Installing, upgrading, and removing Unified Manager software on Red Hat or CentOS

OnCommand Unified Manager 9.5

NetApp
October 23, 2024

Table of Contents

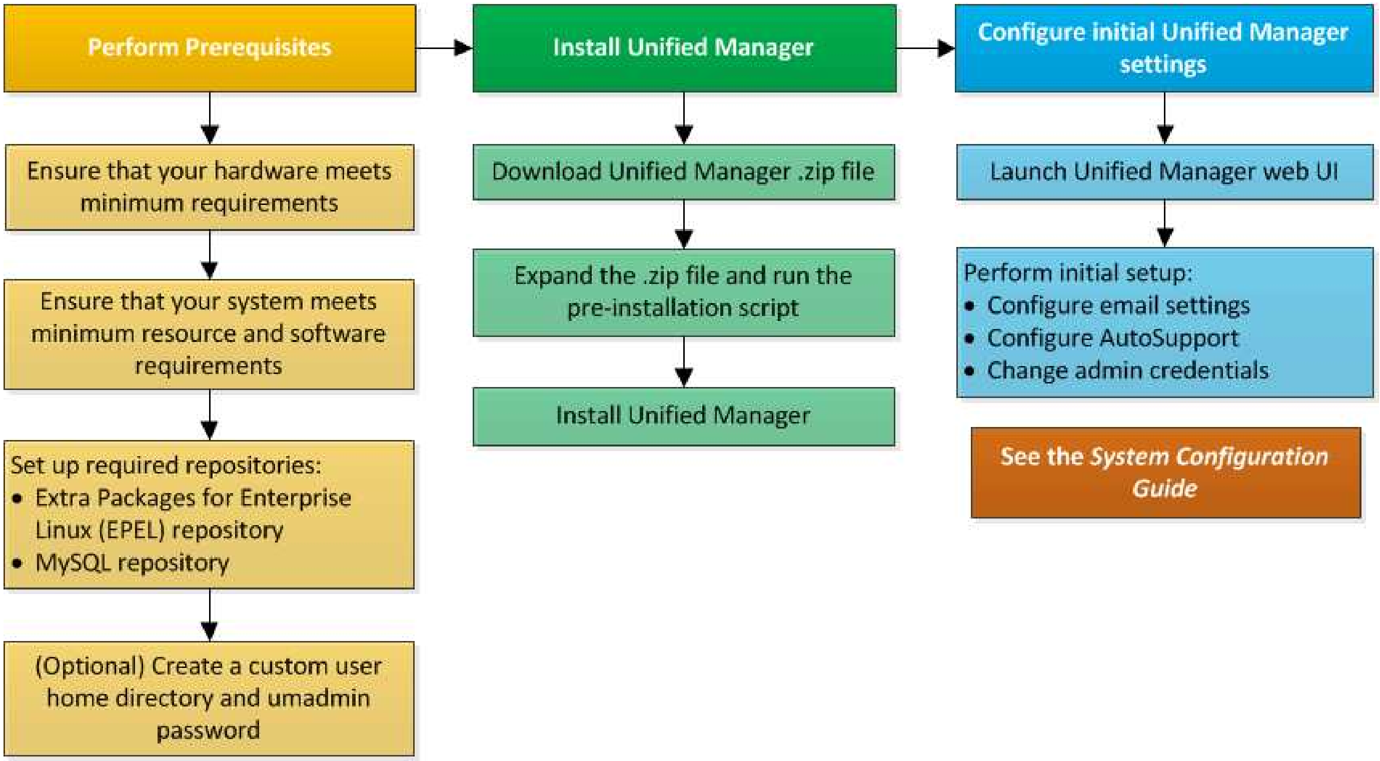
Installing, upgrading, and removing Unified Manager software on Red Hat or CentOS

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 on Red Hat or CentOS

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


Perform Prerequisites
Ensure that your hardware meets minimum requirements
Ensure that your system meets minimum resource and software requirements
Set up required repositories:
• Extra Packages for Enterprise Linux (EPEL) repository
• MySQL repository
(Optional) Create a custom user home directory and umadmin password
Install Unified Manager
Download Unified Manager .zip file
Expand the .zip file and run the pre-installation script
Install Unified Manager
Configure initial Unified Manager settings
Launch Unified Manager web UI
Perform initial setup:
• Configure email settings
• Configure AutoSupport
• Change admin credentials
See the System Configuration Guide

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.

