



OnCommand® Unified Manager 6.4

Installation and Setup Guide

For Red Hat® Enterprise Linux

February 2016 | 215-10952_A0
doccomments@netapp.com

Contents

Introduction to Unified Manager installation and setup on Red Hat Enterprise Linux	6
Integration of Performance Manager and Unified Manager	6
How Unified Manager works with Red Hat Enterprise Linux	7
Contents of the Unified Manager installation package for Red Hat Enterprise Linux	7
Functions that umadmin users can perform	8
What AutoSupport does	9
Requirements for Unified Manager on Red Hat Enterprise Linux	10
System requirements	10
Software requirements	11
Installation requirements	12
Requirements for Unified Manager in VCS	14
Installing Unified Manager on Red Hat Enterprise Linux	16
Creating a custom user home directory and umadmin password prior to installation	16
Downloading and installing OnCommand Unified Manager on a blank Red Hat Enterprise Linux system	17
Downloading and installing OnCommand Unified Manager on a partially configured Red Hat Enterprise Linux system	20
Downloading and installing OnCommand Unified Manager on a fully configured Red Hat Enterprise Linux system	24
Installing Unified Manager on VCS	27
Manually configuring the EPEL repository	28
Users created during Unified Manager installation	28
Configuring after installation	30
Configuring initial settings	30
Configuring your environment after initial setup	31
Configuring Unified Manager to send alert notifications	31
Configuring notification settings	32
Enabling remote authentication	32
Disabling nested groups from remote authentication	33
Adding authentication servers	34
Testing the configuration of authentication servers	35
Editing global threshold settings	35
Adding a user	37
Adding clusters	38
Adding an alert	39
Changing the umadmin password	40
Managing storage objects using the Favorites option	41
Adding storage objects to favorites list	42

Connecting Performance Manager and Unified Manager	42
Creating a user with Event Publisher role privileges	43
Configuring a full integration connection between a Performance Manager server and Unified Manager	43
Configuring a partial integration connection between a Performance Manager server and Unified Manager	45
Changing Unified Manager connection settings	46
Deleting a connection between a Performance Manager server and Unified Manager	47
Setting up a connection between OnCommand Workflow Automation and Unified Manager	47
Creating a database user	48
Setting up a connection between OnCommand Workflow Automation and Unified Manager	48
Setting up Unified Manager for high availability	50
Configuring Unified Manager server with VCS using configuration scripts	50
Configuring VCS with Unified Manager server service resources	51
Configuring an existing Unified Manager setup for high availability	52
Configuring backup and restore operations	54
What database backup is	54
Configuring database backup settings	54
What a database restore is	55
Restoring a database backup on Red Hat Enterprise Linux	55
Upgrading OnCommand Unified Manager	56
Upgrade overview of Unified Manager 6.3 on Red Hat Enterprise Linux	56
Downloading the Unified Manager software bundles	56
Upgrading to OnCommand Unified Manager 6.4 on Red Hat Enterprise Linux	57
Upgrading the host OS from Red Hat Enterprise Linux 6.x to 7.x	59
Unified Manager administrative operations	61
Stopping and starting Unified Manager in Red Hat Enterprise Linux	61
Changing the OnCommand Unified Manager host name in Red Hat Enterprise Linux	61
Removing Unified Manager from the Red Hat Enterprise Linux host	63
Generating a support bundle if OnCommand Unified Manager is installed on Red Hat Enterprise Linux	64
Adding disk space to the “data” directory of the Red Hat Enterprise Linux host	64
Moving content from /data to /opt/netapp/data after upgrading from Unified Manager 6.3	66
Removing the custom umadmin user and maintenance group	67
Changing the JBoss password	67
Troubleshooting Unified Manager Installation on Red Hat Enterprise Linux	69
Notification of nonsigned software packages during installation on Red Hat Enterprise Linux	69
Unified Manager installation terminates due to MySQL packages upgrade fail	69

Email notification of initial cron job failure at the end of the Unified Manager	
Red Hat Enterprise Linux installation operation can be disregarded	70
Maintenance user is not created during installation if noexec privilege is set	
in /tmp partition	70
Intermittent cluster connectivity issue	70
Copyright information	72
Trademark information	73
How to send comments about documentation and receive update	
notifications	74
Index	75

Introduction to Unified Manager installation and setup on Red Hat Enterprise Linux

You can install Unified Manager on both physical servers and virtual servers running Red Hat Enterprise Linux.

Unified Manager supports monitoring of clustered Data ONTAP 8.3.2, 8.3.1, 8.3.0, and 8.2.x systems. Unified Manager also supports features such as vaulting, nondisruptive operations, and Storage Virtual Machines (SVMs) with Infinite Volume.

If you configure a connection with a Performance Manager server, you can track the performance incidents discovered by that Performance Manager server from within the Unified Manager web UI.

If you pair Unified Manager with the Workflow Automation (WFA) server, you can enable automated SnapMirror and SnapVault-based data protection operations through Unified Manager.

Unified Manager can be run as a virtual appliance on a VMware ESXi server. For more information about this type of deployment, see the *OnCommand Unified Manager Installation and Setup Guide for VMware Virtual Appliances*.

For the most current compatibility information, see the Interoperability Matrix.

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 this 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 server. All of the Unified Manager server data must be configured for access from a shared data disk.

Related concepts

[*Installing Unified Manager on Red Hat Enterprise Linux*](#) on page 16

Related tasks

[*Connecting Performance Manager and Unified Manager*](#) on page 42

[*Setting up a connection between OnCommand Workflow Automation and Unified Manager*](#) on page 47

Related information

[*NetApp Interoperability Matrix Tool*](#)

[*OnCommand Unified Manager 6.3 Installation and Setup Guide for VMware Virtual Appliances*](#)

Integration of Performance Manager and Unified Manager

Performance Manager 2.0 and earlier has been able to report performance events to a connected Unified Manager server. This connection is called the “Partial Integration (Event Publishing only)” connection. This information enables administrators to monitor storage performance issues on Data ONTAP clusters through the Unified Manager web UI.

Unified Manager 6.4 and Performance Manager 2.1 and later are more tightly integrated than in previous versions. This connection is called the “Full Integration” connection. When connected in this fashion they share a management interface that provides the following improvements:

- Provides a single URL to manage both products.
- Displays cluster health and performance attributes through a central dashboard.
- Provides a single location to configure clusters, users, and authentication attributes that apply across both products.
- Avoids redundant and multiple logins when switching from one product to the other.
- Provides a favorites dashboard that enables fast access to storage objects that you reference frequently.

Note: The products are still installed individually on separate servers.

You can continue to install Unified Manager in a standalone configuration where it is not paired with Performance Manager.

How Unified Manager works with Red Hat Enterprise Linux

Red Hat Enterprise Linux is a commercial-grade operating system. It is one of the supported systems on which you can install and run Unified Manager to monitor and manage your clustered Data ONTAP storage domain.

The Red Hat Enterprise 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 Server or Microsoft Hyper-V. To install Unified Manager on Red Hat Enterprise Linux, you must first download and run Red Hat package manager modules (RPMs), which are the package formats most often used for installing software applications on the Red Hat OS.

Contents of the Unified Manager installation package for Red Hat Enterprise Linux

The Unified Manager download web page enables you to download two zipped bundles to install Unified Manager on Red Hat Enterprise Linux: an optional third-party-dependencies bundle, and the main Unified Manager bundle.

Contents of the Unified Manager bundle

The Unified Manager bundle includes all the modules necessary to install the Unified Manager software on top of the required vendor software not made by NetApp.

The contents of this zipped bundle include the following RPM modules and scripts:

- ocie-serverbase rpm
- ocie-server rpm
- ocie-au rpm
- netapp-node.rpm
- rp.rpm
- netapp-ocum rpm
- pre_install_check.sh
- upgrade.sh

Contents of the third-party-dependencies bundle

The third-party-dependencies bundle is a zipped file that contains packages for installing MySQL. The MySQL database software is necessary to support Unified Manager. If your Red Hat Enterprise Linux system is not already installed with the required MySQL software necessary to support a

Unified Manager installation, you can download and install the contents of this bundle to ensure a successful installation.

The contents of this bundle includes RPM packages for the following product:

- MySQL 5.6.28 Community Server (GPL) Edition

Related information

[*NetApp Support*](#)

Functions that umadmin users can perform

For each instance of Performance Manager or Unified Manager that is installed on Red Hat Enterprise Linux, an initial user, always named “umadmin”, is automatically created. The umadmin users access the Performance Manager web UI or the Unified Manager web UI after installation and from there perform configuration and management functions.

umadmin users and customized passwords

The name umadmin, whether created for Performance Manager or for Unified Manager, can never be changed; however, the password assigned to each umadmin user can and should be customized prior to installation, or immediately after installation.

For example, in a storage management infrastructure consisting of a Unified Manager server and two Performance Manager servers, access to the three objects might be configured as follows:

- The umadmin user with a password customized for Unified Manager access, such as “UMx9x947”, can log in as umadmin.
- The umadmin user with a password customized for Performance Manager server 1 access, such as “PMz8z831”, can log in as umadmin.
- The umadmin user with a password customized for Performance Manager server 2 access, such as “PMz468RT”, can log in as umadmin.

The umadmin user OnCommand Administrator role and maintenance user type

During an installation of Unified Manager or Performance Manager on a Red Hat Enterprise Linux machine, the associated umadmin user is assigned an OnCommand Administrator user role and configured as the maintenance user type. As such, each umadmin user can perform functions reserved for that role and that type.

Performance Manager umadmin user abilities

The Performance Manager umadmin user can perform the following functions:

- In the OnCommand Administrator role, the umadmin user can log in to the Performance Manager web UI and perform all of the performance monitoring and troubleshooting operations supported through that interface.
- As the maintenance user type, the umadmin user can perform the following operations:
 - Start the initial configuration of the Performance Manager web UI.
 - Access the Performance Manager maintenance console and perform all menu operations displayed through that interface, including configuring a connection between Performance Manager and Unified Manager.

Unified Manager umadmin user abilities

The Unified Manager umadmin user can perform the following functions:

- As the OnCommand Administrator, log in to the Unified Manager web UI and perform all of the monitoring and configuration operations supported through that interface.
- As the sole user assigned the maintenance user type, the umadmin user alone is authorized to start the initial configuration of Unified Manager.

What AutoSupport does

With the help of the AutoSupport feature, Unified Manager sends information to technical support to help with troubleshooting. AutoSupport messages are scanned for potential problems and are available to technical support when they assist you in resolving issues.

Requirements for Unified Manager on Red Hat Enterprise Linux

To ensure successful installation of Unified Manager on Red Hat Enterprise Linux, you must confirm that the system on which Unified Manager is being installed meets certain system and software requirements.

System requirements

The Red Hat Enterprise Linux system on which you install Unified Manager must meet or exceed the specific required capabilities.

Hardware requirements

The following capabilities and capacities must be reserved to support Unified Manager.

These requirements must be observed whether the target machine is a virtual machine running on VMware ESXi or Microsoft Hyper-V, or a physical machine.

Hardware configuration	Minimum requirement
Reserved free hard disk space	<p>150 GB, where the capacity is allotted as follows:</p> <ul style="list-style-type: none"> 50 GB allotted to the root partition of the target system 100 GB of free disk space allotted to the <code>/opt/netapp/data</code> directory, which is mounted on an LVM drive on or on a separate local disk attached to the target system <p>Important: Mounting <code>/opt/netapp/data</code> on an NFS or CIFS share is not supported.</p>
Reserved RAM	<p>16 GB for JBoss, MySQL, and Acquisition unit.</p> <p>Note: Red Hat recommends that systems with 16 GB to 64 GB of RAM require a minimum swap space of 4 GB.</p>
Reserved CPU cycle capacity	9572 MHz

This configuration enables you to use a Red Hat Enterprise Linux machine with a smaller root partition and also enables you to expand the `/opt/netapp/data` directory if required later.

Note: Unified Manager 6.3 and earlier required disk space in `/data` instead of `/opt/netapp/data`. Therefore, when performing an upgrade to Unified Manager 6.4 or later, the necessary disk space must be available in `/data`.

In addition to these free space requirements, the `/tmp` directory must be a minimum of 15 GB.

Note: If the Red Hat Enterprise Linux target machine has a preexisting configuration in which the `/opt` directory and `/var/log` directory are mounted on a separate partition, at least 5 GB must be allocated to the `/opt` directory and 15 GB allocated to the `/var/log` directory in addition to the required allocations for the root directory and the `/opt/netapp/data` directory.

Host connectivity requirements

The Red Hat Enterprise Linux physical or virtual system on which you install Unified Manager must be FQDN-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, the host name should be taken from the DNS.

User authorization requirements

Installation of Unified Manager on a Red Hat Enterprise Linux system can be performed by the root user, or by nonroot users using the `sudo` command.

License requirements

No special licenses are required to install Unified Manager on Red Hat Enterprise Linux.

Dedicated use requirement

The Red Hat Enterprise Linux physical or virtual system on which you install Unified Manager must be used exclusively for Unified Manager and not shared with other applications. Other applications will consume system resources and can drastically reduce the performance of Unified Manager.

Important: This restriction includes Performance Manager. Performance Manager cannot be installed on the same Red Hat Enterprise Linux server on which you are installing Unified Manager.

