report 4621: Unified Manager Best Practices Guide

Memory-page swapping negatively impacts the performance of the system and the management application. Competing for CPU resources that are unavailable because of overall host utilization can degrade performance.

Requirement for dedicated use

The physical or virtual system on which you install Unified Manager should be used exclusively for Unified Manager and should not be shared with other applications. Other applications might consume system resources and can drastically reduce the performance of Unified Manager.

Space requirements for backups

If you plan to use the Unified Manager backup and restore feature, allocate additional capacity so that the “data” directory or disk has 150 GB of space. A backup can be written to a local destination or to a remote destination. The best practice is to identify a remote location that is external to the Unified Manager host system that has a minimum of 150 GB of space.

Requirements for host connectivity

The physical system or virtual system on which you install Unified Manager should be configured in such a way that you can successfully `ping` the host name from the host itself. In case of IPv6 configuration, you should verify that `ping6` to the host name is successful to ensure that the Unified Manager installation succeeds.

You can use the host name (or the host IP address) to access the product web UI. If you configured a static IP address for your network during deployment, then you designated a name for the network host. If you configured the network using DHCP, you should obtain the host name from the DNS.

If you plan to allow users to access Unified Manager by using the short name instead of using the fully qualified domain name (FQDN) or IP address, then your network configuration has to resolve this short name to a valid FQDN.

Linux software and installation requirements

The Linux system on which you install Unified Manager requires specific versions of the operating system and supporting software.

Operating system software

The Linux system must have the following versions of the operating system and supporting software installed:

- Red Hat Enterprise Linux versions 7.x and from 8.0 to 8.7, based on x86_64 architecture.
- CentOS version 7.x based on x86_64 architecture. CentOS Stream is not supported.

See the Interoperability Matrix for the complete and most current list of supported Red Hat Enterprise Linux and CentOS versions.

mysupport.netapp.com/matrix

Third-party software

Unified Manager is deployed on a WildFly web server. WildFly 26.1.3 is bundled and configured with Unified Manager.

The following third-party packages are required, but not included with Unified Manager. These packages are automatically installed by the `yum` installer during installation, provided you have configured the repositories as mentioned in the following sections.

- MySQL Community Edition version 8.0.32 (from the MySQL repository).
- OpenJDK version 11.0.18 (from the Red Hat Extra Enterprise Linux Server repository)
- Python 3.6.x
- p7zip version 16.02 or later (from the Red Hat Extra Packages for Enterprise Linux repository)

> You must shut down a running instance of Unified Manager before upgrading any third-party software. After the third-party software installation is complete, you can restart Unified Manager.

User authorization requirements

Installation of Unified Manager on a Linux system can be performed by the root user or by non-root users by using the `sudo` command.

Installation requirements

The best practices for installing Red Hat Enterprise Linux or CentOS and the associated repositories on your system are listed below. Systems installed or configured differently, or deployed off premise (in the cloud),

might require additional steps, and Unified Manager might not run properly in such deployments.

- You must install Red Hat Enterprise Linux or CentOS according to Red Hat best practices, and you should select the following default options, which requires selecting the “Server with GUI” base environment.
- While installing Unified Manager on Red Hat Enterprise Linux or CentOS, the system must have access to the appropriate repository so that the installation program can access and install all the required software dependencies.
- For the `yum` installer to find dependent software in the Red Hat Enterprise Linux repositories, you must have registered the system during the Red Hat Enterprise Linux installation or afterwards by using a valid Red Hat subscription.

  See the Red Hat documentation for information about the Red Hat Subscription Manager.

- You must enable the Extra Packages for Enterprise Linux (EPEL) repository to successfully install the required third-party utilities on your system.

  If the EPEL repository is not configured on your system, you must manually download and configure the repository.

  See Manually configuring the EPEL repository.

- If the correct version of MySQL is not installed, you must enable the MySQL repository to successfully install MySQL software on your system.

  If the MySQL repository is not configured on your system, you must manually download and configure the repository.

  See Manually configuring the MySQL repository.

If your system does not have internet access, and the repositories are not mirrored from an internet-connected system to the unconnected system, you should follow the installation instructions to determine the external software dependencies of your system. Then you can download the required software to the internet-connected system, and copy the `.rpm` files to the system on which you plan to install Unified Manager. To download the artifacts and packages, you must use the `yum install` command. You must ensure that the two systems are running the same operating system version and that the subscription license is for the appropriate Red Hat Enterprise Linux or CentOS version.

> You must not install the required third-party software from repositories other than the repositories that are listed here. Software installed from the Red Hat repositories is designed explicitly for Red Hat Enterprise Linux, and conforms to Red Hat best practices (directory layouts, permissions, and so on). Software from other locations might not follow these guidelines, which might cause the Unified Manager installation to fail, or might cause issues with future upgrades.

Port 443 requirement

Generic images of Red Hat Enterprise Linux and CentOS might block external access to port 443. Due to this restriction, you might be unable to connect to the Administrator web UI after installing Unified Manager. Running the following command allows access to port 443 for all external users and applications on a generic Red Hat Enterprise Linux or CentOS system.

```
# firewall-cmd --zone=public --add-port=443/tcp --permanent; firewall-cmd
--reload
```

You must install Red Hat Enterprise Linux and CentOS with the “Server with GUI” base environment. It provides the commands used by Unified Manager installation instructions. Other base environments might require you to install additional commands to validate or complete the installation. If the `firewall-cmd` is not available on your system, you must install it by running the following command:

```
# sudo yum install firewalld
```

Contact your IT department before running the commands to see if your security policies require a different procedure.

> THP (Transparent Huge Pages) should be disabled on CentOS and Red Hat systems. When enabled, in some cases it can cause Unified Manager to be shut down when certain processes consume too much memory and are terminated.

Supported browsers

To access the Unified Manager web UI, use a supported browser.

The Interoperability Matrix has the list of supported browser versions.

mysupport.netapp.com/matrix

For all browsers, disabling pop-up blockers ensures that software features are displayed properly.