About this task

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 or CentOS system.

Steps

1. Download the EPEL repository for your installation: `wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm`
2. Configure the EPEL repository: `yum install epel-release-latest-7.noarch.rpm`

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.

About this task

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

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

Steps

1. Download the appropriate MySQL repository for your installation: `wget http://repo.mysql.com/yum/mysql-5.7-community/el/7/x86_64/mysql57-community-release-el7-7.noarch.rpm`
2. Configure the MySQL repository: `yum install mysql57-community-release-el7-7.noarch.rpm`

SELinux requirements for mounting `/opt/netapp` or `/opt/netapp/data` on an NFS or CIFS share

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 the following considerations.

About this task

If are planning to mount `/opt/netapp` or `/opt/netapp/data` from anywhere other that the root file system, and you have SELinux enabled in your environment, you must set the correct context for the mounted directories. Follow these two steps for setting and confirming the correct SELinux context.

- Configure SELinux context when `/opt/netapp/data` is mounted
- Configure SELinux context when `/opt/netapp` is mounted

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` that must be changed 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 mysql_db_t "/opt/netapp/data"``restorecon -R -v /opt/netapp/data```

   b. If you have configured `/opt/netapp/data` in `/etc/fstab`, you must 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 `mysql_db_t`: `mount <nfsshare>:/<mountpoint> /opt/netapp/data -o context=system_u:object_r:mysql_db_t:s0`