Software requirements

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

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

- Operating system
 - Red Hat Enterprise Linux version 6.6, 6.7, 7.0, or 7.1 (64-bit)
- Third-party software
 - MySQL Community Edition 5.6.28, or later
This version must be supplied by Oracle Corporation (by selecting the “Linux - Generic” version) or by the downloaded third-party-dependencies bundle.
 - Oracle JRE 1.8.0.71, or later (from the Third Party Oracle Java repository)
 - p7zip 9.20.1, or later (from the Extra Packages for Enterprise Linux repository)
 - rrd tool and libraries 1.3.8, or later (from the RHEL repository)

Installation requirements

The recommended practices for installing Red Hat Enterprise Linux and its repositories on your system are as follows:

- You must install Red Hat Enterprise Linux according to Red Hat best practices, and you should select the following default options:

- For Red Hat Enterprise Linux 6.x, select “Basic Server” and “Red Hat Enterprise Linux” repository
- For Red Hat Enterprise Linux 7.x, select “Server with GUI”
- The system must have Red Hat Enterprise Linux repository access so that the installation program can access and install all 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, using a valid Red Hat subscription.
See the Red Hat documentation for information about the Red Hat Subscription Manager.
- You should enable the Red Hat Enterprise Linux Extra Packages for Enterprise Linux (EPEL) repository to successfully install required third-party utilities on your system.
If your system does not have the EPEL repository configured, you can manually download and configure the particular repository. [Manually configuring the EPEL repository](#) on page 28
- If you do not have the required MySQL software installed, you can download and install the software from the third-party-dependencies bundle supplied from NetApp.
- If you do not have the Oracle JRE software installed, you should enable the Third Party Oracle Java repository so that the installation program downloads and installs the required JRE software on your system.

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 your systems' external software dependencies. Then you can download the required software to the Internet-connected system and copy the .rpm files to the system where you plan to install Unified Manager. Ensure that the two systems are running the same operating system versions (6.x or 7.x) and that the subscription license is for the appropriate Red Hat version.

o not install required third-party software from repositories other than those mentioned here. Software installed from the RHEL 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 may not follow these guidelines. This could cause the Unified Manager installation to fail, or cause issues with future upgrades.

Installation requirements

To ensure the successful installation of OnCommand Unified Manager on Red Hat Enterprise Linux, you must ensure that the system on which Unified Manager is being installed meets the browser, platform, protocol, and software requirements.

Supported browsers

- Microsoft Internet Explorer version 11 and Edge
- Google Chrome version 45 and 47
- Mozilla Firefox version 42, 43 (and ESR 38)
- Apple Safari version 9

Supported browser client platforms

- Windows Vista, Windows 7, Windows 8, and Windows 10
- Red Hat Enterprise Linux version 6
- SUSE Linux Enterprise Server version 11 SP2
- Macintosh OS X 10.10 or later

Protocol and port requirements

When using a browser, API client, or SSH, the required ports must be accessible to the Unified Manager UI and APIs. The 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

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 runs on its default port, you can enter `https://host` instead of `https://host:443`. The default port numbers cannot be changed.

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.
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.
Red Hat Enterprise Linux command line	SSH/SFTP	22	Used to access the Red Hat Enterprise Linux command line and to retrieve support bundles.
MySQL database	MySQL	3306	Used to enable access for OnCommand Workflow Automation and OnCommand Report to Unified Manager.
Syslog	UDP	514	Used to listen to and access EMS messages from Data ONTAP clusters and to create events based on the messages. Currently, only MetroCluster configuration events use this interface.
Unified Manager web UI and Reverse Proxy	TCP/IP	2043	Used by Unified Manager to listen to the reverse proxy.
Unified Manager web UI and Reverse Proxy	TCP/IP	8443	Used by the reverse proxy to listen to the port.

Connections from the Unified Manager server

You must configure your firewall to open the ports that enable communication between the Unified Manager server and the 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 for connecting to specific destinations.

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

Destination	Protocol	Port	Description
Storage system	HTTPS	443	Used to monitor and manage storage systems.

Destination	Protocol	Port	Description
AutoSupport server	HTTPS	443	Used to send AutoSupport information (requires Internet access).
Authentication server	LDAP	389	Used to make authentication requests, as well as user and group lookup requests.
	LDAPS	636	Used for secure 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.

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.
- 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.
- OnCommand 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 5.2.2 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.

Related tasks

[Installing Unified Manager on VCS](#) on page 27

Related information

[SnapDrive 5.3 for UNIX Administration Guide for Linux](#)

[SnapDrive 5.3 for UNIX Installation and Setup Guide for Linux for Clustered Data ONTAP](#)

[NetApp Interoperability Matrix Tool](#)

Installing Unified Manager on Red Hat Enterprise Linux

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

Related tasks

[Installing Unified Manager on VCS](#) on page 27

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 be running Red Hat Enterprise Linux 6.5, 6.6, 7.0, or 7.1.
- You must be able to log in as the root user to the Red Hat Enterprise Linux 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.

Steps

1. Log in as the root user to the Red Hat Enterprise Linux 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 --shell /bin/maintenance-user-shell.sh --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.

Downloading and installing OnCommand Unified Manager on a blank Red Hat Enterprise Linux system

If you want to install Unified Manager on a Red Hat Enterprise Linux platform that is not yet installed with the Java packages, MySQL packages, or utilities necessary to support the installation, you can download zipped bundles that enable you to automatically install Unified Manager and all the additional modules and utilities necessary to support it.

Before you begin

- The system on which you want to install Unified Manager must meet the system and software requirements. [System requirements](#) on page 10 and [Software requirements](#) on page 11.
- You must have login credentials for the NetApp Support Site.
- You must have a supported Internet browser.
- Your terminal emulation software must have scrollbar enabled.

About this task

In this context, a blank Red Hat Enterprise Linux system has a supported version of Red Hat Enterprise Linux installed, but it does not have any of the required supporting software (Java, MySQL, additional utilities) installed.

Steps

1. Navigate to the NetApp Support Site at mysupport.netapp.com, and locate the Download pages for installing Unified Manager on the Red Hat Enterprise Linux platform.
2. Download the Unified Manager bundle (OnCommandUnifiedManager-6.4.zip) to a target directory on the target Red Hat Enterprise Linux system.
3. Download the third-party-dependencies bundle to the same directory on the target Red Hat Enterprise Linux system.

Download `thirdpartydependencies-6.4-rhel6.zip` for Red Hat 6 systems or `thirdpartydependencies-6.4-rhel7.zip` for Red Hat 7 systems.
4. Log in to the target Red Hat Enterprise Linux system.
5. Navigate to the target directory and expand the third-party-dependencies bundle.

Example

```
unzip thirdpartydependencies-6.4-rhel7.zip
```

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

6. Still in the target directory, expand the Unified Manager bundle:

```
unzip OnCommandUnifiedManager-6.4.zip
```

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

7. Confirm the presence of the following modules:

```
ls *.rpm
```

- MySQL Community Edition rpms:
 MySQL-client-5.6.28-1.el6.x86_64.rpm (Red Hat 6 only)
 MySQL-server-5.6.28-1.el6.x86_64.rpm (Red Hat 6 only)
 MySQL-shared-compat-5.6.28-1.el6.x86_64.rpm (Red Hat 6 only)
 MySQL-client-5.6.28-1.el7.x86_64.rpm (Red Hat 7 only)
 MySQL-server-5.6.28-1.el7.x86_64.rpm (Red Hat 7 only)
 MySQL-shared-compat-5.6.28-1.el7.x86_64.rpm (Red Hat 7 only)
 - ocie-serverbase rpm:
 ocie-serverbase-<version>.x86_64.rpm
 - ocie-server rpm:
 ocie-server-<version>.x86_64.rpm
 - ocie-au rpm:
 ocie-au-<version>.x86_64.rpm
 - netapp-node rpm:
 node-<version>.x86_64.rpm
 - rp rpm:
 rp-<version>.x86_64.rpm
 - netapp-ocum rpm
 netapp-ocum-<version>.x86_64.rpm
8. Enter the appropriate command to enable the Third Party Oracle Java repository so that the correct JRE software is installed:

If you are using...	Enter this command...
Red Hat 6 systems	subscription-manager repos --enable rhel-6-server-thirdparty-oracle-java-rpms
Red Hat 7 systems	subscription-manager repos --enable rhel-7-server-thirdparty-oracle-java-rpms

These commands require that you have a subscription to the Red Hat Enterprise Linux Subscription Manager.

9. Ensure that there are no system configuration settings or installed software that will conflict with the Unified Manager installation:

```
pre_install_check.sh
```

If the script identifies any issues, you must fix the issues before installing Unified Manager.

Note: You must perform [step 10](#) on page 18 *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 11](#) on page 19.

10. Optional: 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. On the system where you plan to install Unified Manager, view the list of available and unavailable packages:

If you are using...	Enter this command...
Red Hat 6 systems	yum install *.rpm Answer “no” to the prompt about installing each package, and note the names of the packages that are not available in the current directory.
Red Hat 7 systems	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 --downloadaddr=.
```

Note: 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.

11. Install the software:

```
yum install *.rpm
```

This command automatically executes the RPM modules, installing the necessary supporting software and the Unified Manager modules that run on top of them.

Important: Do not attempt installation by using alternative commands (such as `rpm -ivh ...`). Successful installation of Unified Manager on Red Hat Enterprise Linux requires that all Unified Manager files and related files be installed in a specific order into a specific directory structure that are executed and configured automatically by the `yum install *.rpm` command.

12. 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.

13. After the installation messages are complete, scroll back 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 is successfully installed on the computer.
The following login username and password are configured for the
OnCommand Unified Manager GUI:
    username: umadmin
    password: admin
To change the default password, use the command: passwd umadmin.

https://default_ip_address
or
https://default_url
```

14. Change the umadmin user password from the default “admin” string to a personalized string by using the `passwd umadmin` command.

Note: If you defined a custom umadmin user password prior to installing the software, you do not need to change the password now.

15. Record the IP address or URL, the assigned user name (umadmin), and current password.

16. Block access to non-essential open ports.

The following ports, which are opened during the installation process, are no longer necessary. For security purposes, these ports should be blocked from user access by firewall or other means with no impairment to Unified Manager functions.

- 1090
Used as the RMI/JRMP socket for connecting to the JMX MBeanServer
- 1091
Used as the RMI server socket
- 1098
Used by the Socket Naming service to receive RMI requests from client proxies
- 1099
Used as the listening socket for the Naming service
- 4446
Used as JBoss Remoting Connector by UnifiedInvoker
- 5500
Used for clear/non-SSL Remoting connections

After you finish

Enter the specified IP address or URL into a supported web browser to start the Unified Manager web UI and begin initial configuration.

Related concepts

[Functions that umadmin users can perform](#) on page 8

Related references

[Requirements for Unified Manager on Red Hat Enterprise Linux](#) on page 10

Related information

[NetApp Support](#)

Downloading and installing OnCommand Unified Manager on a partially configured Red Hat Enterprise Linux system

If you want to install Unified Manager on a physical or virtual Red Hat Enterprise Linux platform that is only partially configured with the necessary Java packages, MySQL packages, and utilities, you can download zipped bundles that enable you to automatically install Unified Manager and upgrade all the third-party modules and utilities necessary to support it.

Before you begin

- The system on which you want to install Unified Manager must meet system and software requirements. [System requirements](#) on page 10 and [Software requirements](#) on page 11.
- You must have login credentials for the NetApp Support Site.
- You must have a supported web browser.

- Your installation of Red Hat Enterprise Linux must have some version of the following additional software packages installed:
 - Oracle JRE 1.8.0.71
 - MySQL 5.6.28 Community Edition
 - p7zip 9.20.1
 - rrd tool 1.3.8
- Your terminal emulation software must have scrollback enabled.

About this task

In this context, a Red Hat Enterprise Linux system is *partially configured* if it has Red Hat Enterprise Linux installed but does not have all required versions of the required supporting software (Java, MySQL, additional utilities) installed.

Steps

1. Log in to the Red Hat Enterprise Linux server on which you want to install Unified Manager and enter the appropriate commands to assess what software might require installation or upgrade on the target system to support installation:

Required software and version	Command to verify software and version
Oracle JRE 1.8.0_71	<code>java -version</code>
MySQL 5.6.28 Community Edition	<code>rpm -qa grep -i mysql</code>
p7zip 9.20.1	<code>rpm -qa grep p7zip</code>
rrdtool-1.3.8-1.el6.wrl.x86_64 rrdtool-perl-1.3.8-1.el6.wrl.x86_64	<code>rpm -qa grep rrd</code>

2. 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 5.6.28 Community Edition and not supplied by Oracle Corporation or with the third-party-dependencies bundle)	<code>rpm -e mysql_package_name</code> Note: If you receive dependency errors, you must add the <code>--nodeps</code> option to uninstall the component.
All other modules	<code>yum remove module_name</code>

3. Navigate to the NetApp Support Site at mysupport.netapp.com, and locate the Download pages for installing Unified Manager on the Red Hat Enterprise Linux platform.
4. Download the Unified Manager bundle (`OnCommandUnifiedManager-6.4.zip`) to a target directory on the target Red Hat Enterprise Linux system.
5. Download the third-party-dependencies bundle to the same directory on the target Red Hat Enterprise Linux system.

Download `thirdpartydependencies-6.4-rhel6.zip` for Red Hat 6 systems or `thirdpartydependencies-6.4-rhel7.zip` for Red Hat 7 systems.
6. Navigate to the target directory and expand the third-party-dependencies bundle.

Example

```
unzip thirdpartydependencies-6.4-rhel7.zip
```

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

7. Still in the target directory, expand the Unified Manager bundle:

```
unzip OnCommandUnifiedManager-6.4.zip
```

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

8. Confirm the presence of the following modules:

```
ls *.rpm
```

- MySQL Community Edition rpms:
 MySQL-client-5.6.28-1.el6.x86_64.rpm (Red Hat 6 only)
 MySQL-server-5.6.28-1.el6.x86_64.rpm (Red Hat 6 only)
 MySQL-shared-compat-5.6.28-1.el6.x86_64.rpm (Red Hat 6 only)
 MySQL-client-5.6.28-1.el7.x86_64.rpm (Red Hat 7 only)
 MySQL-server-5.6.28-1.el7.x86_64.rpm (Red Hat 7 only)
 MySQL-shared-compat-5.6.28-1.el7.x86_64.rpm (Red Hat 7 only)
- ocie-serverbase rpm:
 ocie-serverbase-<version>.x86_64.rpm
- ocie-server rpm:
 ocie-server-<version>.x86_64.rpm
- ocie-au rpm:
 ocie-au-<version>.x86_64.rpm
- netapp-node rpm:
 node-<version>.x86_64.rpm
- rp rpm:
 rp-<version>.x86_64.rpm
- netapp-ocum rpm
 netapp-ocum-<version>.x86_64.rpm

9. Enter the appropriate command to enable the Third Party Oracle Java repository so that the correct JRE software is installed:

If you are using...	Enter this command...
Red Hat 6 systems	subscription-manager repos --enable rhel-6-server-thirdparty-oracle-java-rpms
Red Hat 7 systems	subscription-manager repos --enable rhel-7-server-thirdparty-oracle-java-rpms

These commands require that you have a subscription to the Red Hat Enterprise Linux Subscription Manager.