If you plan to configure Unified Manager for SAML authentication, so that an identity provider (IdP) can authenticate users, you should check the list of browsers supported by the IdP as well.

Protocol and port requirements

The required ports and protocols enable communication between the Unified Manager server and the managed storage systems, servers, and other components.

Connections to the Unified Manager server

In typical installations you do not have to specify port numbers when connecting to the Unified Manager web UI, because default ports are always used. For example, because Unified Manager always attempts to run on its default port, you can enter `https://<host>` instead of `https://<host>:443`.

The Unified Manager server uses specific protocols to access the following interfaces:

Interface	Protocol	Port	Description
Unified Manager web UI	HTTP	80	Used to access the Unified Manager web UI; automatically redirects to the secure port 443.

Interface	Protocol	Port	Description
Unified Manager web UI and programs using APIs	HTTPS	443	Used to securely access the Unified Manager web UI or to make API calls; API calls can only be made using HTTPS.
Maintenance console	SSH/SFTP	22	Used to access the maintenance console and retrieve support bundles.
Linux command line	SSH/SFTP	22	Used to access the Red Hat Enterprise Linux or CentOS command line and retrieve support bundles.
MySQL database	MySQL	3306	Used to enable OnCommand Workflow Automation and OnCommand API Services access to Unified Manager.
Syslog	UDP	514	Used to access subscription-based EMS messages from ONTAP systems and to create events based on the messages.
REST	HTTPS	9443	Used to access realtime REST API-based EMS events from authenticated ONTAP systems.

The default port for MySQL, 3306, is restricted only to localhost while installing Unified Manager on Linux systems. This does not impact any upgrade scenario, where the previous configuration is maintained. This configuration can be modified, and the connection can be made available to other hosts by using the `Control access to MySQL port 3306` option on the maintenance console. For information, see Additional menu options. The ports used for HTTP and HTTPS communication (ports 80 and 443) can be changed using the Unified Manager maintenance console. For more information, see Maintenance console menus.

Connections from the Unified Manager server

You should configure your firewall to open ports that enable communication between the Unified Manager server and managed storage systems, servers, and other components. If a port is not open, communication fails.

Depending on your environment, you can choose to modify the ports and protocols used by the Unified Manager server to connect to specific destinations.

The Unified Manager server connects using the following protocols and ports to the managed storage systems, servers, and other components:

Destination	Protocol	Port	Description
Storage system	HTTPS	443/TCP	Used to monitor and manage storage systems.
Storage system	NDMP	10000/TCP	Used for certain Snapshot restore operations.
AutoSupport server	HTTPS	443	Used to send AutoSupport information. Requires the internet access to perform this function.
Authentication server	LDAP	389	Used to make authentication requests, and user and group lookup requests.
	LDAPS	636	Used for secure LDAP communication.
Mail server	SMTP	25	Used to send alert notification emails.
SNMP trap sender	SNMPv1 or SNMPv3	162/UDP	Used to send alert notification SNMP traps.
External data provider server	TCP	2003	Used to send performance data to an external data provider, such as Graphite.
NTP server	NTP	123/UDP	Used to synchronize the time on the Unified Manager server with an external NTP time server. (VMware systems only)

Completing the worksheet

Before you install and configure Unified Manager, you should have specific information about your environment readily available. You can record the information in the worksheet.

Unified Manager installation information

The details required to install Unified Manager.

System on which software is deployed	Your value
Host fully qualified domain name	
Host IP address	
Network mask	
Gateway IP address	
Primary DNS address	
Secondary DNS address	
Search domains	
Maintenance user name	
Maintenance user password	

Unified Manager configuration information

The details to configure Unified Manager after installation. Some values are optional depending on your configuration.

Setting	Your value
Maintenance user email address	
SMTP server host name or IP address	
SMTP user name	
SMTP password	
SMTP port	25 (Default value)
Email from which alert notifications are sent	
Authentication server host name or IP address	
Active Directory administrator name or LDAP bind distinguished name	

Setting	Your value
Active Directory password or LDAP bind password	
Authentication server base distinguished name	
Identity provider (IdP) URL	
Identity provider (IdP) metadata	
SNMP trap destination host IP addresses	
SNMP port	

Cluster information

The details for the storage systems that you manage using Unified Manager.

Cluster 1 of N	Your value
Host name or cluster-management IP address	
ONTAP administrator user name The administrator must have been assigned the “admin” role.	
ONTAP administrator password	
Protocol	HTTPS