3. Verify whether the context is set correctly: `ls -dZ /opt/netapp/data/`

   ```
   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

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`.

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` that must 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```
   b. If you have configured `/opt/netapp` in `/etc/fstab`, you must edit the `/etc/fstab` file. For the `/opt/netapp` mount option, add the MySQL label as: `context=system_u:object_r:usr_t:s0`
   c. Unmount and remount `/opt/netapp` for enabling the context.
   d. 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`
3. Verify whether the context is set correctly: `ls -dZ /opt/netapp`

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

Installing Unified Manager on Red Hat Enterprise Linux or CentOS

It is important that you understand that the sequence of steps to download and install Unified Manager varies according to your installation scenario. Before you install Unified Manager on Red Hat Enterprise Linux or CentOS, you can decide if you want to configure Unified Manager for high availability.

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.

Before you begin

- 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.

About this task

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.

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 finish

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

Downloading Unified Manager for Red Hat Enterprise Linux or CentOS

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

Before you begin

You must have login credentials for the NetApp Support Site.

About this task

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 installing Unified Manager on the Red Hat Enterprise Linux platform.

   NetApp Downloads: Software

2. Download the Unified Manager`.zip` file to a directory on the target system.
3. Verify the checksum to ensure that the software downloaded correctly.

Installing Unified Manager on Red Hat Enterprise Linux or CentOS

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

CentOS platform.

Before you begin

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

  Hardware system requirements

  Red Hat and CentOS software and installation requirements

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

About this task

The Red Hat Enterprise Linux or CentOS system may have all the required versions of the required supporting software (Java, MySQL, additional utilities) installed, or it may have only some of the required software installed, or it may 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	`java -version`
MySQL 5.7.23 Community Edition	`rpm -qa | grep -i mysql`
p7zip 9.20.1	`rpm -qa | grep p7zip`

3. If any version of the listed software is earlier than the required version, enter the appropriate command to uninstall that module:

Software to uninstall	Command to uninstall the software
MySQL Uninstall any version that is not MySQL 5.7.23 Community Edition or later.	`rpm -e <mysql_package_name>` If you receive dependency errors, you must add the `--nodeps` option to uninstall the component.
All other modules	`yum remove module_name`

4. Navigate to the directory where you downloaded the installation `.zip` file and expand the Unified Manager bundle: `unzip OnCommandUnifiedManager-rhel7-9.5.zip`

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

5. Verify that the following modules are available in the directory: `ls *.rpm`
   - `ocie-au-<version>.x86_64.rpm`
   - `ocie-server-<version>.x86_64.rpm`
   - `ocie-serverbase-<version>.x86_64.rpm`
   - `netapp-application-server-<version>.x86_64.rpm`
   - `netapp-platform-base-<version>.x86_64.rpm`
   - `netapp-ocum-<version>.x86_64.rpm`
6. Run the pre-installation script to ensure that there are no system configuration settings or any installed software that will conflict with the installation of Unified Manager: `pre_install_check.sh`

   The pre-installation script checks that the system has a valid Red Hat 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.

   > You must perform step 7 *only* if you are required to manually download the packages that are required for your installation. If your system has Internet access and all the required packages are available, go to step 8.

7. 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 *.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 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. Install the software: `yum install *.rpm`

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

> Do not attempt installation by using alternative commands (such as `rpm -ivh ...`). The 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 *.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:

    ```
    OnCommand 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`

After you finish

You can access the web UI to perform the initial setup of Unified Manager, as described in the *OnCommand Unified Manager System Configuration Guide*.

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 “OnCommand 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 create a new, custom JBoss password to overwrite the default password that is set during installation. This task is optional, but some sites might require this security capability to override the Unified Manager installation default setting. This operation also changes the password JBoss uses to access MySQL.