10. 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
```

If the script identifies any issues, fix the issues prior to installing Unified Manager.

Note: You must perform [step 11](#) on page 23 *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 12](#) on page 23.

11. Optional: 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. On the system where you plan to install Unified Manager, view the list of available and unavailable packages:

For...	Enter this command...
Red Hat 6 systems	yum install *.rpm Answer “no” to the prompt about installing each package, and note the names of the packages that are not available in the current directory.
Red Hat 7 systems	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 --downloadaddir=.
```

Note: 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.

12. Install the software:

```
yum install *.rpm
```

This command automatically executes the RPM modules, installing the necessary third-party systems and the Unified Manager modules that run on top of them.

Important: Do not attempt installation by using alternative commands (such as `rpm -ivh ...`). Successful installation of Unified Manager on Red Hat Enterprise Linux requires that all Unified Manager files and related files be installed in a specific order into a specific directory structure that are executed and configured automatically by the `yum install *.rpm` command.

13. 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.

14. After the installation messages are complete, scroll back 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 is successfully installed on the computer.
The following login username and password are configured for the
OnCommand Unified Manager GUI:
  username: umadmin
  password: admin
To change the default password, use the command: passwd umadmin.
```

```
https://default_ip_address
or
https://default_url
```

15. Change the umadmin user password from the default “admin” string to a personalized string by using the `passwd umadmin` command.

Note: If you defined a custom umadmin user password prior to installing the software, you do not need to change the password now.

16. Record the IP address or URL, the assigned user name (umadmin), and current password.
17. Block access to non-essential open ports.

The following ports, which are opened during the installation process, are no longer necessary. For security purposes, these ports should be blocked from user access by firewall or other means with no impairment to Unified Manager functions.

- 1090
Used as the RMI/JRMP socket for connecting to the JMX MBeanServer
- 1091
Used as the RMI server socket
- 1098
Used by the Socket Naming service to receive RMI requests from client proxies
- 1099
Used as the listening socket for the Naming service
- 4446
Used as JBoss Remoting Connector by UnifiedInvoker
- 5500
Used for clear/non-SSL Remoting connections

After you finish

Enter the specified IP address or URL into a supported web browser to start the Unified Manager web UI and begin initial configuration.

Related concepts

[Functions that umadmin users can perform](#) on page 8

Related references

[Requirements for Unified Manager on Red Hat Enterprise Linux](#) on page 10

Related information

[NetApp Support](#)

Downloading and installing OnCommand Unified Manager on a fully configured Red Hat Enterprise Linux system

If you want to install Unified Manager on a physical or virtual Red Hat Enterprise Linux platform that is already fully configured with the necessary Java packages, MySQL packages, and utilities,

you can download a single zipped bundle that enables you to automatically install Unified Manager on that platform.

Before you begin

- The system on which you want to install Unified Manager must meet system and software requirements. [System requirements](#) on page 10 and [Software requirements](#) on page 11.
- You must have login credentials for the NetApp Support Site.
- You must have a supported web browser.
- Your installation of Red Hat Enterprise Linux must have the following additional software installed:
 - Oracle JRE 1.8.0_71
 - MySQL 5.6.28 Community Edition
 - p7zip 9.20.1
 - rrd tool 1.3.8
- Your terminal emulation software must have scrollback enabled.

About this task

In this context, a Red Hat Enterprise Linux system is *fully configured* if it has Red Hat Enterprise Linux installed and has all the required versions of the required additional software already installed.

Steps

1. Log in to the Red Hat Enterprise Linux server on which you want to install Unified Manager and enter the appropriate commands to verify that the target system has the Java and MySQL versions and utilities required to support installation of Unified Manager.

Required software and version	Command to verify software and version
Oracle JRE 1.8.0_71	<code>java -version</code>
MySQL 5.6.28 Community Edition	<code>rpm -qa grep -i mysql</code>
p7zip 9.20.1	One of the following commands: <ul style="list-style-type: none"> • <code>rpm -qa grep p7zip</code> • <code>p7zip-9.20.1-8.1.1.x86_64</code>
rrdtool-1.3.8-1.el6.wrl.x86_64 rrdtool-perl-1.3.8-1.el6.wrl.x86_64	<code>rpm -qa grep rrd</code>

Note: If the required versions of software are not installed, see the task titled [Downloading and installing Unified Manager on a partially configured Red Hat Enterprise Linux system](#) on page 20.

2. Navigate to the NetApp Support Site at mysupport.netapp.com, and locate the Download pages for installing Unified Manager on the Red Hat Enterprise Linux platform.
3. Download the Unified Manager bundle (OnCommandUnifiedManager-6.4.zip) to a target directory on the target Red Hat Enterprise Linux system.
4. Navigate to the target directory and expand the Unified Manager bundle:


```
unzip OnCommandUnifiedManager-6.4.zip
```

The required OnCommand RPM modules are unzipped to the target directory.

5. Confirm the presence of the following modules:

```
ls *.rpm
```

- ocie-serverbase rpm:
ocie-serverbase-<version>.x86_64.rpm
- ocie-server rpm:
ocie-server-<version>.x86_64.rpm
- ocie-au rpm:
ocie-au-<version>.x86_64.rpm
- netapp-node rpm:
node-<version>.x86_64.rpm
- rp rpm:
rp-<version>.x86_64.rpm
- netapp-ocum rpm
netapp-ocum-<version>.x86_64.rpm

6. 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
```

If the script identifies any issues, fix the issues prior to installing Unified Manager.

7. Install the software:

```
yum install *.rpm
```

This command automatically executes the RPM modules, installing the Unified Manager modules.

Important: Do not attempt installation by using alternative commands (such as rpm -ivh ...). Successful installation of Unified Manager on Red Hat Enterprise Linux requires that all Unified Manager files and related files be installed in a specific order into a specific directory structure that are executed and configured automatically by the `yum install *.rpm` command.

8. 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.

9. After the installation messages are complete, scroll back 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 is successfully installed on the computer.
The following login username and password are configured for the
OnCommand Unified Manager GUI:
    username: umadmin
    password: admin
To change the default password, use the command: passwd umadmin.