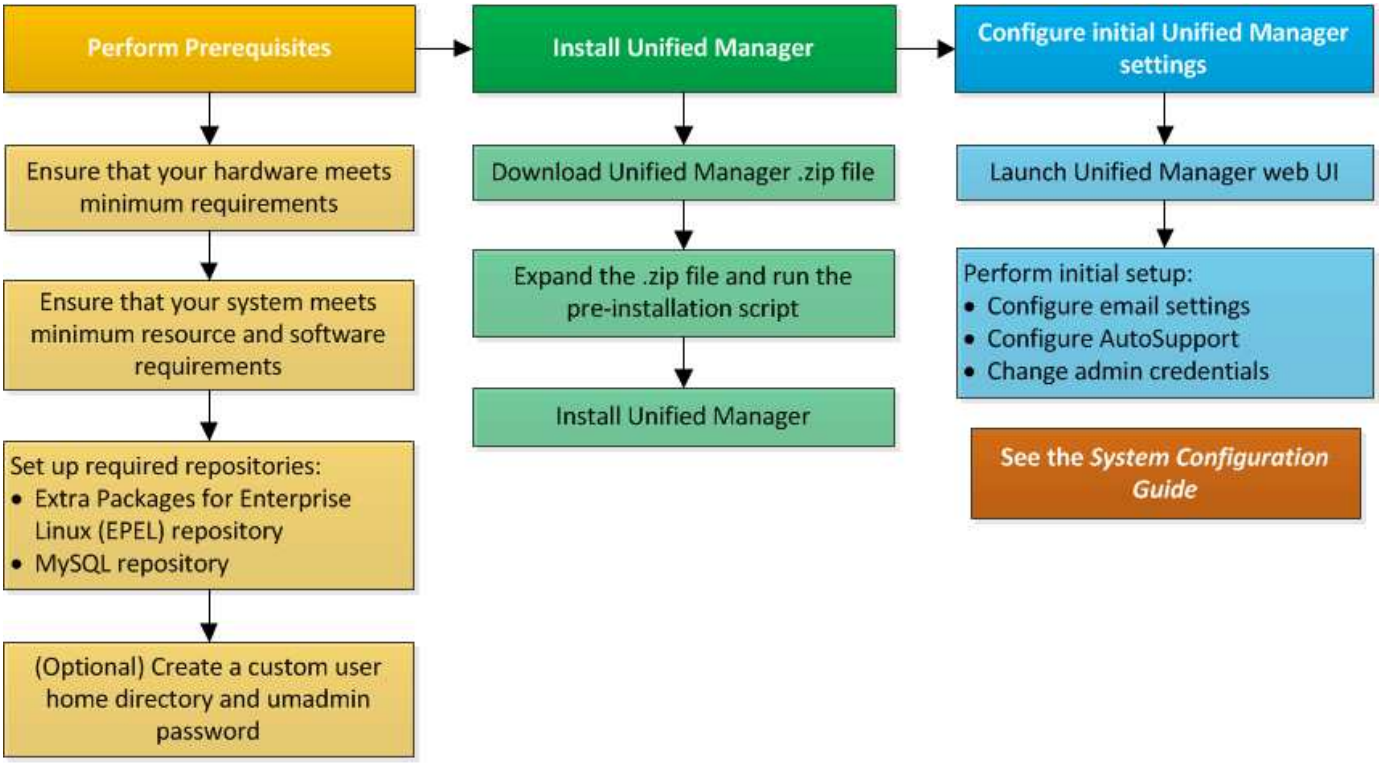
Installing, upgrading, and removing Unified Manager software

On Linux systems, you can install Unified Manager software, upgrade to a newer version of software, or remove Unified Manager.

Unified Manager can be installed on Red Hat Enterprise Linux or CentOS servers. The Linux server on which you install Unified Manager can be running either on a physical machine or on a virtual machine running on VMware ESXi, Microsoft Hyper-V, or Citrix XenServer.

Overview of the installation process

The installation workflow describes the tasks that you must perform before you can use Unified Manager.



Setting up required software repositories

The system must have access to certain repositories so that the installation program can access and install all required software dependencies.

Manually configuring the EPEL repository

If the system on which you are installing Unified Manager does not have access to the Extra Packages for Enterprise Linux (EPEL) repository, then you must manually download and configure the repository for a successful installation.

The EPEL repository provides access to the required third-party utilities that must be installed on your system. You use the EPEL repository whether you are installing Unified Manager on a Red Hat Enterprise Linux or CentOS system.

Steps

1. Download the EPEL repository for your installation. For Red Hat Enterprise Linux 7, download it from:

   ```
   wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
   ```

   For version 8, download it from:

   ```
   wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

2. Configure the EPEL repository:

   ```
   yum install epel-release-latest-<version>.noarch.rpm
   ```

For Red Hat Enterprise Linux 8 systems, if you have internal repositories with modular RPM packages, for

example, *javapackages-filesystem-<version>.module.rpm*, ensure that the metadata for the modular packages is also available in the same repository.

Manually configuring the MySQL repository

If the system on which you are installing Unified Manager does not have access to the MySQL Community Edition repository, then you must manually download and configure the repository for a successful installation.

The MySQL repository provides access to the required MySQL software that must be installed on your system.

> This task might fail if the system does not have the internet connectivity. Refer to the MySQL documentation if the system on which you are installing Unified Manager does not have the internet access.

Steps

1. Download the appropriate MySQL repository for your installation. For Red Hat Enterprise Linux 7, download it from:

   ```
   wget http://repo.mysql.com/yum/mysql-8.0-community/el/7/x86_64/mysql80-community-release-el7-3.noarch.rpm
   ```

   For version 8, download it from:

   ```
   wget http://repo.mysql.com/yum/mysql-8.0-community/el/8/x86_64/mysql80-community-release-el8-1.noarch.rpm
   ```

2. Configure the MySQL repository:

   ```
   yum install mysql80-community-release-<version>.noarch.rpm
   ```

For Red Hat Enterprise Linux 8 system, if you have internal repositories with java-11-openjdk, p7zip, and other software packages provided by the AppStream repository, you must disable your AppStream repository and install MySQL Community Server. Run the following command:

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install  mysql-community-server
```

If you receive an error on missing key or key mismatch, and your installation fails, try these steps:

- On a connected system, import the updated MySQL key by running the following command:

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-<xxxx>

for example:

rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022
```

- On a system that does not have internet connectivity, update your MySQL repo file and disable `gpgcheck` by marking `gpgcheck=0`.

SELinux requirements on NFS and CIFS shares

If you are planning to mount `/opt/netapp` or `/opt/netapp/data` on an NAS or SAN device, and you have SELinux enabled, you need to be aware of a few considerations.

If you are planning to mount `/opt/netapp` or `/opt/netapp/data` from anywhere other than the root file system, and you have SELinux enabled in your environment, you should set the correct context for the mounted directories. For the applicable scenario in your environment, follow these steps for setting and confirming the correct SELinux context.

Configuring the SELinux context when `/opt/netapp/data` is mounted

If you have mounted `/opt/netapp/data` in your system and SELinux is set to `Enforcing`, ensure that the SELinux context type for `/opt/netapp/data` is set to `mysqld_db_t`, which is the default context element for the location of the database files.

1. Run this command to check the context:

   ```
   ls -dZ /opt/netapp/data
   ```

   A sample output:

   ```
   drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0
   /opt/netapp/data
   ```

   In this output, the context is `default_t`. You should change this context to `mysqld_db_t`.

2. Perform these steps to set the context based on how you have mounted `/opt/netapp/data`.
   a. Run the following commands to set the context to `mysqld_db_t`: `semanage fcontext -a -t mysqld_db_t "/opt/netapp/data" `restorecon -R -v /opt/netapp/data`
   b. If you have configured `/opt/netapp/data` in `/etc/fstab`, you should edit the `/etc/fstab` file. For the `/opt/netapp/data/` mount option, add the MySQL label as:

      ```
      context=system_u:object_r:mysqld_db_t:s0
      ```

   c. Unmount and remount `/opt/netapp/data/` for enabling the context.
   d. If you have a direct NFS mount, run the following command to set the context to `mysqld_db_t`:

      ```
      mount <nfsshare>:/<mountpoint> /opt/netapp/data -o
      context=system_u:object_r:mysqld_db_t:s0
      ```

3. Verify whether the context is set correctly:

```
ls -dZ /opt/netapp/data/
```

A sample output:

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/
```

Configuring the SELinux context when `/opt/netapp` is mounted, and `/opt/netapp/data/` is also mounted separately

In this scenario, at first, you should set the context for `/opt/netapp/data/` as described in the previous section. After setting the correct context for `/opt/netapp/data/`, ensure that the parent directory `/opt/netapp` does not have the SELinux context set to `file_t`.

Steps

1. Run this command to check the context:

   ```
   ls -dZ /opt/netapp
   ```

   A sample output:

   ```
   drwxr-xr-x. mysql root unconfined_u:object_r:file_t:s0 /opt/netapp
   ```

   In this output, the context is `file_t` should be changed. The following commands set the context to `usr_t`. You can set the context to any value other than `file_t` based on your security requirements.

2. Perform these steps to set the context, based on how you have mounted `/opt/netapp`.
   a. Run the following commands to set the context:

```
semanage fcontext -a -t usr_t "/opt/netapp"
restorecon -v /opt/netapp
```

   a. If you have configured `/opt/netapp` in `/etc/fstab`, you should edit the `/etc/fstab` file. For the `/opt/netapp` mount option, add the MySQL label as:

      ```
      context=system_u:object_r:usr_t:s0
      ```

   b. Unmount, and then again mount `/opt/netapp` for enabling the context.
   c. If you have a direct NFS mount, run the following command to set the context:

      ```
      mount <nfsshare>:/<mountpoint> /opt/netapp -o
      context=system_u:object_r:usr_t:s0
      ```

      1. Verify whether the context is set correctly:

         ```
         ls -dZ /opt/netapp
         ```

         A sample output

```
drwxr-xr-x. mysql root unconfined_u:object_r:usr_t:s0 /opt/netapp
```

Configuring the SELinux context when `/opt/netapp` is mounted, and `/opt/netapp/data/` is not mounted separately

If you have mounted `/opt/netapp` in your system and SELinux is set to `Enforcing`, ensure that the SELinux context type for `/opt/netapp` is set to `mysqld_db_t`, which is the default context element for the location of the database files.

Steps

1. Run this command to check the context:

   ```
   ls -dZ /opt/netapp
   ```

   A sample output:

   ```
   drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0 /opt/netapp
   ```

   In this output, the context is `default_t`. You should change this context to `mysqld_db_t`.

2. Perform the following steps to set the context based on how you have mounted `/opt/netapp`.
   a. Run the following commands to set the context to `mysqld_db_t`: `semanage fcontext -a -t mysqld_db_t "/opt/netapp" `restorecon -R -v /opt/netapp`
   b. If you have configured `/opt/netapp` in `/etc/fstab`, edit the `/etc/fstab` file. For the `/opt/netapp/` mount option, add the MySQL label as: `context=system_u:object_r:mysqld_db_t:s0`
   c. Unmount, and then again mount `/opt/netapp/` for enabling the context.
   d. If you have a direct NFS mount, run the following command to set the context to `mysqld_db_t`: `mount <nfsshare>:/<mountpoint> /opt/netapp -o context=system_u:object_r:mysqld_db_t:s0`
3. Verify whether the context is set correctly:

```
ls -dZ /opt/netapp/
```

A sample output:

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysqld_db_t:s0 /opt/netapp/
```

Installing Unified Manager on Linux systems

It is important that you understand that the sequence of steps to download and install Unified Manager varies according to your installation scenario.

Creating a custom user home directory and umadmin password prior to installation

You can create a custom home directory and define your own umadmin user password prior to installing Unified Manager. This task is optional, but some sites might need the flexibility to override Unified Manager installation default settings.

What you'll need

- The system must meet the requirements described in Hardware system requirements.
- You must be able to log in as the root user to the Red Hat Enterprise Linux or CentOS system.

The default Unified Manager installation performs the following tasks:

- Creates the umadmin user with `/home/umadmin` as the home directory.
- Assigns the default password "admin" to the umadmin user.

Because some installation environments restrict access to `/home`, the installation fails. You must create the home directory in a different location. Additionally, some sites might have rules about password complexity or require that passwords be set by local administrators rather than being set by the installing program.

If your installation environment requires that you override these installation default settings, follow these steps to create a custom home directory and to define the umadmin user's password.

When this information is defined prior to installation, the installation script discovers these settings and uses the defined values instead of using the installation default settings.

Additionally, the default Unified Manager installation includes the umadmin user in the sudoers files (`ocum_sudoers` and `ocie_sudoers`) in the `/etc/sudoers.d/` directory. If you remove this content from your environment because of security policies, or because of some security monitoring tool, you must add it back. You need to preserve the sudoers configuration because some Unified Manager operations require these sudo privileges.

The security policies in your environment must not restrict sudo privileges for the Unified Manager maintenance user. Some Unified Manager operations might fail if the privileges are restricted. Verify that you are able to run the following sudo command when logged in as the umadmin user after successful installation.