Before you begin

- 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: `service ocieau stop``service ocie stop`

   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 old JBoss password.

   The default password is `D11h1aMu@79%`.

5. When prompted, enter the new JBoss password, and then enter it a second time for confirmation.
6. When the script completes, start the Unified Manager services by entering the following commands in the order shown: `service ocie start``service ocieau start`
7. After all of the services are started, you can log in to the Unified Manager UI.

Setting up Unified Manager for high availability

You can create a high-availability setup by using the Veritas Cluster Server (VCS). The high-availability setup provides failover capability and helps in disaster recovery.

In a high-availability setup, only one node remains active at a time. When one node fails, VCS service recognizes this event and immediately transfers control to the other node. The second node in the setup becomes active and starts providing services. The failover process is automatic.

A VCS cluster configured with the Unified Manager server consists of two nodes, with each node running the same version of the Unified Manager. All of the Unified Manager server data must be configured for access from a shared data disk.

After you install Unified Manager in VCS, you must configure Unified Manager to work in the VCS environment. You can use configuration scripts to set up Unified Manager to work in VCS environments.

Requirements for Unified Manager in VCS

Before installing Unified Manager in a Veritas Cluster Server (VCS) environment, you must ensure that the cluster nodes are properly configured to support Unified Manager.

You must ensure that the VCS configuration meets the following requirements:

- Both the cluster nodes must be running a supported operating system version.
- The same version of Unified Manager must be installed using the same path on both the cluster nodes.
- The MySQL user on both the nodes must have the same user ID and group ID.
- Native ext3, ext4 file systems, and Logical Volume Manager (LVM) must be used.
- Unified Manager must be connected to the storage system through Fibre Channel (FC) or iSCSI.

  You must also ensure that the FC link is active and that the LUNs created on the storage systems are accessible to both the cluster nodes.
- The shared data disk must have enough space (minimum 80 GB) for the Unified Manager database, reports, certificates, and script plug-in folders.
- A minimum of two network interfaces must be set up on each system: one for node-to-node communication and the other for node-to-client communication.

  The name of the network interface used for node-to-client communication must be the same on both the systems.
- A separate heartbeat link must be established between the cluster nodes; otherwise, the network interface is used to communicate between the cluster nodes.
- Optional: SnapDrive for UNIX should be used to create a shared location that is accessible to both the nodes in a high availability setup.

  See the *SnapDrive for UNIX Installation and Administration Guide* for information about installing and creating a shared location. You can also manage LUNs using SnapDrive or the storage system command-line interface. See the SnapDrive for UNIX compatibility matrix for more information.
- Additional RAM must be available for the SnapDrive and VCS applications.

Installing Unified Manager on VCS

For configuring high availability, you must install Unified Manager on both the cluster nodes of VCS.

Before you begin

- VCS must be installed and configured on both the nodes of the cluster.

  See the instructions provided in the *Veritas Cluster Server 6.2.1 Installation Guide* for more information about installing VCS.

- You must have clear root privileges to log in to the Unified Manager server console.

About this task

You must configure both the instances of Unified Manager to use the same database and to monitor the same set of nodes.

Steps

1. Log in to the first node of the cluster.
2. Install Unified Manager on the first node.

   Installing Unified Manager on Red Hat Enterprise Linux or CentOS

3. Repeat Steps 1 and 2 on the second node of the cluster.
4. On the second instance of Unified Manager, log in as the root user to the Red Hat Enterprise Linux or CentOS server and enter the same umadmin password as you defined on the first instance of Unified Manager.`passwd umadmin`

Configuring Unified Manager with VCS using configuration scripts

You can configure Unified Manager with Veritas Cluster Server (VCS) using configuration scripts.

Before you begin

- Unified Manager must be installed on both the nodes in the VCS setup.
- The XML:: LibXML module must be bundled with Perl for VCS scripts to work.
- You must have created a shared LUN with sufficient size to accommodate the source Unified Manager data.
- You must have specified the absolute mount path for the script to work.

  The script will not work if you create a folder inside the mount path.

- You must have downloaded the `ha_setup.pl` script at `/opt/netapp/ocum/scripts`.

About this task

In the VCS setup, the node for which the virtual IP interface and mount point are active is the first node. The other node is the second node.

Steps

1. Log in to the first node of the cluster.

   You must have stopped all the Unified Manager services on the second node in the high availability setup.