https://default_ip_address
or
https://default_url
```

10. Change the umadmin user password from the default “admin” string to a personalized string by running the `passwd umadmin` command.

Note: If you defined a custom umadmin user password prior to installing the software, you do not need to change the password now.

11. Record the IP address or URL, the assigned user name (umadmin), and current password.
12. Block access to non-essential open ports.

The following ports, which are opened during the installation process, are no longer necessary. For security purposes, these ports should be blocked from user access by firewall or other means with no impairment to Unified Manager functions.

- 1090
Used as the RMI/JRMP socket for connecting to the JMX MBeanServer
- 1091
Used as the RMI server socket
- 1098
Used by the Socket Naming service to receive RMI requests from client proxies
- 1099
Used as the listening socket for the Naming service
- 4446
Used as JBoss Remoting Connector by UnifiedInvoker
- 5500
Used for clear/non-SSL Remoting connections

After you finish

Enter the specified IP address or URL into a supported web browser to start the Unified Manager web UI and begin initial configuration.

Related references

[Requirements for Unified Manager on Red Hat Enterprise Linux](#) on page 10

Related information

[NetApp Support](#)

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 6.1.1 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](#) on page 16
3. Repeat steps 1 and 2 on the second node of the cluster.

Related concepts

[Requirements for Unified Manager in VCS](#) on page 14

Related information

[Symantec Documentation](#)

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.

Steps

1. Download the appropriate EPEL repository for your installation:

If you are using...	Enter this command...
Red Hat 6 systems	<code>wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm</code>
Red Hat 7 systems	<code>wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm</code>

2. Configure the EPEL repository:

If you are using...	Enter this command...
Red Hat 6 systems	<code>yum install epel-release-latest-6.noarch.rpm</code>
Red Hat 7 systems	<code>yum install epel-release-latest-7.noarch.rpm</code>

Users created during Unified Manager installation

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

umadmin

Used to log in to Unified Manager for the first time. 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.

rrdcache

Uses the rrdtool to collect Unified Manager health data. This user is created by the rrdtool third-party utility.

cliadmin

Used to authenticate and enable the user to run Unified Manager commands for scripts associated with alerts. The cliadmin user is created during installation of Unified Manager.

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

Note: If you created your own 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.

Configuring after installation

After installation of the software is complete, you can log in to the web UI as the default user `umadmin`, and complete an initial setup to configure a minimum software configuration. You can then configure additional options, such as adding email alerts, adding users, changing the passwords, and adding clusters you want to monitor.

Because the default user `umadmin` is assigned the OnCommand Administrator user role, that user has authorization to perform any configuration task that is possible through the web UI.

Configuring initial settings

After the installation of Unified Manager on Red Hat Enterprise Linux is completed, you can access the Unified Manager web UI to configure initial details about the `umadmin` user and the cluster that user is to manage and monitor.

Before you begin

- At the end of Unified Manager installation on the target Red Hat Enterprise Linux system, you must have obtained the following information:
 - An IP address or URL at which to access the login window to Unified Manager web UI
 - An assigned user name (`umadmin`)
 - A password for the user `umadmin`
- You must be able to specify the following maintenance user information:
 - An email address at which the user `umadmin` can receive email alerts and AutoSupport messages
 - The host name of the associated SMTP mail server
- If you want to specify a cluster for Unified Manager to manage and monitor, you must have the following information available about that cluster:
 - Host name or cluster management IP address

The host name is the FQDN or short name that Unified Manager uses to connect to the cluster. This host name must resolve to the cluster-management IP address.

The cluster-management IP address must be the cluster-management LIF of the admin Storage Virtual Machine (SVM). If you use a node-management LIF, the operation fails.
 - The type of protocol (HTTP or HTTPS) that can be configured on the cluster and the port number of the cluster
 - The port number of the cluster

Steps

1. Use a web browser to log in to the Unified Manager web UI, using the IP address (IPv4 or IPv6) or URL, the `umadmin` user name, and password that you assigned to `umadmin` during the installation procedure.
2. In the Unified Manager **Initial Setup** dialog box, choose **Yes** to enable AutoSupport capabilities, and click **Continue**.

While enabling AutoSupport is a best practice, it is not mandatory. If you do not enable AutoSupport when configuring the initial setup, you can enable it later using the Setup Options dialog box.

3. Type an email address for umadmin, the SMTP server host name, and any additional SMTP options, and click **Save**.
4. In the **Get Started** area, click **Add Cluster** to add clusters for monitoring.
Adding a cluster enables Unified Manager to monitor your cluster components, but alert notifications are not sent until they are configured.

After you finish

If you choose not to add clusters while configuring initial settings, you can configure additional options, such as alerts and thresholds, and then add clusters for monitoring.

Configuring your environment after initial setup

After you perform initial setup of the software, there are several configuration tasks that you might want to perform before you start monitoring your clusters, such as adding users, enabling user authentication, and adding alerts.

Configuring Unified Manager to send alert notifications

You can configure Unified Manager to send notifications that alert you about events in your environment. Before notifications can be sent, you must configure several other Unified Manager options.

Before you begin

You must have the OnCommand Administrator role.

About this task

After deploying Unified Manager and completing the initial configuration, you should consider configuring your environment to trigger alerts and generate notification emails or SNMP traps.

Steps

1. [Configure notification settings](#) on page 32
If you want alert notifications sent when certain events occur in your environment, you must supply an email address from which the alert notification can be sent. If your configuration uses an SMTP server for email authentication, then you must provide the user name and password for the server. If you want to use SNMP traps, you can select that option and provide the necessary information.
2. [Enable remote authentication](#) on page 32
If you want remote LDAP or Active Directory users to access the Unified Manager instance and receive alert notifications, then you must enable remote authentication.
3. [Add authentication servers](#) on page 34
If you enable remote authentication, then you must identify authentication servers.
4. [Edit global threshold settings](#) on page 35
You can modify the threshold settings for aggregates, volumes, and certain types of protection relationships. These settings determine when an event should be generated, which can affect when an alert notification is sent.

5. [Add users](#) on page 37

You can add several different types of local or remote users and assign specific roles. When you create an alert, you assign a user to receive the alert notifications.

6. [Add alerts](#) on page 39

After you have added the email address for sending notifications, added users to receive the notifications, configured your network settings, and configured SMTP and SNMP options needed for your environment, then you can assign alerts.

Related concepts

[What AutoSupport does](#) on page 9

Configuring notification settings

You can configure the settings for the Unified Manager server to send alert notifications when an event is generated or when it is assigned to a user. You can configure the corresponding mail server to be used and various notification mechanisms—for example, alert notifications can be sent as emails or SNMP traps.

Before you begin

The following information must be available:

- Email address from which the alert notification is sent
- Host name, user name, password, and default port to configure the SMTP server
- SNMP version, trap destination host, outbound trap port, and community to configure the SNMP trap

You must have the OnCommand Administrator or Storage Administrator role.

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **General Settings > Notification**.
3. Configure the appropriate settings.

You can specify the email address and SMTP server from which the alert notifications are sent, and enter the SNMP trap settings.

Tip: If the host name of the SMTP server cannot be resolved, you can specify the IP address of the SMTP server instead of the host name.

Enabling remote authentication

You can enable remote authentication, using either Open LDAP or Active Directory, so that the management server can communicate with your authentication servers and so that users of the authentication servers can use Unified Manager to manage the storage objects and data.

Before you begin

You must have the OnCommand Administrator role.

About this task

If remote authentication is disabled, remote users or groups can no longer access Unified Manager.

The only two supported remote authentication methods are Active Directory and Open LDAP. LDAPS is not supported.

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Management Server > Authentication**.
3. Select **Enable Remote Authentication**.
4. In the Authentication Service field, select either **Active Directory** or **Open LDAP**.

If you are using Active Directory as the authentication service, enter the following information:

- Authentication server administrator name (using one of following formats):
 - *domainname\username*
 - *username@domainname*
 - *Bind Distinguished Name* (using appropriate LDAP notation)
- Administrator password
- Base distinguished name (using the appropriate LDAP notation)

If you are using Open LDAP as the authentication service, you can enter the following information:

- Bind distinguished name (using appropriate LDAP notation)
- Bind password
- Base distinguished name

If authentication of an Active Directory user takes a long time or times out, the authentication server is probably taking a long time to respond. Disabling support for nested groups in Unified Manager might reduce the authentication time.

5. Optional: Add authentication servers and test the authentication.
6. Click **Save and Close**.

Disabling nested groups from remote authentication

If you have remote authentication enabled, you can disable nested group authentication so that only individual users and not group members can remotely authenticate to Unified Manager. You might disable nested groups when you want to improve Active Directory authentication response time.

Before you begin

You must be logged in as an Active Directory domain user to perform this task. Logging in as an Active Directory administrator is not required.

About this task

Disabling support for nested groups in Unified Manager might reduce the authentication time. If nested group support is disabled and if a remote group is added to Unified Manager, individual users must be members of the remote group to authenticate to Unified Manager.

Steps

1. Click **Administration > Setup Options**.

2. In the **Setup Options** dialog box, click **Management Server > Authentication**.
3. In the **Authentication Service** field, select **Others**.
4. In the **Member** field, change the member information from member:1.2.840.113556.1.4.1941: to member.
5. Click **Save and Close**.

Adding authentication servers

You can add authentication servers and enable remote authentication on the management server to enable remote users within the authentication server to access Unified Manager.

Before you begin

- The following information must be available:
 - Host name or IP address of the authentication server
 - Port number of the authentication server
- You must have enabled remote authentication and configured your authentication service so that the management server can authenticate remote users or groups in the authentication server.
- You must have the OnCommand Administrator role.

About this task

If the authentication server that you are adding is part of a high-availability pair (using the same database), you can also add the partner authentication server. This enables the management server to communicate with the partner when one of the authentication servers is unreachable.

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Management Server > Authentication**.
3. In the Servers area, click **Add**.
4. In the **Add Authentication Server** dialog box, specify either the host name or IP address of the server, and the port details.
5. Click **Add**.

Result

The authentication server that you added is displayed in the Servers area.

After you finish

Perform a test authentication to confirm that you are able to authenticate users in the authentication server that you added.

Testing the configuration of authentication servers

You can validate the configuration of your authentication servers to ensure that the management server is able to communicate with them. You can validate by searching for a remote user or group from your authentication servers and authenticate them using the configured settings.

Before you begin

- You must have enabled remote authentication and configured your authentication service so that the OnCommand Unified Manager server can authenticate the remote user or group.
- You must have added your authentication servers so that the management server can search for the remote user or group from these servers and authenticate them.
- You must be assigned the OnCommand Administrator role to perform this task.

About this task

If the authentication service is set to Active Directory and if you are validating the authentication of remote users who belong to the primary group of the authentication server, information about the primary group is not displayed in the authentication results.

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Management Server > Authentication**.
3. In the **Authentication Setup Options** dialog box, click **Test Authentication**.
4. In the **Test User** dialog box, specify the user name and password of the remote user or group, and then click **Test**.

If you are authenticating a remote group, you must not enter the password.

Editing global threshold settings

You can configure global threshold conditions for capacity, growth, Snapshot reserve, quotas, and inodes to monitor your aggregate and volume size effectively. You can also edit the settings for generating events for exceeding lag thresholds.

About this task

Global threshold settings apply to all objects with which they are associated, such as aggregates, volumes, and so forth. When thresholds are crossed, an event is generated and, if alerts are configured, an alert notification is sent. Threshold defaults are set to recommended values, but you can modify them to generate events at intervals to meet your specific needs. When thresholds are changed, events are generated or obsoleted in the next monitoring cycle.

Global threshold settings are accessible from the Setup Options dialog box. You can also modify threshold settings for individual objects, from the inventory page or the details page for that object.

Choices

- [Configuring global aggregate threshold values](#) on page 36

You can edit the threshold settings for capacity, growth, and Snapshot copies for all aggregates to track any threshold breach.

- [Configuring global volume threshold values](#) on page 36

You can edit the threshold settings for capacity, Snapshot copies, quotas, volume growth, overwrite reserve space, and inodes for all volumes to track any threshold breach.

- [Editing unmanaged relationship lag thresholds](#) on page 37

You can increase or decrease the warning or error lag time percentage so that events are generated at intervals that are more appropriate to your needs.

Configuring global aggregate threshold values

You can configure global threshold values for all aggregates to track any threshold breach. Appropriate events are generated for threshold breaches and you can take preventive measures based on these events. You can configure the global values based on the best practice settings for thresholds that apply to all monitored aggregates.

Before you begin

You must have the OnCommand Administrator or Storage Administrator role.

About this task

- Most of the threshold options have default values for better monitoring. However, you can change the values to suit the requirements of your environment.
- The threshold values are not applicable to the root aggregate of the node.

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Thresholds > Aggregates**.
3. Configure the appropriate threshold values for capacity, growth, and Snapshot copies.
4. Click **Save and Close**.

Configuring global volume threshold values

You can configure the global threshold values for all volumes to track any threshold breach. Appropriate events are generated for threshold breaches, and you can take preventive measures based on these events. You can configure the global values based on the best practice settings for thresholds that apply to all monitored volumes.

Before you begin

You must have the OnCommand Administrator or Storage Administrator role.

About this task

Most of the threshold options have default values for better monitoring. However, you can change the values to suit the requirements of your environment.

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Thresholds > Volumes**.
3. Configure the appropriate threshold values for capacity, Snapshot copies, quotas, volume growth, and inodes.
4. Click **Save and Close**.

Editing unmanaged relationship lag threshold settings

You can edit the global default lag warning and error threshold settings for unmanaged protection relationships so that events are generated at intervals that are appropriate to your needs.

Before you begin

You must have the OnCommand Administrator or Storage Administrator role.

About this task

The settings described in this operation are applied globally to all unmanaged protection relationships. They cannot be specified and applied exclusively to a single unmanaged protection relationship.

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Thresholds > Relationships**.
3. In the **Lag** area of the **Lag Thresholds for Unmanaged Relationships** dialog box, increase or decrease the warning or error lag time percentage as needed.
4. Click **Save and Close**.

Adding a user

You can add local users or database users by using the Manage Users page. You can also add remote users or groups belonging to an authentication server. You can assign roles to these users and, based on the privileges of the roles, users can effectively manage the storage objects and data using Unified Manager or view data in a database.

Before you begin

- To add a remote user or group, you must have enabled remote authentication and configured your authentication server.
- You must have the OnCommand Administrator role.

About this task

If you add a group from Windows Active Directory, then all direct members and nested subgroups can authenticate to Unified Manager, unless nested subgroups are disabled. If you add a group from OpenLDAP or other authentication services, then only direct members of that group can authenticate to Unified Manager.

Steps

1. Click **Administration > Manage Users**.
2. In the **Manage Users** page, click **Add**.
3. In the **Add User** dialog box, select the type of user that you want to add and enter the required information.

When entering the required user information, you must specify an email address unique to that user. Specifying email addresses shared by multiple users must be avoided.

4. Click **Add**.

Adding clusters

You can add a cluster to OnCommand Unified Manager to obtain cluster information such as the health, capacity, and configuration of the cluster so that you can find and resolve any issues that might occur. You can also view the cluster discovery status and monitor the performance of the cluster if you associate an Performance Manager instance with the cluster.


Before you begin

- You must have the following information:
 - Host name or cluster-management IP address
The host name is the FQDN or short name that Unified Manager uses to connect to the cluster. The host name must resolve to the cluster-management IP address.
The cluster-management IP address must be the cluster-management LIF of the administrative Storage Virtual Machine (SVM). If you use a node-management LIF, the operation fails.
 - Data ONTAP administrator user name and password
 - Type of protocol (HTTP or HTTPS) that can be configured on the cluster and the port number of the cluster
- You must have the OnCommand Administrator or Storage Administrator role.
- The Data ONTAP administrator must have the ONTAPI and SSH administrator roles.
- The Unified Manager FQDN must be able to ping Data ONTAP.
You can verify this by using the following Data ONTAP command: `ping -node node_name -destination Unified_Manager_FQDN`.

About this task

For a MetroCluster configuration, you must add both the local and remote clusters, and the clusters must be configured correctly.

Steps

1. Click  > **Clusters**.
2. From the **Managed Clusters** page, click **Add**.
3. In the **Add Cluster** dialog box, specify the required values, such as the host name or IP address (IPv4 or IPv6) of the cluster, user name, password, protocol for communication, and port number.

By default, the HTTPS protocol is selected.

You can change the cluster-management IP address from IPv6 to IPv4 or from IPv4 to IPv6. The new IP address is reflected in the cluster grid and the cluster configuration page after the next monitoring cycle is complete.
4. In the **Link Performance Manager** section, specify the required values, such as the host name or IP address (IPv4 or IPv6) of the cluster, user name, and password to associate an instance of Performance Manager.

You can associate an instance of Performance Manager either while adding a cluster or while modifying the cluster configuration.
5. Click **Save**.

6. If HTTPS is selected, perform the following steps:
 - a. In the **Authorize Host** dialog box, click **View Certificate** to view the certificate information about the cluster.
 - b. Click **Yes**.

Unified Manager checks the certificate only when the cluster is added initially. Unified Manager does not check the certificate for each API call to Data ONTAP.

If the certificate has expired, you cannot add a new cluster. You must first renew the SSL certificate and then add the cluster.

The cluster is added to the Unified Manager database after the default monitoring interval of approximately 15 minutes. If the cluster is associated with an instance of Performance Manager, the cluster is automatically added to Performance Manager.

Adding an alert

You can create alerts to notify you when a particular event is generated. You can create alerts for a single resource, for a group of resources, or for events of a particular severity type. You can specify the frequency with which you want to be notified and associate your script to the alert.

Before you begin

- You must have configured notification settings such as the email address, SMTP server, and SNMP trap host so that the Unified Manager server can use these settings to send notifications to users when an event is generated.
- You must know the resources and events for which you want to trigger the alert, and user names or email addresses of users you want to notify.
- You must have added scripts to Unified Manager using the Manage Scripts page.
- You must have the OnCommand Administrator or Storage Administrator role.

About this task

- You can create an alert based on resources, events, or both.

Steps

1. Click **Administration > Manage Alerts**.
2. In the **Manage Alerts** page, click **Add**.
3. In the **Add Alert** dialog box, perform the following steps:
 - a. Click **Name** and enter a name and description for the alert.
 - b. Click **Resources** and select the resources to be included or excluded from the alert.

You can set a filter by specifying a text string in the **Name contains** field to select a group of resources. Based on the text string you specify, the list of available resources displays only those resources that match the filter rule. The text string that you specify is case-sensitive.

If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule, and the alert is not generated for events related to the excluded resource.
 - c. Click **Events** and select the events based on the event name or event severity type for which you want to trigger an alert.

- d. Click **Actions** and select the users that you want to notify, the notification frequency, and assign a script to be executed when an alert is generated.

Note: If you modify the email address that is specified for the user and reopen the alert for editing, the **Name** field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you have modified the email address of the selected user from the Manage Users page, the modified email address is not updated for the selected user.

You can also choose to notify users through SNMP traps.

4. Click **Save**.

Example of adding an alert

This example shows how to create an alert that meets the following requirements:

- Alert name: Test
- Resources: includes all volumes whose name contains “abc” and excludes all the volumes whose name contains “xyz”
- Events: includes all critical events
- Actions: includes “sample@domain.com”, a “Test” script and the user has to be notified every 15 minutes

Perform the following steps in the Add Alert dialog box:

1. Click **Name** and enter **Test** in the **Alert Name** field.
2. Click **Resources** and in the Include tab, select Volumes from the drop-down list.
 - a. Enter **abc** in the **Name contains** field to display the volumes whose name contains abc.
 - b. Select <<All Volumes whose name contains 'abc'>> from the Available Resources area and move it to the Selected Resources area.
 - c. Click **Exclude** and enter **xyz** in the **Name contains** field and then click **Add**.
3. Click **Events** and select Critical from the **Event Severity** field.
4. Select **All Critical Events** from the Matching Events area and move it to the Selected Events area.
5. Click **Actions** and enter **sample@domain.com** in the **Alert these users** field.
6. Select **Remind every 15 minutes** to set the frequency to notify the user every 15 minutes. You can configure an alert to repeatedly send notification to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.
7. In the Select Script to Execute menu, select “Test” script .
8. Click **Save**.

Changing the umadmin password

For security, you are expected to change the default password for the umadmin user immediately after completing installation. If necessary, you can change the password again anytime thereafter. On

Red Hat Enterprise Linux, you change the Unified Manager umadmin password with a Linux command.

Before you begin

- Unified Manager must be installed on a Red Hat Enterprise Linux system.
- You must be able to log in as the root user to the Red Hat Enterprise Linux system upon which Unified Manager is running.

Steps

1. Log in as the root user to the target Red Hat Enterprise Linux system on which Unified Manager is running.
2. Change the umadmin password:

```
passwd umadmin
```

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

Note: If Unified Manager is installed in a VCS environment, then you must change the umadmin password on both nodes of the VCS setup. The umadmin password for both nodes must be same.

Related concepts

[Functions that umadmin users can perform](#) on page 8

Managing storage objects using the Favorites option

The Favorites option enables you to manage the storage objects in OnCommand Unified Manager by marking them as favorites. You can quickly view the status of your favorite storage objects and fix issues before they become critical.

Tasks you can perform from the Favorites dashboard

- View the list of storage objects marked as favorite.
- Add storage objects to the Favorites list.
- Remove storage objects from the Favorites list.

Viewing the Favorites list

You can view the capacity, performance, and protection details of different storage objects from the Favorites list. The performance details of storage objects are displayed only if OnCommand Unified Manager is paired with OnCommand Performance Manager. The details of a maximum of 20 storage objects are displayed in the Favorites list.

Adding storage objects to the Favorites list

You can use OnCommand Unified Manager to add storage objects to the Favorites list, and then monitor these objects for health, capacity, and performance. You can only mark clusters, volumes, and aggregates as favorite.

Removing storage objects from the Favorites list

You can remove storage objects from the Favorites list in OnCommand Unified Manager when you no longer require them to be marked as favorite.

Adding storage objects to favorites list

You can use OnCommand Management to add storage objects to a favorites list and monitor the objects for health, capacity, and performance. You can use the favorite list to determine issues and fix them before they become critical. The favorites list also provide the most recent monitoring status of an object.

Steps

1. Go to the details page of the required storage object.
2. Click the star icon to add the storage object to the favorites list.

The favorite object is added to the My Favorite list.

Example for adding a cluster to the favorites list

1. Click Clusters.
2. From the Clusters page, click the cluster that you want to add to the favorites list..
3. In the Cluster details page, click the star icon.
The cluster is added to the My Favorite list.

Connecting Performance Manager and Unified Manager

A connection between Performance Manager and Unified Manager enables you to monitor performance issues through the Unified Manager web UI.

Before you begin

- You must have installed Unified Manager.
- You must have installed Performance Manager.
- You must have the OnCommand Administrator role in Unified Manager.
If Unified Manager is installed on Red Hat Enterprise Linux, this role is automatically assigned to the “umadmin” user.
- You must have maintenance user login access to Performance Manager.
If Performance Manager is installed on Red Hat Enterprise Linux, the maintenance user is automatically named “umadmin”.

About this task

When using Performance Manager 2.1 or later and Unified Manager 6.4 or later, you can choose to connect using the new “full integration” connection mechanism or the legacy “partial integration” mechanism.

You can configure connections between one Unified Manager server and multiple Performance Manager servers.

Related information

[NetApp Documentation: OnCommand Performance Manager for Clustered Data ONTAP](#)

Creating a user with Event Publisher role privileges

To support a connection between a Performance Manager server and Unified Manager and the display of Performance Manager performance information in the Unified Manager web UI, you must create a local user for Unified Manager and assign to it the Event Publisher role.

Before you begin

You must have the OnCommand Administrator role in Unified Manager.

About this task

When you configure a connection between a Performance Manager server and Unified Manager, the local user assigned the Event Publisher role is specified as the user under which performance incident notification is posted in the Unified Manager web UI.

Steps

1. Click **Administration > Manage Users**.
2. In the **Manage Users** page, click **Add**.
3. In the **Add User** dialog box, select **Local User** for `type` and **Event Publisher** for `role`, and then enter the other required information.
4. Click **Add**.

After you finish

You can now configure a connection between one or more Performance Manager servers and Unified Manager.

Related concepts

[Functions that umadmin users can perform](#) on page 8

Configuring a full integration connection between a Performance Manager server and Unified Manager

To display performance issues discovered by a Performance Manager server in the Unified Manager web UI, you must configure a connection between Performance Manager and Unified Manager in the Performance Manager maintenance console.

Before you begin

- You intend to configure a full integration connection.
- The Unified Manager server must be installed with version 6.4 or later software.
- The versions of Unified Manager and Performance Manager must be compatible.
See the Interoperability Matrix at mysupport.netapp.com/matrix for the list of compatible versions.
- You must have the Performance Manager umadmin user ID.
- You must be prepared to specify the following information about the Unified Manager server:
 - Unified Manager server name or IP address
 - Unified Manager Administrator user name and password
 - Unified Manager Event Publisher user name and password

Note: When Unified Manager is installed in a high availability configuration, you must use the global IP address; you cannot use the Unified Manager server name or FQDN.

- The Unified Manager server, Performance Manager servers, and clusters that are being managed, must be set to the same absolute (UTC) time (or they must use the same NTP server) or new performance events are not correctly identified.

About this task

You can configure connections between a single Unified Manager server and up to five Performance Manager servers.

Important: Implementing a full integration connection with a Unified Manager server cannot be undone. You cannot disable the connection to run the Performance Manager server in a standalone configuration.

Steps

1. Log in using SSH as the maintenance user to the Performance Manager host to set up the Performance Manager and Unified Manager connection.
 - If Performance Manager is installed on Red Hat Enterprise Linux, log in as umadmin (the maintenance user's automatically assigned name) to the Red Hat Enterprise Linux machine that hosts the Performance Manager server for which you want to create the Unified Manager connection.

The Performance Manager maintenance console prompts are displayed.

2. In the maintenance console, type the number of the menu option labeled **Unified Manager Integration** and then select **Full Integration > Enable Full Integration**.
3. When prompted, supply the Unified Manager server name or IP address (IPv4 or IPv6).
The maintenance console checks the validity of the specified Unified Manager server name or IP address (IPv4 or IPv6) and Unified Manager server port and, if necessary, prompts you to accept the Unified Manager server trust certificate to support the connection.
4. When prompted, supply the Administrator user name and password.
5. When prompted, supply the Event Publisher user name and password.
6. When prompted, supply the unique name for this instance of Performance Manager.
This name enables you to easily identify the Performance Manager you want to manage when there are many instances integrated with Unified Manager.
7. Type **y** to confirm that the connection settings are correct, or type **n** if the settings are incorrect and you want to discard your changes.
8. If Performance Manager is installed on Red Hat Enterprise Linux, restart the Performance Manager server.

Result

After the connection is complete, all new performance events discovered by Performance Manager are reflected on the Unified Manager Dashboard page and Events page.

Note: Until an initial performance event is discovered, the Unified Manager Dashboard page remains unchanged.

Configuring a partial integration connection between a Performance Manager server and Unified Manager

To display performance issues discovered by a Performance Manager server in the Unified Manager web UI, you must configure a connection between Performance Manager and Unified Manager in the Performance Manager maintenance console.

Before you begin

- You intend to configure a partial integration connection.
- The version of Unified Manager must be compatible with the version of Performance Manager. See the Interoperability Matrix at mysupport.netapp.com/matrix for the list of compatible versions.
- You must have created a local user with Event Publisher privileges on Unified Manager in the connection you want to create.
- You must have the Performance Manager umadmin user ID.
- You must be prepared to specify the following information about Unified Manager:
 - Unified Manager server name or IP address
 - Unified Manager server port (must always be 443)
 - Event Publisher user name (the name of the local Unified Manager user assigned Event Publisher privileges)
 - Event Publisher password (the password of the local Unified Manager user assigned Event Publisher privileges)

Note: When Unified Manager is installed in a high availability configuration, you must use the global IP address; you cannot use the Unified Manager server name or FQDN.

- The clusters that are to be managed by Performance Manager and Unified Manager must have been added to both Performance Manager and Unified Manager.
- The Unified Manager server, Performance Manager servers, and clusters that are being managed, must be set to the same absolute (UTC) time (or they must use the same NTP server) or new performance events are not correctly identified.

About this task

You can configure connections between one Unified Manager server and multiple Performance Manager servers.

Steps

1. Log in using SSH as the maintenance user to the Performance Manager host to set up the Performance Manager and Unified Manager connection.
 - If Performance Manager is installed on Red Hat Enterprise Linux, log in as umadmin (the maintenance user's automatically assigned name) to the Red Hat Enterprise Linux machine that hosts the Performance Manager server for which you want to create the Unified Manager connection.

The Performance Manager maintenance console prompts are displayed.

2. In the maintenance console, type the number of the menu option labeled **Unified Manager Integration** and then select **Partial Integration > Add Unified Manager Server Connection**.

3. When prompted, supply the Unified Manager server name or IP address (IPv4 or IPv6) and Unified Manager server port information.

The maintenance console checks the validity of the specified Unified Manager server name or IP address (IPv4 or IPv6) and Unified Manager server port and, if necessary, prompts you to accept the Unified Manager server trust certificate to support the connection. The default Unified Manager server port 443 must be used.

4. When prompted, supply the Event Publisher user name and password, and then confirm that the settings are correct.
5. If you want to configure an additional connection between the Unified Manager and another Performance Manager server, log in as the maintenance user to that Performance Manager server and repeat Steps 2 through 4 for each connection.

You can configure connections between a single Unified Manager server and up to five Performance Manager servers.

Result

After the connection is complete, all new performance events discovered by Performance Manager are reflected on the Unified Manager Dashboard page and Events page.

Note: Until an initial performance event is discovered, the Unified Manager Dashboard page remains unchanged.

Changing Unified Manager connection settings

You can change the settings related to the Unified Manager server to which Performance Manager is connected, including the IP address, administrator name and password, and event publisher name and password. You can also refresh the connection details when a new Unified Manager security certificate has been generated and Performance Manager needs to accept the new certificate.

Before you begin

- You must have the Performance Manager umadmin user ID.
- Depending on the type of change you are making, you must be prepared to specify the following information about the Unified Manager server:
 - Unified Manager server name or IP address
 - Administrator user name and password
 - Event Publisher user name and password

Steps

1. Using SSH, log in as the maintenance user to the Performance Manager host.
 - If Performance Manager is installed on Red Hat Enterprise Linux, log in as umadmin (the maintenance user's automatically assigned name) to the Red Hat Enterprise Linux machine that hosts the Performance Manager server.

The Performance Manager maintenance console prompts are displayed.

2. In the maintenance console, type the number of the menu option labeled **Unified Manager Integration** and then select **Full Integration > Modify Full Integration Settings**.
3. Change the settings as necessary.
4. Type **y** to confirm that the new connection settings are correct.

5. If Performance Manager is installed on Red Hat Enterprise Linux, restart the Performance Manager server.

Deleting a connection between a Performance Manager server and Unified Manager

If you no longer want to display performance issues discovered by a specific Performance Manager server in the Unified Manager web UI, you can delete the connection between that server and Unified Manager. Additionally, if you are planning to delete a Performance Manager instance that has an existing connection to Unified Manager, you must delete the connection before deleting the instance.

Before you begin

You must have the umadmin user ID, which is authorized to log in to the Red Hat Enterprise Linux machine on which sits the Performance Manager server.

About this task

This option is available only for a partial integration (Performance Event Publishing only) connection between Performance Manager and Unified Manager. You cannot delete a full integration connection between Performance Manager and Unified Manager.

Steps

1. Log in as the maintenance user (umadmin) to the Red Hat Enterprise Linux machine on which Performance Manager is installed.
The Performance Manager maintenance console prompts are displayed.
2. In the maintenance console, type the number of the **Unified Manager Integration** menu option.
3. Select **Partial Integration > Delete Unified Manager Server Connection**.
4. When prompted about whether you want to delete the connection, type **y** to delete the connection.

Result

Performance events discovered by the specific Performance Manager server are no longer displayed in the Unified Manager web UI.

Setting up a connection between OnCommand Workflow Automation and Unified Manager

This workflow shows you how to set up a secure connection between Workflow Automation and Unified Manager. Connecting to Workflow Automation enables you to use protection features like SnapMirror and SnapVault configuration workflows, as well as commands for managing SnapMirror relationships.

Before you begin

You must have installed Unified Manager.

You must have installed OnCommand Workflow Automation version 3.0 or later.

You must have the OnCommand Administrator or Storage Administrator role.

Related information

[NetApp Documentation: OnCommand Workflow Automation \(current releases\)](#)

Creating a database user

To support a connection between Workflow Automation and Unified Manager or to access report-specific database views, you must first create a database user with the Integration Schema or Report Schema role in the Unified Manager web UI.

Before you begin

You must have the OnCommand Administrator role.

About this task

Database users provide integration with Workflow Automation and access to report-specific database views. Database users do not have access to the Unified Manager web UI.

Steps

1. Click **Administration > Manage Users**.
2. In the **Manage Users** page, click **Add**.
3. In the **Add User** dialog box, select **Database User** in the **Type** drop-down list.
4. Type a name and password for the database user.
5. In the **Role** drop-down list, select the appropriate role.

If you are...	Choose this role
Connecting Unified Manager with Workflow Automation	Integration Schema
Accessing report-specific database views	Report Schema

6. Click **Add**.

Related concepts

[Functions that umadmin users can perform](#) on page 8

Setting up a connection between OnCommand Workflow Automation and Unified Manager

You can set up a secure connection between Workflow Automation and Unified Manager. Connecting to Workflow Automation enables you to use protection features like SnapMirror and SnapVault configuration workflows, as well as commands for managing SnapMirror relationships.

Before you begin

- You must have the name of a database user that you created in Unified Manager to support Workflow Automation and Unified Manager connections. This database user must have been assigned the Integration Schema user role.
- You must be assigned either the Administrator role or the Architect role in Workflow Automation.
- You must have the host address, port number 443, user name, and password for the OnCommand Workflow Automation setup.
- You must have the OnCommand Administrator or Storage Administrator role.

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Add-ons > Workflow Automation**.
3. In the **Unified Manager Database User** area of the **Set Up OnCommand Workflow Automation** dialog box, select the name and enter the password for the database user that you created to support Unified Manager and OnCommand Workflow Automation connections.
4. In the **Workflow Automation Credentials** area of **Set Up OnCommand Workflow Automation** dialog box, type the host name or IP address and user name and password for the OnCommand Workflow Automation setup.

You must use Unified Manager server port 443.
5. Click **Save and Close**.
6. If you use a self-signed certificate, click **Yes** to authorize the security certificate.

The Workflow Automation Options Changed dialog box displays.
7. Click **Yes** to reload the web UI and add the Workflow Automation features.

Related information

[NetApp Documentation: OnCommand Workflow Automation \(current releases\)](#)

Setting up Unified Manager for high availability

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.

Configuring Unified Manager server with VCS using configuration scripts

You can configure Unified Manager with VCS using configuration scripts.

Before you begin

- Unified Manager must be installed on both the nodes in the VCS setup.
- XML::LibXML module must be bundled with Perl for VCS scripts to work.
- A shared LUN of sufficient size to accommodate the source Unified Manager data must be created.
- 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.

About this task

In the VCS setup, the node that has the virtual IP interface and mount point active is the first node. The other node is the second node.

Steps

1. Log in to the first node of the cluster.
Unified Manager services on the second node in the high availability setup must be in stopped state.
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 obtain the support bundle.
4. Run the `ha_setup.pl` script, which is available at `/opt/netapp/ocum/scripts`:

```
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
```
5. Use the Veritas Operation Manager web console or VCS Cluster Manager to verify that a failover group is created and the Unified Manager server services, mount point, virtual IP, NIC, and volume group are added to the cluster group.
6. Manually move the service group to the secondary node and verify that cluster failover is working.
7. Verify that the VCS has switched over to the second node of the cluster.
You must verify that data mount, virtual IP, volume group, and NIC cards 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 configuration scripts to obtain the global IP address required for setting up a connection to OnCommand Performance Manager.
 - a. Click **Administration > Setup Options**.
 - b. In the **Setup Options** dialog box, click **Management Server**.
 - c. In the HTTPS section, click **Regenerate HTTPS Certificate**.

The regenerated certificate provides the cluster IP address but not the FQDN name. Therefore, you must use the global IP address to set up a connection between OnCommand Performance Manager and Unified Manager.

12. Access Unified Manager UI using the link

`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 before and after failover. Both the nodes in the high-availability setup must be able to access the shared location.

Related tasks

[Installing Unified Manager on VCS](#) on page 27

[Connecting Performance Manager and Unified Manager](#) on page 42

[Setting up a connection between OnCommand Workflow Automation and Unified Manager](#) on page 47

Configuring VCS with Unified Manager server service resources

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

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

Category	Services
Storage resource	<ul style="list-style-type: none"> • <code>vol</code> • <code>mount</code>
Database resource	<ul style="list-style-type: none"> • <code>mysql</code>

Category	Services
Network resource	<ul style="list-style-type: none"> <code>nic</code> <code>vip</code>
Unified Manager resource	<ul style="list-style-type: none"> <code>ocie</code> <code>ocieau</code>

Configuring an existing Unified Manager setup for high availability

You can upgrade your existing Unified Manager installation and configure your setup environment to provide 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 node to your cluster and installed VCS.
See the instructions provided in the *Veritas Cluster Server 6.1.1 Installation Guide*.
- The new node must be configured to access the same shared location as the first node in the high-availability setup.

Steps

- Log in to the new node of the cluster.
- Install Unified Manager on the node.
[Installing Unified Manager on Red Hat Enterprise Linux](#) on page 16
- Restore the backup on the first node.
[Restoring a database backup on Red Hat Enterprise Linux](#) on page 55
- Configure the Unified Manager server using configuration scripts.
- Manually failover to the other node.
- 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.
- If Workflow Automation is configured, remove and reconfigure Workflow Automation.
- If Performance Manager is configured with Unified Manager, reconfigure Performance Manager with a new cluster IP address.
- If SnapProtect is configured with Unified Manager, reconfigure SnapProtect with a new cluster IP address and the existing storage policies.
- Regenerate custom reports and add them to Unified Manager with the cluster IP address.

Related tasks

[Connecting Performance Manager and Unified Manager](#) on page 42

Setting up a connection between OnCommand Workflow Automation and Unified Manager on
page 47

Related information

Symantec Documentation

Configuring backup and restore operations

You can create scheduled backups of Unified Manager and use the restore feature to restore the backup to a local system or a remote system.

What database backup is

A backup is a copy of the Unified Manager database and configuration files that you use in case of a system failure or data loss. In Unified Manager, you can perform a scheduled local or remote backup.

You can create a scheduled backup by adding or editing the backup setting attributes. By default, the scheduled backup is disabled. You can also view backup failure and success events.

Before beginning a backup operation, Unified Manager performs an integrity check to verify that all the required backup files and backup directories exist and are writable.

You can restore a Unified Manager backup only on the same version of Unified Manager. For example, if you created a backup on Unified Manager 6.3, the backup can be restored only on Unified Manager 6.3.

Configuring database backup settings

You can configure the Unified Manager database backup settings to set the local database backup path, retention count, and database backup schedules. You can also enable daily or weekly schedule backups. By default the scheduled backup is disabled.

Before you begin

- You must have the Operator, OnCommand Administrator, or Storage Administrator role.
- Ensure that JBoss user has write permissions to the backup directory.

Steps

1. Click **Administration > Database Backup**.
2. In the **Backup and Restore** page, click **Actions > Database Backup Settings**.
3. Configure the appropriate values for a backup path and retention count.
The default value for retention count is 10; you can use 0 for creating unlimited backups.
4. Select **Schedule Frequency**.
5. In the Backup Schedule section, specify a daily or weekly schedule.

Daily

If you select this option, you should enter a time in 24 hour format for creating the backup. For example, if you specify 18.30, then a backup is created daily at 6:30 PM.

Weekly

If you select this option, you should specify the time and day for creating the backup. For example, if you specify the day as Monday and time as 16:30, then a weekly backup is created every Monday at 4:30 PM.

6. Click **Save and Close**.

What a database restore is

Database restore is the process of copying backup files from a secondary storage to a disk to restore the original data in the event of a data loss. You can perform the restore operation on Unified Manager database from the console.

During the restore process, you will be logged out of Unified Manager. You can log in to the system after the restore process is complete.

Using the restore feature, you can view the messages related to restore failure and success. The restore operation is performed using restore commands that are executed on the Unified Manager server from the console.

Note: The restore operation is version and platform specific, which means that backups of a specific platform and version are restored only to the same platform and version.

Restoring a database backup on Red Hat Enterprise Linux

In the event of data loss or data corruption, you can restore Unified Manager to the previous stable state with minimum loss of data. You can restore the Unified Manager database to a local or remote Red Hat Enterprise Linux system.

Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- You must have installed and configured Unified Manager.
- A backup of Unified Manager must already exist in the system on which you want to perform the restore operation.
- The backup file must be of 7z type.

Steps

1. Log in to the Unified Manager console as a maintenance user.
2. If Unified Manager is installed in VCS setup, then stop the Unified Manager ocie, ocieau, and rp services using Veritas Operations Manager.
3. At the command prompt, restore the backup:

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

Example

```
um backup restore -f /opt/netapp/data/ocum-backup/  
UM_6.3.N150513.1348_backup_unix_05-25-2015-04-45.7z
```

If the folder name contains a space, you must include the absolute path or relative path in double quotation marks; for example: `"/opt/netapp/data/ocum-backup/UM_6.3.N150418.2300_backup_rhel_04-20-2015-02-51.7z"`

After the restore operation is complete, you can log in to Unified Manager.

Upgrading OnCommand Unified Manager

You can upgrade OnCommand 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.

Upgrade overview of Unified Manager 6.3 on Red Hat Enterprise Linux

Because Unified Manager installed on Red Hat Enterprise Linux was not supported in Unified Manager 6.1, you cannot upgrade from Unified Manager 6.1 (which is always installed as a virtual appliance) to Unified Manager 6.3 installed on Red Hat Enterprise Linux. However, you can upgrade from Unified Manager 6.2 to Unified Manager 6.3.

To transition from Unified Manager 6.1 on a virtual appliance to Unified Manager 6.3 on Red Hat Enterprise Linux, you must download the `OnCommandUnifiedManager-6.3RC1.zip` bundle from the NetApp Support Site, and install it on a Red Hat Enterprise Linux physical or virtual machine. Then, you must configure the newly installed version to monitor the same clusters that were being monitored by Unified Manager 6.1.

Both Unified Manager 6.1 installed as a virtual appliance and Unified Manager 6.3 installed on Red Hat Linux can monitor the same clustered Data ONTAP systems concurrently. However, if Unified Manager 6.1 installed as a virtual appliance and Unified Manager 6.3 installed on Red Hat Linux are both polling the same clusters, the increased overhead might result in slower response times.

Note: Unified Manager 6.3 installed on Red Hat Enterprise Linux does not automatically discover and use the relationships and alerts that you configured for Unified Manager 6.1. Therefore, when you install Unified Manager 6.3, you must reconfigure all the backup and mirror relationships and all the alerts.

Note: You can upgrade from Unified Manager 6.1 to Unified Manager 6.3 installed as a virtual appliance.

Downloading the Unified Manager software bundles

Before upgrading to Unified Manager 6.4, you must download the software bundles from the NetApp Support Site.

Before you begin

You must have login credentials for the NetApp Support Site.

About this task

You must download both the OnCommand Unified Manager bundle and the third-party-dependencies bundle for the upgrade to be successful.

Steps

1. Navigate to the NetApp Support Site at mysupport.netapp.com, and locate the Download pages for installing Unified Manager on the Red Hat Enterprise Linux platform.
2. Download the Unified Manager bundle (`OnCommandUnifiedManager-6.4.zip`) to a target directory on the target Red Hat Enterprise Linux system.

3. Download the third-party-dependencies bundle to the same directory on the target Red Hat Enterprise Linux system.

Download `thirdpartydependencies-6.4-rhel6.zip` for Red Hat 6 systems or `thirdpartydependencies-6.4-rhel7.zip` for Red Hat 7 systems.

4. Verify the checksums to ensure that the software downloaded correctly.

Related information

[Software Downloads: mysupport.netapp.com/NOW/cgi-bin/software](https://mysupport.netapp.com/NOW/cgi-bin/software)

Upgrading to OnCommand Unified Manager 6.4 on Red Hat Enterprise Linux

You can upgrade from Unified Manager 6.2 or 6.3 to Unified Manager 6.4 by downloading and running the installation file on the Red Hat Linux platform. You must unzip both the third-party-dependencies bundle and Unified Manager bundle for the upgrade to be successful.

Before you begin

- The system on which you are upgrading Unified Manager must meet the system and software requirements. *[System requirements](#)* on page 10 and *[Software requirements](#)* on page 11.
- 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 machine in case there is an issue during the upgrade.
- You should complete any running operations because Unified Manager is unavailable during the upgrade process.

About this task

When upgrading Unified Manager, the database files remain in `/data` instead of `/opt/netapp/data` as is created with a new Unified Manager 6.4 installation. However, the upgrade process creates a symlink from `/opt/netapp/data` to `/data`.

Steps

1. Log in to the target Red Hat Enterprise Linux system.
2. Navigate to the target directory and expand the third-party-dependencies bundle for the version of Red Hat Enterprise Linux you are using.

Example

```
unzip thirdpartydependencies-6.4-rhel6.zip
```

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

3. In the target directory, expand the Unified Manager bundle:

```
unzip OnCommandUnifiedManager-6.4.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:

- MySQL Community Edition rpms:
 MySQL-client-5.6.28-1.el6.x86_64.rpm (Red Hat 6 only)
 MySQL-server-5.6.28-1.el6.x86_64.rpm (Red Hat 6 only)
 MySQL-shared-compat-5.6.28-1.el6.x86_64.rpm (Red Hat 6 only)
 MySQL-client-5.6.28-1.el7.x86_64.rpm (Red Hat 7 only)
 MySQL-server-5.6.28-1.el7.x86_64.rpm (Red Hat 7 only)
 MySQL-shared-compat-5.6.28-1.el7.x86_64.rpm (Red Hat 7 only)
 - ocie-serverbase rpm:
 ocie-serverbase-<version>.x86_64.rpm
 - ocie-server rpm:
 ocie-server-<version>.x86_64.rpm
 - ocie-au rpm:
 ocie-au-<version>.x86_64.rpm
 - netapp-node rpm:
 node-<version>.x86_64.rpm
 - rp rpm:
 rp-<version>.x86_64.rpm
 - netapp-ocum rpm:
 netapp-ocum-<version>.x86_64.rpm
5. Enable the Third Party Oracle Java repository so that the correct JRE software is installed during the upgrade:

If you are using...	Enter this command...
Red Hat 6 systems	subscription-manager repos --enable rhel-6-server-thirdparty-oracle-java-rpms
Red Hat 7 systems	subscription-manager repos --enable rhel-7-server-thirdparty-oracle-java-rpms

These commands require that you have a subscription to the Red Hat Enterprise Linux Subscription Manager.

6. If Unified Manager is configured for high availability, then using Veritas Operation Manager stops all Unified Manager services on the first node.
7. Upgrade Unified Manager using one of the following methods:
- Using the following script:
upgrade.sh
 - Using the following manual steps:
 - a. Stop the “ocie” and “ocieau” services:
/etc/init.d/ocie stop
 - b. Upgrade MySQL:
rpm -U --nodeps MySQL-*.rpm
 - c. Create a directory to move the MySQL data:
mkdir mysql

- d. Move the MySQL files and folders to the new folder:

```
mv MySQL-*.rpm mysql/
```

- e. Upgrade Unified Manager:

```
yum upgrade *.rpm
```

This command automatically executes the RPM modules, upgrading the necessary supporting software and the Unified Manager modules that run on of them.

Important: 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 should be upgraded in a specific order to a specific directory structure that are executed and configured automatically by the `yum upgrade *.rpm` command.

