



Active IQ Unified Manager 9.6 Installation Guide



First Edition (June 2019)

© Copyright Lenovo 2019.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to a General Services Administration (GSA) contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925

Contents

About this manualiii
------------------------------------	-------------

Chapter 1. Introduction to Active IQ Unified Manager 1

What the Unified Manager server does	1
Active IQ Unified Manager product documentation	1
Overview of the installation sequence	2

Chapter 2. Requirements for installing Unified Manager 3

Virtual infrastructure and hardware system requirements	3
VMware software and installation requirements	4
Linux software and installation requirements	5
Windows software and installation requirements	7
Supported browsers	8
Protocol and port requirements.	8
Completing the worksheet	9

Chapter 3. Installing, upgrading, and removing Unified Manager software on VMware vSphere 13

Overview of the deployment process on VMware	13
Deploying Unified Manager	13
Downloading the Unified Manager OVA file	14
Deploying the Unified Manager virtual appliance	14
Upgrading Unified Manager on VMware	16
Downloading the Unified Manager ISO image	17
Upgrading the Unified Manager virtual appliance	17
Restarting the Unified Manager virtual machine	18
Removing Unified Manager from VMware.	19

Chapter 4. Installing, upgrading, and removing Unified Manager software on Red Hat or CentOS. 21

Overview of the installation process on Red Hat or CentOS	21
Setting up required software repositories	21
Manually configuring the EPEL repository	21
Manually configuring the MySQL repository	22
SELinux requirements for mounting /opt/netapp or /opt/netapp/data on an NFS or CIFS share.	22
Installing Unified Manager on Red Hat Enterprise Linux or CentOS	23

Creating a custom user home directory and umadmin password prior to installation	23
Downloading Unified Manager for Red Hat Enterprise Linux or CentOS	24
Installing Unified Manager on Red Hat Enterprise Linux or CentOS	25
Users created during Unified Manager installation	27
Changing the JBoss password on Linux	27
Setting up Unified Manager for high availability	28
Requirements for Unified Manager in VCS.	28
Installing Unified Manager on VCS.	29
Configuring Unified Manager with VCS using configuration scripts	29
Unified Manager service resources for VCS configuration	30
Updating an existing Unified Manager setup for high availability	31
Upgrading Unified Manager on Red Hat Enterprise Linux or CentOS	31
Upgrading Unified Manager on Red Hat Enterprise Linux or CentOS	32
Upgrading the host OS from Red Hat Enterprise Linux 6.x to 7.x	34
Upgrading third-party products on Linux	35
Upgrading JRE on Linux	35
Upgrading MySQL on Linux	35
Restarting Unified Manager in Red Hat Enterprise Linux or CentOS	36
Removing Unified Manager from the Red Hat Enterprise Linux or CentOS host	37
Removing the custom umadmin user and maintenance group	37

Chapter 5. Installing, upgrading, and removing Unified Manager software on Windows 39

Overview of the installation process on Windows	39
Installing Unified Manager on Windows	39
Installing Unified Manager on a Windows system	39
Performing an unattended installation of Unified Manager on Windows	40
Setting up Unified Manager in a failover clustering environment	41
Requirements for Unified Manager in a failover clustering environment	42
Installing Unified Manager on MSCS	42
Configuring Unified Manager server with MSCS using configuration scripts	43

Changing the JBoss password on Windows. . . .	44
Upgrading Unified Manager on Windows	45
Upgrading third-party products on Windows . . .	47
Upgrading JRE on Windows	47
Upgrading MySQL on Windows.	47
Restarting Unified Manager on Windows	48

Uninstalling Unified Manager from Windows . . .	48
---	----

Appendix A. Contacting Support . . . 51

Appendix B. Notices. 53

Trademarks	54
----------------------	----

About this manual

Lenovo does not have support for the following so ignore all references and related procedures:

- Citrix
- Veritas Cluster Server (VCS)
- SnapDrive for Unix
- Veritas Operations Manager

Note: Ignore the following guide mentioned in this manual: *Veritas Cluster Server 6.2.1. Installation Guide*

All references to reference the Interop Matrix may be ignored. Lenovo does not support this online ability.

It is Lenovo's recommendation to change all default passwords on first access that adheres to the password recommendations:

- Contains at least 1 letter
- Contains at least 1 number
- Contains at least 2 of the following:
 - Upper case letter
 - Lower case letter
 - Special character
- Should not be a repeat or be the reverse of the username

Chapter 1. Introduction to Active IQ Unified Manager

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

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

What the Unified Manager server does

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

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

Active IQ Unified Manager product documentation

Active IQ Unified Manager is accompanied by a set of guides that describe how to install and use the product. Online help is also provided in the user interface.

Installing Unified Manager

Provides installation, upgrade, and setup instructions for Unified Manager on the VMware, Linux, and Windows platforms.

Configuring Unified Manager

Provides initial setup and configuration instructions for Unified Manager. This includes adding clusters, adding users, configuring alerts, and setting up remote authentication.

Workflows for managing cluster health

Provides information about using Unified Manager to manage and troubleshoot cluster storage health issues. This guide also describes how to use the Unified Manager maintenance console to perform special operations such as restoring a database backup and connecting to an external data provider to offload performance statistics.

Workflows for managing cluster performance

Provides information about using Unified Manager to manage and troubleshoot cluster storage performance issues. This includes identifying workloads that are overusing cluster components so that you can take corrective action to bring performance back to normal levels of operation.