2. Add the VCS installation directory `/opt/VRTSvcs/bin` to the PATH environmental variable.
3. If you are configuring an existing Unified Manager setup, create a Unified Manager backup and generate the support bundle.
4. Run the `ha_setup.pl` script: `perl ha_setup.pl --first -t vcs -g group_name -e eth_name -i cluster_ip -m net_mask -n fully_qualified_cluster_name -f mount_path -v volume_group -d disk_group -l install_dir -u user_name -p password`

   ```
   perl \ha_setup.pl --first -t vcs -g umgroup -e eth0 -i 10.11.12.13 -m
   255.255.255.0 -n cluster.eng.company.com -f /mnt/ocumdb -v ocumdb_SdHv -d
   ocumdb_SdDg -l /opt/netapp/ -u admin -p wx17yz
   ```

5. Use the Veritas Operation Manager web console or VCS Cluster Manager to verify that a failover group is created, and that the Unified Manager server services, mount point, virtual IP, network interface card (NIC), and volume group are added to the cluster group.
6. Manually move the Unified Manager service group to the secondary node and verify that cluster failover is working.
7. Verify that VCS has switched over to the second node of the cluster.

   You must verify that the data mount, virtual IP, volume group, and NIC are online on the second node of the cluster.

8. Stop Unified Manager using Veritas Operation Manager.
9. Run the ```perl ha_setup.pl --join -t vcs -f``mount_path``` command on the second node of the cluster so that the Unified Manager server data points to the LUN.
10. Verify that the Unified Manager server services are starting properly on the second node of the cluster.
11. Regenerate the Unified Manager certificate after running the configuration scripts to obtain the global IP address.

    a. In the toolbar, click ⚙, and then click **HTTPS Certificate** from the **Setup** menu.

    b. Click **Regenerate HTTPS Certificate**.

    The regenerated certificate provides only the cluster IP address, not the fully qualified domain name (FQDN). You must use the global IP address to set up Unified Manager for high-availability.

12. Access the Unified Manager UI using the following: `https://<FQDN of Global IP>`

After you finish

You must create a shared backup location after high availability is configured. The shared location is required for containing the backups that you create before and after failover. Both the nodes in the high-availability setup must be able to access the shared location.

Unified Manager service resources for VCS configuration

You must add the cluster service resources of Unified Manager to Veritas Cluster Server (VCS). These cluster service resources are used for various purposes, such as monitoring storage systems, scheduling jobs, processing events, and monitoring all the other Unified Manager services.

The following table lists the category of all the Unified Manager services:

Category	Services
Storage resource	• `vol` • `mount`
Database resource	• `mysqld`
Network resource	• `nic` • `vip`
Unified Manager resource	• `ocie` • `ocieau`

Updating an existing Unified Manager setup for high availability

You can update your existing Unified Manager installation and configure your setup environment for high availability.

Before you begin

- You must have created a backup and support bundle of your existing data.
- You must have the OnCommand Administrator or Storage Administrator role.
- You must have added a second node to your cluster and installed Veritas Cluster Server (VCS) on the second node.

  See the *Veritas Cluster Server 6.2.1 Installation Guide*.
- The newly added node must be configured to access the same shared location as that of the existing node in the high-availability setup.

Steps

1. Log in to the new node of the cluster.
2. Install Unified Manager on the node.

   Installing Unified Manager on Red Hat Enterprise Linux or CentOS
3. Configure the Unified Manager server using configuration scripts on the existing node with data.

4. Initiate manual fail over to the second node.
5. Run the perl ha_setup.pl --join -t vcs -f``mount_path command on the second node of the cluster so that the Unified Manager server data points to the shared LUN.
6. If OnCommand Workflow Automation (WFA) is configured for Unified Manager, disable and then reconfigure the WFA connection.
7. If SnapProtect is configured with Unified Manager, reconfigure SnapProtect with a new cluster IP address and the existing storage policies.
8. Regenerate the custom reports and add these reports to Unified Manager with the new cluster IP address.

Upgrading Unified Manager on Red Hat Enterprise Linux or CentOS

You can upgrade Unified Manager when a new version of software 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.

Upgrading Unified Manager on Red Hat Enterprise Linux or CentOS

You can upgrade from Unified Manager version 7.3 or 9.4 to Unified Manager 9.5 by downloading and running the installation file on the Red Hat platform.

Before you begin

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

  Hardware system requirements

  Red Hat and CentOS software and installation requirements

- Starting with Unified Manager 9.4, Red Hat Enterprise Linux 6.x is no longer supported. If you are using RHEL 6, you must upgrade your instance of RHEL to version 7.x prior to upgrading to Unified Manager 9.5.
- Starting with Unified Manager 9.5, Oracle Java is no longer supported. The correct version of OpenJDK must be installed prior to upgrading to Unified Manager 9.5.