8. Stop all Unified Manager services on the second node using Veritas Operation Manager.
9. Switch the service group to the second node in the high-availability setup.
10. Upgrade Unified Manager on the second node.
11. 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 the URL https://default_ip_address to access
the OnCommand Unified Manager GUI.
```

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 installed Unified Manager on a Red Hat Enterprise Linux 6.x system and want to upgrade to Red Hat Enterprise Linux 7.x, you must follow specific process. You must create a backup of Unified Manager on the Red Hat Enterprise Linux 6.x system, and then restore the backup onto a new Red Hat Enterprise Linux 7.x system.

Before you begin

You must have a server on which you can install Red Hat Enterprise Linux 7.x and the Unified Manager software.

About this task

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.

Steps

1. Install and configure a new server with Red Hat Enterprise Linux 7.x software.
[Requirements for Unified Manager on Red Hat Enterprise Linux](#) on page 10
2. On the Red Hat Enterprise Linux 7.x system, install the same version of the Unified Manager software that you have on the existing Red Hat Enterprise Linux 6.x system.
[Downloading and installing Unified Manager on a blank Red Hat Enterprise Linux system](#) on page 17
3. On the Red Hat Enterprise Linux 6.x system, create a backup of Unified Manager.
4. On the Red Hat Enterprise Linux 6.x system, shut down Unified Manager.
5. On the Red Hat Enterprise Linux 7.x system, restore Unified Manager.
[Restoring a database backup on Red Hat Enterprise Linux](#) on page 55

After you finish

You can 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.

Unified Manager administrative operations

When Unified Manager is installed on a Red Hat Enterprise Linux system, operations such as stopping and restarting the service, uninstalling the software, generating a support bundle, or changing the hostname are performed using Linux commands.

Stopping and starting Unified Manager in Red Hat Enterprise Linux

You might occasionally have to stop Unified Manager prior to performing maintenance operations, such as backup and restore or changing the hostname, and then restart Unified Manager after those operations are completed.

Before you begin

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

Steps

1. Log in as root user to the Red Hat Enterprise Linux machine on which you want to stop the Unified Manager service.
2. Stop the Unified Manager service using either VCS Operations Manager or VCS commands.
3. After the shutdown is complete, perform the maintenance operation that you stopped Unified Manager to perform.
4. After you complete your maintenance operation, restart Unified Manager service using either VCS Operations Manager or VCS commands.

Changing the OnCommand Unified Manager host name in Red Hat Enterprise Linux

At some point, you might want to change the host name of the Red Hat Enterprise Linux machine on which you have installed Unified Manager. For example, you might want to rename the host to more easily identify your Unified Manager servers by type, workgroup, or monitored cluster group when you list your Red Hat Enterprise Linux machines.

Before you begin

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

About this task

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

Regardless of how the host name was assigned, if you change the host name and intend to use the new host name to access the Unified Manager web UI, you must generate a new security certificate.

If you access the web UI by using the server's IP address instead of the host name, you do not have to generate a new certificate if you change the host name. However, it is the best practice to update the certificate, so that the host name in the certificate matches the actual host name. If you change the host name in Unified Manager, you must manually update the host name in Workflow Automation. The host name is not updated automatically. The new certificate does not take effect until the Red Hat Enterprise Linux machine is restarted.

Important: If connections that enable performance monitoring are currently configured between the Unified Manager server and one or more Performance Manager servers, executing this task invalidates those connections and deactivates any further performance monitoring updates from Performance Manager servers to the Unified Manager UI. You must reactivate those connections after completing this task.

Steps

1. Log in as the root user to the Unified Manager Red Hat Enterprise Linux machine that you want to modify.
2. Stop the Unified Manager software and the associated MySQL software by entering the following commands in the order shown:

```
service ocieau stop
service ocie stop
service rp stop
service mysql stop
```

3. Edit the HOSTNAME parameter in the `/etc/sysconfig/network` file to specify the new fully qualified domain name and save the file:

```
HOSTNAME=new_FQDN
```

Example

```
HOSTNAME=nuhost.corp.widget.com
```

4. If there is an entry in the `/etc/hosts` file listing your IP address with the old host name, change it to the new name:

```
ip-address new_FQDN new_hostname
```

Example

```
10.10.10.54 nuhost.corp.widget.com nuhost
```

5. Change the host name using the Linux `hostname` command:

```
hostname new_FQDN
```

Example

```
hostname nuhost.corp.widget.com
```

6. Regenerate the HTTPS certificate:

```
/opt/netapp/essentials/bin/cert.sh create
```

7. Restart the network service:

```
service network restart
```

8. After the service is restarted, verify whether the new host name is able to ping itself:

```
ping new_hostname
```

Example

```
ping nuhost
```

This command should return the same IP address that was set earlier for the original host name.

9. After you complete and verify your host name change, restart Unified Manager by entering the following commands in the order shown:

```
service mysql start
service rp start
service ocie start
service ocieau start
```

Removing Unified Manager from the Red Hat Enterprise Linux host

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

Before you begin

You must have root user access to the Red Hat Enterprise Linux machine from which you want to remove Unified Manager.

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 Red Hat Enterprise Linux machine:

```
rpm -e netapp-ocum ocie-au ocie-server ocie-serverbase rp netapp-node
```

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 and remove Unified Manager from the second node:

```
rpm -e netapp-ocum ocie-au ocie-server ocie-serverbase rp netapp-node
```

7. Prevent the service group from using VCS Operations Manager or VCS commands.
8. Optional: If appropriate, remove the supporting software modules, such as Java, MySQL, rrdTools, and p7zip:

```
rpm -e p7zip rrdtool rrdtool-perl MySQL-client MySQL-server jre
```

Result

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.

Generating a support bundle if OnCommand Unified Manager is installed on Red Hat Enterprise Linux

You can generate a zipped support bundle for Unified Manager that can be used for storage domain troubleshooting. You can generate the support bundle from the command line.

Before you begin

You must have the root user credentials for the Red Hat Enterprise Linux host on which Unified Manager is installed.

About this task

You usually perform this task at the request of technical support.

Steps

1. Log in as the root user to the Red Hat Enterprise Linux host on which Unified Manager is installed.
2. Generate the support bundle:

create_support_bundle

The `create_support_bundle` command compiles the support files, and bundles these files into a zipped package. A message is displayed with the location of the zipped support bundle, similar to the following:

```
Support bundle saved to /opt/netapp/data/support/  
support_bundle_20140822_004711_467.7z
```

3. Send the zipped support bundle to technical support or whoever asked for it.

Adding disk space to the “data” directory of the Red Hat Enterprise Linux host

If you allotted insufficient disk space to the `/opt/netapp/data` directory to support Unified Manager when you originally set up the Red Hat Enterprise Linux host and then installed Unified Manager, you can add disk space after installation by increasing disk space on the `/opt/netapp/data` directory.

Before you begin

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

About this task

Unified Manager requires at least 100 GB of disk space allocated to the `/opt/netapp/data` directory of the Red Hat Enterprise Linux host on which it is installed.

Note: Space for the data directory was allocated in `/data` in Unified Manager 6.3 and earlier. Unified Manager version 6.4 and later creates the data directory in `/opt/netapp/data`. If you are working on a system that has been upgraded from Unified Manager 6.3, you must expand the space in `/data`.

Steps

1. Log in as root user to the Red Hat Enterprise Linux machine on which you want to add disk space.
2. Stop the Unified Manager service and the associated MySQL software by entering the following commands in the order shown:


```
service ocieau stop
service ocie stop
service rp stop
service mysql stop
```
3. Create a temporary backup folder (for example, /backup-data) with sufficient disk space to contain the data in the current /opt/netapp/data directory.
4. Copy the content and privilege configuration of the existing /opt/netapp/data directory to the backup data directory:


```
cp -rp /opt/netapp/data/* /backup-data
```
5. If SE Linux is enabled, perform the following substeps:
 - a. Get the SE Linux type for folders on existing /opt/netapp/data folder:


```
se_type=`ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' | head -1`
```

The system returns a confirmation similar to the following:

```
echo $se_type
mysqld_db_t
```
 - b. Run the chcon command to set the SE Linux type for the backup directory:


```
chcon -R --type=mysqld_db_t /backup-data
```
6. Remove the contents of the /opt/netapp/data directory:


```
cd /opt/netapp/data
rm -rf *
```
7. Expand the size of the /opt/netapp/data directory to 100 GB through LVM commands or by adding extra disks.

Important: Mounting the /opt/netapp/data directory on an NFS export or CIFS share is not supported.
8. Confirm that the /opt/netapp/data directory owner (mysql) and group (root) are unchanged:


```
ls -ltr / | grep opt/netapp/data
```

The system returns a confirmation similar to the following:

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```
9. If SE Linux is enabled, confirm that the context for the /opt/netapp/data directory is still set to mysqld_db_t with the following commands:


```
touch /opt/netapp/data/abc
ls -Z /opt/netapp/data/abc
```

The system returns a confirmation similar to the following:

```
-rw-r--r--. root root unconfined_u:object_r:mysql_db_t:s0 /opt/
netapp/data/abc
```

10. Copy the contents from backup-data, back to the expanded /opt/netapp/data directory:
`cp -rp /backup-data/* /opt/netapp/data/`
11. Start the MySQL service:
`service mysql start`
12. After the MySQL service is started, start the ocie and ocieau services by entering the following commands in the order shown:
`service rp start`
`service ocie start`
`service ocieau start`
13. After all of the services are started, delete the backup folder /backup-data:
`rm -rf /backup-data`

Moving content from /data to /opt/netapp/data after upgrading from Unified Manager 6.3

After upgrading from Unified Manager 6.3 or earlier, you can move data files from /data to /opt/netapp/data to correspond with Red Hat installation best practices.

Before you begin

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

About this task

Unified Manager 6.3 and earlier installed database files in /data. Based on Red Hat installation best practices, Unified Manager 6.4 and later installs database files in /opt/netapp/data. During an upgrade from Unified Manager 6.3 to Unified Manager 6.4, the process creates a symlink from /opt/netapp/data to /data.

If required, you can move the data files from /data to /opt/netapp/data.

Steps

1. Log in as the root user to the Red Hat Enterprise Linux machine on which Unified Manager is installed.
2. Stop the Unified Manager service and the associated MySQL software by entering the following commands in the order shown:
`service ocieau stop`
`service ocie stop`
`service rp stop`
`service mysql stop`
3. Remove the symlink from /opt/netapp/data to /data:

```
rm /opt/netapp/data
```

4. Copy the contents of /data to /opt/netapp/data:

```
cp -rp /data /opt/netapp/data
```

5. If SE Linux is enabled, disable it:

```
setenforce 0
```

6. Start the MySQL service:

```
service mysql start
```

7. After the MySQL service is started, start the ocie, rp, and ocieau services by entering the following commands in the order shown:

```
service rp start
```

```
service ocie start
```

```
service ocieau start
```

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
```

Changing the JBoss password

You can create a new, custom JBoss password to overwrite the default password that is set during installation.

Before you begin

- You must have root user access to the Red Hat Enterprise Linux machine 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 to the Red Hat Enterprise Linux machine.
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
```
4. When prompted, enter the old JBoss password.
The default old password is D11h1aMu@79%.
5. When prompted, enter the new JBoss password, and then enter it a second time as 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.

Troubleshooting Unified Manager Installation on Red Hat Enterprise Linux

During or shortly after installation of Unified Manager on Red Hat Enterprise Linux, you might encounter some issues that require further attention.

Notification of nonsigned software packages during installation on Red Hat Enterprise Linux

If you are installing Unified Manager on a Red Hat Enterprise Linux system on which a signed software package requirement is enabled, your attempt to install Unified Manager with the normal `yum install *.rpm` command might fail.

In such circumstances, at the point of failure, the `yum install` program displays a message similar to the following:

```
Package ocie-au-xyz.rpm is not signed
```

Workaround

If you encounter this situation, you can run the `yum install *.rpm` command again but insert the `--nogpgcheck` option to suspend the signing requirement during installation:

```
yum install --nogpgcheck *.rpm
```

Unified Manager installation terminates due to MySQL packages upgrade fail

The presence of any version of MySQL other than MySQL Community Edition, supplied by Oracle, on the target Red Hat Community Linux system causes the automated Unified Manager installation to terminate with a MySQL-related error.

If you attempt to install Unified Manager on a Red Hat Community Linux system by downloading and unzipping the Unified Manager bundle and third-party-dependencies bundle and then invoking the `yum install *.rpm` command, and if that system has a preexisting version of MySQL other than MySQL Community Edition, the installation terminates and displays a message similar to the following:

```
Error in PREIN scriptlet in rpm package MySQL-server-5.x.xx-1.elx.86_64
```

Actions

If you encounter this problem, perform the following steps:

1. Remove the existing MySQL packages from the target system.
2. Restart the Unified Manager installation by using the `yum install *.rpm` command.
The automated installation process automatically installs MySQL Community Edition as supplied in the third-party-dependencies bundle.

Email notification of initial cron job failure at the end of the Unified Manager Red Hat Enterprise Linux installation operation can be disregarded

At the end of the automated installation of Unified Manager in Red Hat Enterprise Linux (invoked by the `yum install *.rpm` command), the root user receives e-mail notification with messages, which can be disregarded, indicating failure of the initial cron job associated with Unified Manager installation.

The contents of the e-mail message contain a log of an automated cron job associated with the installation and display messages that imply a failure of the installation process:

```
cat: /proc//statm: No such file or directory
cat: /proc//io: No such file or directory
cat: /proc//io: No such file or directory
```

These messages mean nothing. You can safely ignore them.

Maintenance user is not created during installation if noexec privilege is set in /tmp partition

If you install Unified Manager on a Red Hat Enterprise Linux system with the `noexec` privilege set in `/tmp` partition, then Unified Manager fails to create the maintenance user during installation.

Actions

Follow these steps to resolve the issue:

1. Uninstall Unified Manager.
2. Log in to the Red Hat Enterprise Linux console as a root user.
3. Edit the `/etc/fstab` file and remove the `noexec` option from the `/tmp` partition.
4. Run the `mount` command and ensure that the `noexec` option is not set in `/tmp` partition.
5. Install Unified Manager.

Intermittent cluster connectivity issue

Issue

Unified Manager might intermittently fail to connect to a cluster. When this happens, it reports one of the following messages: the login has failed, the controller is unavailable, or the connection has been refused.

Cause

Clustered Data ONTAP firewall policies have a maximum connection limit of 4013 TCP sessions.

Typically, this limit is not reached because sessions open and close quickly. The exception is that if Data ONTAP performs DNS lookups for hosts that do not exist, or for hosts that are not listed in DNS, each lookup session can remain open for two minutes because no response to the connection request is returned. These “pending closure” sessions can quickly add up and cause the firewall connection limit to be reached.

Corrective action

If these symptoms match the issue you are having, check the export policies and verify that the listed hosts can be resolved through DNS.

You should clean up the host names that are causing the issue:

1. Delete hosts from the policy if they do not exist or if they no longer need to be in the policy.
2. Add hosts that are located in the policy and that have been verified to exist, but that currently fail the DNS lookup.

Copyright information

Copyright © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

6.3 bundle, installation package for Red Hat Enterprise Linux
contents [7](#)

A

Active Directory
 using to enable remote authentication [32](#)
adding
 alerts [39](#)
 authentication servers [34](#)
 clusters [38](#)
 clusters, volumes, SVMs to favorites list [42](#)
 favorites [41](#)
administrative operations
 for Unified Manager in Red Hat Enterprise Linux [61](#)
aggregates
 configuring global threshold values for [36](#)
alerts
 adding [39](#)
 configuring your environment for [31](#)
 creating [39](#)
authentication
 adding servers [34](#)
 testing for remote users and groups [35](#)
authentication, remote
 disabling nested groups [33](#)
 enabling [32](#)
AutoSupport
 what it does [9](#)

B

backup and restore
 managing [54](#)
backups
 configuring database settings [54](#)
 database, description of [54](#)
 restoring database on Linux [55](#)

C

certificates
 regenerating HTTPS [61](#)
cluster services
 resources added to Unified Manager [51](#)
clustered Data ONTAP systems
 See clusters
clusters
 adding [38](#)
 adding to favorites list [42](#)
 viewing discovery status [38](#)
comments
 how to send feedback about documentation [74](#)
configuration
 of initial settings following product installation on Red Hat Enterprise Linux [30](#)
configuration options

 after initial software setup [31](#)
 after installing Unified Manager [30](#)
configuring
 aggregate global threshold values [36](#)
 database backup settings [54](#)
 EPEL repository manually [28](#)
 notification settings [32](#)
 thresholds [35](#)
 Unified Manager using scripts [50](#)
 volume global threshold values [36](#)
connection refused
 troubleshooting [70](#)
connection settings
 changing [46](#)
connection setup
 between Unified Manager and Workflow Automation [47](#)
connections
 introduction to setting up between Performance Manager and Unified Manager [42](#)
 server [42](#)
creating
 alerts [39](#)

D

data directory
 adding extra disk space [64](#)
database backup
 description [54](#)
database user roles
 Integration Schema, Report Schema [48](#)
database users
 creating [37](#), [48](#)
databases
 configuring backup settings [54](#)
 restore, describing [55](#)
 restoring backup on Linux [55](#)
deleting
 connection between Performance Manager and Unified Manager [47](#)
discovery
 viewing the status of clusters [38](#)
disk space
 adding to the data directory [64](#)
documentation
 how to receive automatic notification of changes to [74](#)
 how to send feedback about [74](#)
download
 of Unified Manager for Red Hat Enterprise Linux on fully configured systems [24](#)
download process
 for Unified Manager for Red Hat Enterprise Linux on partially configured systems [20](#)
 for Unified Manager for Red Hat Enterprise Linux on blank systems [17](#)

E

- editing
 - unmanaged relationship lag threshold settings [37](#)
- EPEL repositories
 - configuring manually [28](#)

F

- failure notification, false
 - when installing Red Hat Enterprise Linux [70](#)
- Favorites list
 - managing storage objects from [41](#)
- feedback
 - how to send comments about documentation [74](#)
- full integration connections
 - configuring [43](#)

G

- groups
 - testing remote authentication [35](#)
- groups, nested
 - disabling remote authentication of [33](#)

H

- high availability
 - configuring Unified Manager with VCS [50](#)
 - introduction to setting up Unified Manager for, in VCS environments [50](#)
 - upgrading Unified Manager [52](#)
- home directory
 - defining [16](#)
- host name
 - changing for Unified Manager in Red Hat Enterprise Linux [61](#)
- HTTPS certificates
 - regenerating [61](#)

I

- information
 - how to send feedback about improving documentation [74](#)
- initial settings
 - configuring after product installation on Red Hat Enterprise Linux [30](#)
- install
 - of Unified Manager for Red Hat Enterprise Linux on fully configured systems [24](#)
- install process
 - for Unified Manager for Red Hat Enterprise Linux on partially configured systems [20](#)
 - for Unified Manager for Red Hat Enterprise Linux on blank systems [17](#)
- installation
 - overview [6](#)
- installation issues
 - maintenance user not created during installation, troubleshooting [70](#)
- installation package for Red Hat Enterprise Linux

- contents [7](#)
- installation, Unified Manager
 - in VCS setup [6](#)
 - on Red Hat Enterprise Linux [6](#)
- installing
 - Unified Manager in VCS [27](#)
 - Unified Manager on Red Hat Enterprise Linux [16](#)
- integrated connections
 - configuring full [43](#)
 - configuring partial [45](#)
- intermittent cluster connectivity
 - troubleshooting [70](#)
- issue resolution
 - what AutoSupport does [9](#)

J

- jboss
 - users created in Unified Manager [28](#)
- JBoss password
 - changing [67](#)

L

- lag threshold settings
 - editing for unmanaged relationships [37](#)
- license requirements
 - to install Unified Manager on Red Hat Enterprise for Linux [10](#)
- Linux
 - configuring EPEL repository manually for Unified Manager installation [28](#)
 - restoring database backup [55](#)
- local users
 - creating [37](#)

M

- maintenance group
 - removing [67](#)
- maintenance user
 - not created during installation, troubleshooting [70](#)
- messages, AutoSupport
 - how used for troubleshooting [9](#)
- modifying
 - unmanaged relationship lag threshold settings [37](#)
- monitoring
 - cluster performance [38](#)
- mysql
 - users created in Unified Manager [28](#)

N

- nested groups
 - disabling remote authentication of [33](#)
- notification
 - adding alerts [39](#)
 - configuring settings [32](#)

O

- OnCommand Administrator user role
 - enabling configuration [30](#)
- OnCommand Workflow Automation
 - setting up a connection with Unified Manager [47](#)
 - setting up connection with Unified Manager [48](#)
- Open LDAP
 - using to enable remote authentication [32](#)
- options, configuration
 - after initial software setup [31](#)

P

- partial integration connections
 - configuring [45](#)
- password, JBoss
 - changing [67](#)
- password, umadmin
 - changing [40](#)
 - setting before installation [16](#)
- performance
 - monitoring for clusters [38](#)
- Performance Manager
 - changing a connection to a Unified Manager server [46](#)
 - configuring full integration connection to a Unified Manager server [43](#)
 - configuring partial integration connection to a Unified Manager server [45](#)
 - connection to Unified Manager [6](#)
 - deleting a connection to a Unified Manager server [47](#)
 - introduction to setting up a connection to Unified Manager [42](#)
- Performance Manager bundle, installation package for Red Hat Enterprise Linux
 - contents [7](#)
- performance monitoring
 - changing connections between Performance Manager and Unified Manager [46](#)
 - configuring full integration connection between Performance Manager and Unified Manager [43](#)
 - configuring partial integration connection between Performance Manager and Unified Manager [45](#)
 - deleting connections between Performance Manager and Unified Manager [47](#)
 - disabling [47](#)
 - enabling [43](#), [45](#), [46](#)
- physical storage
 - adding clusters [38](#)
- privileges
 - creating a user with the Event Publisher role [43](#)

R

- Red Hat Enterprise Linux
 - and running Unified Manager on [7](#)
 - content of installation package [7](#)
 - installation and setup on [6](#)
- Red Hat program modules
 - and installing Unified Manager on Linux [7](#)
- relationships, unmanaged

- editing lag thresholds settings for [37](#)
- remote authentication
 - disabling nested groups [33](#)
 - enabling [32](#)
- remote groups
 - adding [37](#)
 - testing authentication [35](#)
- remote users
 - adding [37](#)
 - testing authentication [35](#)
- removing
 - favorites [41](#)
 - Unified Manager from Red Hat Enterprise Linux [63](#)
- reports
 - creating a database user with the Report Schema role [48](#)
- repositories
 - required third-party [11](#)
- repositories, EPEL
 - configuring manually [28](#)
- requirements
 - for configuring Unified Manager in VCS [14](#)
 - to install Unified Manager on Red Hat Enterprise for Linux [10](#)
- restarting Unified Manager
 - In Red Hat Enterprise Linux [61](#)
- restore
 - database, description [55](#)
- restoring
 - database backup on Linux [55](#)
- role, Event Publisher
 - creating a user having [43](#)
- roles
 - assigning to users [37](#)
 - purpose of umadmin [8](#)
- RPMs
 - See Red Hat program modules
- rrdcache
 - users created in Unified Manager [28](#)

S

- scripts
 - using to set up Unified Manager in VCS [50](#)
- servers
 - connecting [42](#)
- setting up
 - aggregate global threshold values [36](#)
 - notification settings [32](#)
 - SMTP server [32](#)
 - SNMP [32](#)
 - thresholds [35](#)
 - volume global threshold values [36](#)
- setting up connections
 - between Performance Manager and Unified Manager, introduction to [42](#)
- settings, connection
 - setting [46](#)
- settings, initial
 - configuring after product installation on Red Hat Enterprise Linux [30](#)
- settings, lag threshold
 - editing for unmanaged relationships [37](#)

- setup, Unified Manager
 - in VCS environment [6](#)
 - on Red Hat Enterprise Linux [6](#)
- signed package requirement
 - stopping installation [69](#)
- software
 - required third-party [11](#)
- software requirements
 - to install Unified Manager on Red Hat Enterprise for Linux [11](#)
- stopping Unified Manager
 - in Red Hat Enterprise Linux [61](#)
- storage objects
 - adding to favorites [42](#)
- suggestions
 - how to send feedback about documentation [74](#)
- support bundle for Unified Manager
 - generating in Red Hat Enterprise Linux [64](#)
- SVMs
 - adding to favorites list [42](#)
- system requirements
 - to install Unified Manager on Red Hat Enterprise for Linux [10](#)

T

- testing
 - authentication for remote users and groups [35](#)
- third-party-dependencies bundle, installation package
 - for Red Hat Enterprise Linux
 - contents [7](#)
- threshold settings, lag
 - editing for unmanaged relationships [37](#)
- thresholds
 - configuring [35](#)
 - global values for aggregates [36](#)
 - global values for volumes [36](#)
- troubleshooting
 - connection refused [70](#)
 - installation failure notification [70](#)
 - intermittent cluster connectivity [70](#)
 - Unified Manager fails to create a maintenance user
 - during installation [70](#)
 - what AutoSupport does [9](#)
- Twitter
 - how to receive automatic notification of
 - documentation changes [74](#)

U

- umadmin
 - users created in Unified Manager [28](#)
- umadmin password
 - changing [40](#)
 - setting before installation [16](#)
- umadmin user
 - removing [67](#)
- umadmin users
 - necessity of password [8](#)
 - purpose [8](#)
- Unified Manager
 - configuring using scripts in VCS [50](#)

- connection to Performance Manager [6](#)
 - contents of installation package for Red Hat Enterprise Linux [7](#)
 - high-availability setup [16](#)
 - installing in VCS [27](#)
 - introduction to setting up high availability in VCS environments [50](#)
 - moving data files from /data to /opt/netapp/data [66](#)
 - overview of upgrade on Red Hat Enterprise Linux [56](#)
 - software requirements [11](#)
 - stopping and restarting in Red Hat Enterprise Linux [61](#)
 - system requirements [10](#)
 - upgrading [56, 57](#)
 - upgrading for high availability [52](#)
 - upgrading Red Hat Enterprise Linux 6.x to 7.x [59](#)
- Unified Manager in VCS
 - cluster service resources [51](#)
 - configuration requirements [14](#)
- Unified Manager installation
 - failure due to incorrect MySQL version or vendor [69](#)
 - installation requirement
 - Unified Manager [12](#)
 - requirements [12](#)
- Unified Manager installation in Red Hat Enterprise Linux
 - false failure notification [70](#)
- uninstalling
 - Unified Manager from Red Hat Enterprise Linux [63](#)
- unmanaged relationships
 - editing lag thresholds settings for [37](#)
- upgrade process
 - for Unified Manager on Red Hat Enterprise Linux [56](#)
- upgrading
 - Performance Manager, workflow [56](#)
 - Red Hat Enterprise Linux 6.x to 7.x [59](#)
 - to Unified Manager [56, 57](#)
 - Unified Manager for high availability [52](#)
- user roles
 - assigning [37](#)
- users
 - adding [37](#)
 - created in Unified Manager [28](#)
 - creating [37](#)
 - creating having the Event Publisher role [43](#)
 - purpose of umadmin [8](#)
 - testing remote authentication [35](#)
- users, database
 - creating [48](#)

V

- VCS
 - configuration requirements [14](#)
 - installing Unified Manager in [27](#)
 - setting up Unified Manager using scripts [50](#)
- viewing
 - discovery status of clusters [38](#)
 - Favorites list [41](#)
- volumes
 - adding to favorites list [42](#)
 - configuring global threshold values for [36](#)

W

Workflow Automation

- creating a database user with the Integration Schema role [48](#)

- setting up a connection with Unified Manager [47](#)

- setting up connection with Unified Manager [48](#)