```
sudo systemctl status ocie
```

This command should return the appropriate status of the ocie service without any errors.

Steps

1. Log in as the root user to the server.
2. Create the umadmin group account called "maintenance":

   ```
   groupadd maintenance
   ```

3. Create the user account "umadmin" in the maintenance group under a home directory of your choice:

   ```
   adduser --home <home_directory\> -g maintenance umadmin
   ```

4. Define the umadmin password:

   ```
   passwd umadmin
   ```

The system prompts you to enter a new password string for the umadmin user.

After you have installed Unified Manager you must specify the umadmin user login shell.

Downloading Unified Manager

You must download the Unified Manager `.zip` file from the NetApp Support Site to install Unified Manager.

What you'll need

You must have login credentials for the NetApp Support Site.

You download the same Unified Manager installation package for both Red Hat Enterprise Linux and CentOS systems.

Steps

1. Log in to the NetApp Support Site, and navigate to the Download page for Unified Manager:

   NetApp Support Site

2. Select the required version of Unified Manager and accept the end-users license agreement (EULA).
3. Download the Unified Manager installer file for Linux, and save the `.zip` file to a directory on the target system.

   - Ensure that you download the correct version of the installer file for your Red Hat Enterprise Linux system. Based on whether you have Red Hat Enterprise Linux 7 or 8 installed, ensure that you download the appropriate version of the Unified Manager `.zip` file.
   - NetApp recommends that you download the code signing certificate (`.pem`) and digital signature (`.sig`) along with the `.zip` file.

4. Verify the checksum for integrity of the downloaded software.
5. If you have downloaded the code signing certificate and digital signature, you can verify the integrity of the installer file. You can use the following commands to verify the integrity of the installer file:
   - This command creates a file with the public key from the code signing certificate:

     ```
     openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem >
     <public_key_file_name>
     ```

     - Where **AIQUM-RHEL-CLIENT-INTER-ROOT.pem** is the file that contains the code signing certificate.
   - This command verifies the signature on the installer file:

     ```
     openssl dgst -sha256 -verify <public_key_file_name> -signature
     <signature_file_name> ActiveIQUnifiedManager-<version>.zip
     ```

The message similar to `Verified Ok` confirms that the installer file is safe to use.

Installing Unified Manager

You can install Unified Manager on a physical or virtual Red Hat Enterprise Linux or CentOS platform.

What you'll need

- The system on which you want to install Unified Manager must meet the system and software requirements.

  See Hardware system requirements.

  See Linux software and installation requirements.

- You must have downloaded the Unified Manager `.zip` file from the NetApp Support Site to the target system.
- You should have verified the integrity of the downloaded `.zip` file.
- You must have a supported web browser.
- Your terminal emulation software must have scrollback enabled.

The Red Hat Enterprise Linux or CentOS system might have all the required versions of the required supporting software (Java, MySQL, additional utilities) installed, only some of the required software installed, or might be a newly installed system with none of the required software installed.

Steps

1. Log in to the server on which you are installing Unified Manager.
2. Enter the appropriate commands to assess what software might require installation or upgrade on the target system to support installation:

Required software and minimum version	Command to verify software and version
OpenJDK version 11.0.17	`java -version`
MySQL 8.0.32 Community Edition	`rpm -qa | grep -i mysql`
p7zip 16.02	`rpm -qa | grep p7zip`

3. If the installed version of MySQL is earlier than MySQL 8.0.32 Community Edition, enter the following command to uninstall it:

   `rpm -e <mysql_package_name>`

   If you receive dependency errors, you must add the `--nodeps` option to uninstall the component.

4. Navigate to the directory where you downloaded the installation `.zip` file and expand the Unified Manager bundle:

```
unzip ActiveIQUnifiedManager-<version>.zip
```

The required `.rpm` modules for Unified Manager are unzipped to the target directory.

5. Verify that the following module is available in the directory:

```
ls *.rpm
```

```
netapp-um<version>.x86_64.rpm
```

6. Run the pre-installation script to ensure that there are no system configuration settings or any installed software that might conflict with the installation of Unified Manager:

```
sudo ./pre_install_check.sh
```

The pre-installation script checks that the system has a valid Red Hat Enterprise Linux subscription, and that it has access to the required software repositories. If the script identifies any issues, you must fix the issues prior to installing Unified Manager.

For Red Hat Enterprise Linux 8 system, if you have internal repositories with JDK 11 - OpenJDK, p7zip, and other software packages provided by the AppStream repository, you must disable your AppStream repository and install MySQL Community Server. Run the following command:

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install
mysql-community-server
```

7. **Optional:** You must perform step 7 only if your system is not connected to the internet and you have to manually download the packages that are required for your installation. If your system has the internet access and all the required packages are available, go to step 8. For systems that are not connected to the internet or that are not using the Red Hat Enterprise Linux repositories, perform the following steps to determine whether you are missing any required packages, and then download those packages:
   a. On the system on which you are installing Unified Manager, view the list of available and unavailable packages:
   `yum install netapp-um<version>.x86_64.rpm --assumeno`

   The items in the “Installing:” section are the packages that are available in the current directory, and the items in the “Installing for dependencies:” section are the packages that are missing on your system.

   b. On a system that has the internet access, download the missing packages:

```
yum install <package_name> --downloadonly --downloaddir=.
```

> Because the plug-in “yum-plugin-downloadonly” is not always enabled on Red Hat Enterprise Linux systems, you might need to enable the functionality to download a package without installing it: `yum install yum-plugin-downloadonly`

   c. Copy the missing packages from the internet-connected system to your installation system.

8. As the root user, or using `sudo`, run the following command to install the software:

```
yum install netapp-um<version>.x86_64.rpm
```

This command installs the .rpm packages, all other necessary supporting software, and the Unified Manager software.