- You must have a subscription to the Red Hat Enterprise Linux Subscription Manager.
- To avoid data loss, you must have created a backup of the Unified Manager database in case there is an issue during the upgrade. It is also recommended that you move the backup file from the `/opt/netapp/data` directory to an external location.
- You should have completed any running operations, because Unified Manager is unavailable during the upgrade process.

About this task

> ⓘ These steps contain information for systems that are configured for high availability using Veritas Operation Manager. If your system is not configured for high availability, ignore these additional steps.

Steps

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

   Downloading Unified Manager for Red Hat or CentOS

3. Navigate to the target directory and expand the Unified Manager bundle: `unzip OnCommandUnifiedManager-rhel7-9.5.zip`

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

4. Confirm the presence of the listed modules: `ls *.rpm`

   The following RPM modules are listed:

   - `ocie-au-<version>.x86_64.rpm`
   - `ocie-server-<version>.x86_64.rpm`
   - `ocie-serverbase-<version>.x86_64.rpm`
   - `netapp-application-server-<version>.x86_64.rpm`
   - `netapp-platform-base-<version>.x86_64.rpm`
   - `netapp-ocum-<version>.x86_64.rpm`

5. For systems that are not connected to the Internet or that are not using the RHEL repositories, perform the following steps to determine whether you are missing any required packages and download those packages:

   a. View the list of available and unavailable packages: `yum install *.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. Download the missing packages on another system that has Internet access: `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.

6. If Unified Manager is configured for high availability, then using Veritas Operation Manager, stop all Unified Manager services on the first node.
7. 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 will conflict with the upgrade of Unified Manager. If the script identifies any issues, you must fix the issues prior to upgrading Unified Manager.

> Do not attempt to upgrade by using alternative commands (such as `rpm -Uvh ...`). A successful upgrade requires that all Unified Manager files and related files are upgraded in a specific order to a specific directory structure that are executed and configured automatically by the script.

8. For high availability installations, stop all Unified Manager services on the second node with Veritas Operation Manager.
9. For high availability installations, switch the service group to the second node in the high-availability setup and upgrade Unified Manager on the second node.
10. 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:

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

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

After you finish

Enter the specified IP address or URL into 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 6.x to 7.x

If you previously installed Unified Manager on a Red Hat Enterprise Linux 6.x system and now need to upgrade to Red Hat Enterprise Linux 7.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 6.x system, and then restore the backup onto a Red Hat Enterprise Linux 7.x system.

About this task

The difference between the two options listed below is that in one case you are performing the Unified Manager restore onto a new RHEL 7.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 6.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 will appear in the Unified Manager UI for the period of time during which the Red Hat Enterprise Linux 6.x system is shut down and before the new Red Hat Enterprise Linux 7.x is started.

See the *Unified Manager Online Help* if you need to review detailed instructions for the backup and restore processes.

Upgrading the host OS using a new server

Follow these steps if you have a spare system on which you can install RHEL 7.x software so that you can perform the Unified Manager restore on that system while the RHEL 6.x system is still available.

1. Install and configure a new server with Red Hat Enterprise Linux 7.x software.

   Red Hat software and installation requirements

2. On the Red Hat Enterprise Linux 7.x system, install the same version of Unified Manager software that you have on the existing Red Hat Enterprise Linux 6.x system.

   Installing Unified Manager on Red Hat Enterprise 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 6.x system, from the Administration menu in the web UI, create a Unified Manager backup and then copy the backup file to an external location.
4. On the Red Hat Enterprise Linux 6.x system, shut down Unified Manager.
5. On the Red Hat Enterprise Linux 7.x system, copy the backup file from the external location to `/data/ocum-backup/`, and then 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>`
6. Enter the IP address or URL into a supported 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 6.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 RHEL 7.x software.

1. From the Administration menu in the web UI, create a Unified Manager backup and then copy the backup file to an external location.
2. Remove the Red Hat Enterprise Linux 6.x image from the system and completely wipe the system.
3. Install and configure Red Hat Enterprise Linux 7.x software on the same system.

   Red Hat software and installation requirements

4. On the Red Hat Enterprise Linux 7.x system, install the same version of Unified Manager software that you had on the Red Hat Enterprise Linux 6.x system.

   Installing Unified Manager on Red Hat Enterprise 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 from the external location to `/data/ocum-backup/`, and then 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>`
6. Enter the IP address or URL into a supported web browser to start the Unified Manager web UI, and then log in to the system.

Upgrading third-party products on Linux

You can upgrade third-party products, such as JRE and MySQL, on Unified Manager when 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 JRE on Linux

You can upgrade to a newer version of Java Runtime Environment (JRE) on the Linux server on which Unified Manager is installed to obtain fixes for security vulnerabilities.

Before you begin

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

Steps

1. Log in as a root user on the Unified Manager host machine.
2. Download the appropriate version of Java (64-bit) to the target system.
3. Stop the Unified Manager services: `service ocieau stop``service ocie stop`
4. Install the latest JRE on the system.
5. Start the Unified Manager services: `service ocie start``service ocieau start`

Upgrading MySQL on Linux

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

Before you begin

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

About this task

You can only upgrade to minor updates of MySQL 5.7, for example, 5.7.1 to 5.7.2 . You cannot upgrade to major versions of MySQL, for example, version 5.8.

Steps

1. Log in as a root user on the Unified Manager host machine.
2. Download the latest MySQL Community Server `.rpm` bundle on the target system.
3. Untar the bundle to a directory on the target system.
4. You will get multiple `.rpm` packages in the directory after untarring the bundle, but Unified Manager only needs the following rpm packages:
   - mysql-community-client-5.7.x
   - mysql-community-libs-5.7.x
   - mysql-community-server-5.7.x
   - mysql-community-common-5.7.x
   - mysql-community-libs-compat-5.7.x Delete all other `.rpm` packages. Installing all packages in an rpm bundle will not cause any problems.
5. Stop the Unified Manager service and the associated MySQL software in the order shown: `service ocieau stopservice ocie stopservice mysqld stop`
6. Invoke the upgrade of MySQL by using the following command: `yum install *.rpm`

   `*.rpm` refers to the `.rpm` packages in the directory where you downloaded the newer version of MySQL.
7. Start Unified Manager in the order shown: `service mysqld startservice ocie startservice ocieau start`

Restarting Unified Manager in Red Hat Enterprise Linux or CentOS

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

Before you begin

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 software in the order shown: `service ocieau stopservice ocie stopservice mysqld stop`

   When installed in a high-availability setup, stop the Unified Manager service by using either VCS Operations Manager or VCS commands.
3. Start Unified Manager in the order shown: `service mysqld startservice ocie startservice ocieau start`

   When installed in a high-availability setup, start Unified Manager service by using either VCS Operations Manager or VCS commands.

Removing Unified Manager from the Red Hat Enterprise Linux or CentOS host

If you need to remove Unified Manager from the Red Hat Enterprise Linux or CentOS host, you can stop and uninstall Unified Manager with a single command.

Before you begin

- 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 Red Hat machine. 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.
- The Unified Manager server must not have an active connection to an external data provider such as Graphite.

  If it does, you must delete the connection using the Unified Managermaintenance console.

About this task

These steps contain information for systems that are configured for high availability using Veritas Operation Manager. If your system is not configured for high availability, ignore these additional steps.

Steps

1. Log in as root user to the cluster node owning the cluster resources on which you want to remove Unified Manager.
2. Stop all Unified Manager services using VCS Operations Manager or VCS commands.
3. Stop and remove Unified Manager from the server: `rpm -e netapp-ocum ocie-au ocie-server netapp-platform-base netapp-application-server ocie-serverbase`

   This step removes all the associated NetApp RPM packages. It does not remove the prerequisite software modules, such as Java, MySQL, and p7zip.
4. Switch to the other node by using the VCS Operations Manager.
5. Log in to the second node of the cluster.
6. Stop all the services, and then and remove Unified Manager from the second node: `rpm -e netapp-ocum ocie-au ocie-server netapp-platform-base netapp-application-server ocie-serverbase`
7. Prevent the service group from using VCS Operations Manager or VCS commands.
8. 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`

Results

After this operation is complete, the software is removed; however, MySQL data is not deleted. All the data from the `/opt/netapp/data` directory is moved to the `/opt/netapp/data/BACKUP` folder after uninstallation.

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.

About this task

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