If the installation fails with the GPG NOKEY error , use `rpm --import` to import the keys from a URL:

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022
```

> Do not attempt installation by using alternative commands (such as `rpm -ivh`). A successful installation of Unified Manager on a Red Hat Enterprise Linux or CentOS system requires that all Unified Manager files and related files are installed in a specific order into a specific directory structure that is enforced automatically by the `yum install netapp-um<version>.x86_64.rpm` command.

9. Disregard the email notification that is displayed immediately after the installation messages.

   The email notifies the root user of an initial cron job failure, which has no adverse effect on the installation.

10. After the installation messages are complete, scroll back through the messages until you see the message in which the system displays an IP address or URL for the Unified Manager web UI, the maintenance user name (umadmin), and a default password.

    The message is similar to the following:

```
Active IQ Unified Manager installed successfully.
Use a web browser and one of the following URL(s) to configure and
access the Unified Manager GUI.
https://default_ip_address/    (if using IPv4)
https://[default_ip_address]/  (if using IPv6)
https://fully_qualified_domain_name/

Log in to Unified Manager in a web browser by using following details:
  username: umadmin
  password: admin
```

11. Record the IP address or URL, the assigned user name (umadmin), and the current password.
12. If you created a umadmin user account with a custom home directory prior to installing Unified Manager, then you must specify the umadmin user login shell:

```
usermod -s /bin/maintenance-user-shell.sh umadmin
```

Access the web UI to change the default password of the umadmin user, and perform the initial setup of Unified Manager, as described in Configuring Active IQ Unified Manager. It is mandatory to change the default password of the umadmin user.

Users created during Unified Manager installation

When you install Unified Manager on Red Hat Enterprise Linux or CentOS, the following users are created by Unified Manager and third-party utilities: umadmin, jboss, and mysql.

- **umadmin**

  Used to log in to Unified Manager for the first time. This user is assigned an “Application Administrator” user role and is configured as the “Maintenance User” type. This user is created by Unified Manager.

- **jboss**

  Used to run Unified Manager services related to the JBoss utility. This user is created by Unified Manager.

- **mysql**

  Used to run MySQL database queries of Unified Manager. This user is created by the MySQL third-party utility.

In addition to these users, Unified Manager also creates corresponding groups: maintenance, jboss, and mysql. The maintenance and jboss groups are created by Unified Manager, while the mysql group is created by a third-party utility.

If you created a custom home directory and defined your own umadmin user password prior to installing Unified Manager, the installation program does not recreate the maintenance group or the umadmin user.

Changing the JBoss password

You can reset the instance-specific JBoss password that is set during installation. You can reset the password optionally, in case your site requires this security capability to override the Unified Manager installation setting. This operation also changes the password JBoss uses to access MySQL.

- You must have root user access to the Red Hat Enterprise Linux or CentOS system on which Unified Manager is installed.
- You must be able to access the NetApp-provided `password.sh` script in the directory `/opt/netapp/essentials/bin`.

Steps

1. Log in as root user on the system.
2. Stop the Unified Manager services by entering the following commands in the order shown:

   ```
   systemctl stop ocieau

   systemctl stop ocie
   ```

   Do not stop the associated MySQL software.

3. Enter the following command to begin the password change process:

   ```
   /opt/netapp/essentials/bin/password.sh resetJBossPassword
   ```

4. When prompted, enter the new JBoss password, and then enter it a second time for confirmation.

   Note that the password should be between 8 and 16 characters, and must contain at least a digit, an upper case and lower case characters, and at least one of these special characters:

```
!@%^*-_=[]:<>.?/~+
```

5. When the script completes, start the Unified Manager services by entering the following commands in the order shown:

```
systemctl start ocie

systemctl start ocieau
```

6. After all of the services are started, you can log in to the Unified Manager UI.

Upgrading Unified Manager on Red Hat Enterprise Linux or CentOS

You can upgrade Unified Manager when a new version is available.

Patch releases of Unified Manager software, when provided by NetApp, are installed using the same procedure as new releases.

If Unified Manager is paired with an instance of OnCommand Workflow Automation, and there are new versions of software available for both products, you must disconnect the two products and then set up a new Workflow Automation connection after performing the upgrades. If you are performing an upgrade to only one of the products, then you should log into Workflow Automation after the upgrade and verify that it is still acquiring data from Unified Manager.

Supported upgrade path for Unified Manager versions

Active IQ Unified Manager supports a specific upgrade path for each version.

Not all versions of Unified Manager can perform an in-place upgrade to later versions. The Unified Manager upgrades are limited to an N-2 model, meaning an upgrade can only be performed within the next 2 releases on all platforms. For example, you can perform an upgrade to Unified Manager 9.13 from Unified Manager 9.11 and 9.12 only.

If you are running a version that is earlier than the supported versions, your Unified Manager instance will need to be upgraded to one of the supported versions first, and then upgraded to the current version.

For example, if your installed version is OnCommand Unified Manager 9.6 and you want to upgrade to the latest release Active IQ Unified Manager 9.13, you follow a sequence of upgrades.

Sample upgrade path:

1. Upgrade OnCommand Unified Manager 9.6 → Active IQ Unified Manager 9.8
2. Upgrade 9.8 → 9.10
3. Upgrade 9.10 → 9.12
4. Upgrade 9.12 → 9.13

For more information on the upgrade path matrix, see this knowledge base (KB) article.

Upgrading Unified Manager

You can upgrade from Unified Manager 9.11 or 9.12 to 9.13 by downloading and running the installation file on the Linux platform.

What you'll need

- The system on which you are upgrading Unified Manager must meet the system and software requirements.

  See Hardware system requirements.

  See Linux software and installation requirements.

- You must have a subscription to the Red Hat Enterprise Linux Subscription Manager.
- You must install, or upgrade to the correct version of OpenJDK prior to upgrading Unified Manager.

  See Upgrading JRE on Linux.

- To avoid data loss, you must have created a backup of the Unified Manager database in case there is an issue during the upgrade. NetApp recommends that you move the backup file from the `/opt/netapp/data` directory to an external location.
- During upgrade, you may be prompted to confirm whether you want to keep the previous, default settings for retaining performance data for 13 months or to change it to 6 months. On confirming, the historical performance data is purged after 6 months.
- You should have completed any running operations, because Unified Manager is unavailable during the upgrade process.
- MySQL Community Edition is automatically upgraded during Unified Manager upgrade. If the installed version of MySQL on your system is earlier than 8.0.32, the Unified Manager upgrade process automatically upgrades MySQL to 8.0.32.

Steps

1. Log in to the target Red Hat Enterprise Linux or CentOS server.
2. Download the Unified Manager bundle to the server.

   See Downloading Unified Manager for Linux.

3. Navigate to the target directory and expand the Unified Manager bundle:

   ```
   unzip ActiveIQUnifiedManager-<version>.zip
   ```

   The required RPM modules for Unified Manager are unzipped to the target directory.

4. Verify that the following module is available in the directory:

   ```
   ls *.rpm
   ```

   ```
   netapp-um<version>.x86_64.rpm
   ```

5. Run the pre-installation script to ensure that there are no system configuration settings or any installed software that might conflict with the upgrade:

   ```
   sudo ./pre_install_check.sh
   ```

   The pre-installation script checks that the system has a valid Red Hat Enterprise Linux subscription, and that it has access to the required software repositories. If the script identifies any issues, you must fix the issues and continue with the upgrade.

If there are any missing packages detected, perform the steps mentioned in Additional steps to perform for missing packages. If there are no missing packages, continue with the next steps.

6. Upgrade Unified Manager using the following script:

   ```
   upgrade.sh
   ```

   This script automatically executes the RPM modules, upgrading the necessary supporting software and the Unified Manager modules that run on them. Additionally, the upgrade script checks whether there are any system configuration settings or any installed software that might conflict with the upgrade. If the script identifies any issues, you must fix the issues before upgrading Unified Manager. If you have previously installed packages, such as *net-snmp* before you upgraded Unified Manager, the MySQL dependency might uninstall the package during upgrade. You need to install the package manually again for continuing to use it.

7. After the upgrade is complete, scroll back through the messages until you see the message displaying an IP address or URL for the Unified Manager web UI, the maintenance user name (umadmin), and the default password.

   The message is similar to the following:

   ```
   Active IQ Unified Manager upgraded successfully.
   Use a web browser and one of the following URLs to access the Unified
   Manager GUI:

   https://default_ip_address/    (if using IPv4)
   https://[default_ip_address]/  (if using IPv6)
   https://fully_qualified_domain_name/
   ```

Enter the specified IP address or URL in a new window of a supported web browser to start the Unified Manager web UI, and then log in by using the same maintenance user name (umadmin) and password that you set earlier.

Additional steps to perform for missing packages

If there are any missing packages detected at your site during upgrade, or if your system is not connected to the internet, or you are not using the Red Hat Enterprise Linux repositories, perform the following steps to determine whether you are missing any required packages and download those packages.

These steps need to be performed after step *5* of the main procedure. This procedure upgrades Unified Manager and you do not need to run any additional steps for upgrade.

1. View the list of available and unavailable packages:

   ```
   yum install netapp-um<version>.x86_64.rpm --assumeno
   ```

   The items in the “Installing:” section are the packages that are available in the current directory, and the items in the “Installing for dependencies:” section are the packages that are missing on your system.

2. On a different system that has the internet access, run the following command to download the missing packages.

```
yum install package_name --downloadonly --downloaddir=.
```

The packages are downloaded in the directory specified as `--downloaddir=`.

Because the plug-in “yum-plugin-downloadonly” is not always enabled on Red Hat Enterprise Linux systems, you might need to enable the functionality to download a package without installing it:

```
yum install yum-plugin-downloadonly
```

3. Copy the downloaded packages to the directory where you unzipped the Unified Manager bundle on the installation system.
4. Change directories to that directory and run the following command for installing the missing packages, along with their dependencies.

```
yum install *.rpm
```

5. Start the Unified Manager server. Run these commands:

```
systemctl start ocie

systemctl start ocieau
```

This process completes the Unified Manager upgrade process. Enter the specified IP address or URL in a new window of a supported web browser to start the Unified Manager web UI, and then log in by using the same maintenance user name (umadmin) and password that you set earlier.

Upgrading the host OS from Red Hat Enterprise Linux 7.x to 8.x

If you previously installed Unified Manager on a Red Hat Enterprise Linux 7.x system and need to upgrade to Red Hat Enterprise Linux 8.x, you must follow one of the procedures listed in this topic. In both cases you must create a backup of Unified Manager on the Red Hat Enterprise Linux 7.x system, and then restore the backup onto a Red Hat Enterprise Linux 8.x system. Note that the supported versions of Red Hat Enterprise Linux are from 8.0 to 8.7.

The difference between the two options listed below is that in one case you are performing the Unified Manager restore onto a new 8.x server, and in the other case you are performing the restore operation onto the same server.

Because this task requires that you create a backup of Unified Manager on the Red Hat Enterprise Linux 7.x system, you should create the backup only when you are prepared to complete the entire upgrade process so that Unified Manager is offline for the shortest period of time. Gaps in collected data appear in the Unified Manager UI for the period of time during which the Red Hat Enterprise Linux 7.x system is shut down and before the new Red Hat Enterprise Linux 8.x is started.

See Managing backup and restore operations if you need to review detailed instructions for the backup and restore processes.

Follow these steps if you have a spare system on which you can install Red Hat Enterprise Linux 8.x software so that you can perform the Unified Manager restore on that system while the Red Hat Enterprise Linux 7.x system is still available.

1. Install and configure a new server with Red Hat Enterprise Linux 8.x software.

   See Linux software and installation requirements.

2. On the Red Hat Enterprise Linux 8.x system, install the same version of Unified Manager software that you have on the existing Red Hat Enterprise Linux 7.x system.

   See Installing Unified Manager on Linux.

   Do not launch the UI or configure any clusters, users, or authentication settings when the installation is complete. The backup file populates this information during the restore process.

3. On the Red Hat Enterprise Linux 7.x system, from the Administration menu in the web UI, create a Unified Manager backup and then copy the backup file (`.7z` file) and the contents of the database repository directory (`/database-dumps-repo` subdirectory) to an external location.
4. On the Red Hat Enterprise Linux 7.x system, shut down Unified Manager.
5. On the Red Hat Enterprise Linux 8.x system, copy the backup file (`.7z` file) from the external location to `/opt/netapp/data/ocum-backup/` and the database repository files to the `/database-dumps-repo` subdirectory under the `/ocum-backup` directory.
6. Enter the following command to restore the Unified Manager database from the backup file:

   ```
   um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
   ```

7. Enter the IP address or URL into your web browser to start the Unified Manager web UI, and then log in to the system.

Once you have verified that the system is operating properly you can remove Unified Manager from the Red Hat Enterprise Linux 7.x system.

Upgrading the host OS on the same server

Follow these steps if you do not have a spare system on which you can install Red Hat Enterprise Linux 8.x software.

1. From the Administration menu in the web UI, create a Unified Manager backup and then copy the backup file (`.7z` file) and the contents of the database repository directory (`/database-dumps-repo` subdirectory) to an external location.
2. Remove the Red Hat Enterprise Linux 7.x image from the system and completely wipe the system.
3. Install and configure Red Hat Enterprise Linux 8.x software on the same system.

   See Linux software and installation requirements.

4. On the Red Hat Enterprise Linux 8.x system, install the same version of Unified Manager software that you had on the Red Hat Enterprise Linux 7.x system.

   See Installing Unified Manager on Linux.

   Do not launch the UI or configure any clusters, users, or authentication settings when the installation is complete. The backup file populates this information during the restore process.

5. Copy the backup file (`.7z` file) from the external location to `/opt/netapp/data/ocum-backup/` and the database repository files to the `/database-dumps-repo` subdirectory under the `/ocum-backup`

directory.

6. Enter the following command to restore the Unified Manager database from the backup file:

   ```
   um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
   ```

7. Enter the IP address or URL into your web browser to start the Unified Manager web UI, and then log in to the system.

Upgrading third-party products post Unified Manager installation

You can upgrade third-party products, such as JRE, when Unified Manager is already installed on Linux systems.

The companies that develop these third-party products report security vulnerabilities on a regular basis. You can upgrade to newer versions of this software at your own schedule.

Upgrading OpenJDK on Linux

You can upgrade to a newer version of OpenJDK on the Linux server on which Unified Manager is installed to obtain fixes for security vulnerabilities.

What you'll need

You must have root privileges for the Linux system on which Unified Manager is installed.

You can update OpenJDK releases within release families. For example, you can upgrade from OpenJDK 11.0.14 to OpenJDK 11.0.17, but you cannot update directly from OpenJDK 11 to OpenJDK 12.

Steps

1. Log in as a root user on the Unified Manager host machine.
2. Download the appropriate version of OpenJDK (64-bit) to the target system.
3. Stop the Unified Manager services:

   ```
   systemctl stop ocieau

   systemctl stop ocie
   ```

4. Install the latest OpenJDK on the system.
5. Start the Unified Manager services:

   ```
   systemctl start ocie

   systemctl start ocieau
   ```

Restarting Unified Manager

You might have to restart Unified Manager after making configuration changes.

What you'll need

You must have root user access to the Red Hat Enterprise Linux or CentOS server on which Unified Manager is installed.

Steps

1. Log in as root user to the server on which you want to restart the Unified Manager service.
2. Stop the Unified Manager service and the associated MySQL service in this order:

```
systemctl stop ocieau

systemctl stop ocie

systemctl stop mysqld
```

3. Start MySQL and Unified Manager services in this order:

```
systemctl start mysqld

systemctl start ocie

systemctl start ocieau
```

`mysqld` is a daemon program required to start and stop the MySQL server.

Removing Unified Manager

You can stop and uninstall Unified Manager from the Red Hat Enterprise Linux or CentOS host with a single command.

What you'll need

- You must have root user access to the server from which you want to remove Unified Manager.
- Security-Enhanced Linux (SELinux) must be disabled on the Linux system. Change the SELinux runtime mode to "Permissive" by using the `setenforce 0` command.
- All clusters (data sources) must be removed from the Unified Manager server before removing the software.
- You should manually delete the firewall rules that are created to allow or block MySQL port 3306. The firewall rules are not deleted automatically.

Steps

1. Log in as root user to the server on which you want to remove Unified Manager.
2. Stop and remove Unified Manager from the server:

```
rpm -e netapp-um
```

   This step removes all the associated NetApp RPM packages. It does not remove the prerequisite software modules, such as Java, MySQL, and p7zip.

3. **Optional:** If appropriate, remove the supporting software modules, such as Java, MySQL, and p7zip:

```
rpm -e p7zip mysql-community-client mysql-community-server mysql-community-
```

```
common mysql-community-libs java-x.y
```

After this operation is complete, the software is removed. All the data from the `/opt/netapp/data` directory is moved to the `/opt/netapp/data/BACKUP` folder after uninstallation. Uninstalling Unified Manager removes the Java and MySQL packages also, unless the packages are required and used by any other application on the system. However, MySQL data is not deleted.

Removing the custom umadmin user and maintenance group

If you created a custom home directory to define your own umadmin user and maintenance account prior to installing Unified Manager, you should remove these items after you have uninstalled Unified Manager.

The standard Unified Manager uninstallation does not remove a custom-defined umadmin user and maintenance account. You must delete these items manually.

Steps

1. Log in as the root user to the Red Hat Enterprise Linux server.
2. Delete the umadmin user:

   ```
   userdel umadmin
   ```

3. Delete the maintenance group:

   ```
   groupdel maintenance
   ```

Copyright information

Trademark information