Generating custom reports

Provides information about using Unified Manager to create custom reports about the capacity, health, performance, and protection status of your ONTAP storage objects. This includes scheduling the report for delivery to specified users on a regular schedule through email.

Active IQ Unified Manager Online Help

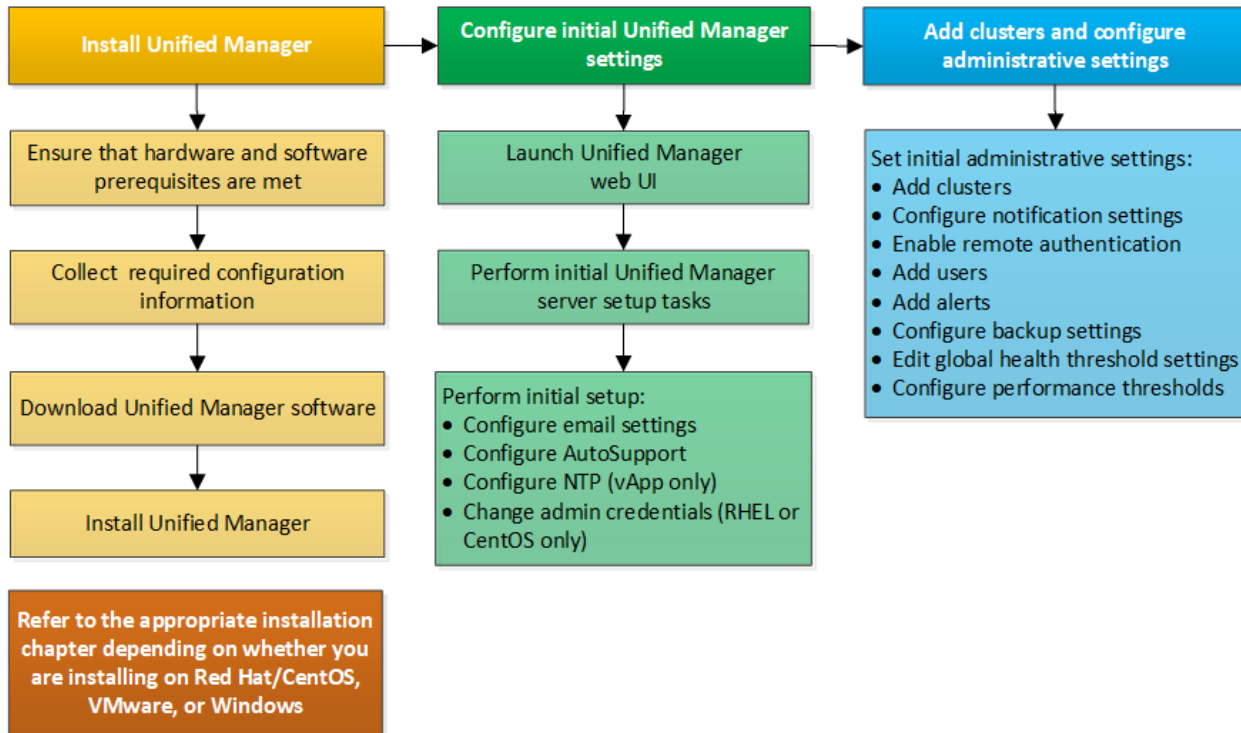
Provides information about using Unified Manager to manage and troubleshoot cluster storage health and performance issues. Additionally, it provides field level descriptions for every UI page in the product.

The online help is included with the software, and is also available as a PDF document that you can review offline.

Overview of the installation sequence

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

The chapters of this installation guide describe each of the items shown in the workflow below.



Chapter 2. Requirements for installing Unified Manager

Before you can install Active IQ Unified Manager you must ensure that the server on which you plan to install Unified Manager meets specific software, hardware, CPU, and memory requirements.

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

Virtual infrastructure and hardware system requirements

Depending on whether you are installing Unified Manager on virtual infrastructure or on a physical system, it must meet minimum requirements for memory, CPU, and disk space.

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

Hardware configuration	Recommended settings
RAM	12 GB (minimum requirement 8 GB)
Processors	4 CPUs
CPU cycle capacity	9572 MHz total (minimum requirement 9572 MHz)
Free disk space	VMware: <ul style="list-style-type: none">• 5 GB (thin provisioned)• 152 GB (thick provisioned)
	Red Hat or CentOS: 150 GB, where the capacity is allocated as follows: <ul style="list-style-type: none">• 50 GB allotted to the root partition• 100 GB of free disk space allotted to the <code>/opt/netapp/data</code> directory, which is mounted on an LVM drive or on a separate local disk attached to the target system Note: The <code>/tmp</code> directory should have at least 10 GB of free space and the <code>/var/log</code> directory should have at least 16 GB of free space.
	Windows: 150 GB, where the capacity is allocated as follows: <ul style="list-style-type: none">• 100 GB of disk space for the installation directory• 50 GB of disk space for the MySQL data directory

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

Additionally, there is a limit to the number of nodes that a single instance of Unified Manager can monitor before you need to install a second instance of Unified Manager.

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

Dedicated use requirement

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

Space requirements for backups

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

Host connectivity requirements

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

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

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

Mounted /opt/netapp or /opt/netapp/data requirements

You can mount /opt/netapp or /opt/netapp/data on an NAS or SAN device. Note that using remote mount points may cause scaling issues. If you do use a remote mount point, ensure that your SAN or NAS network has sufficient capacity to meet the I/O needs of Unified Manager. This capacity will vary and may increase based on the number of clusters and storage objects you are monitoring.

If you have mounted /opt/netapp or /opt/netapp/data from anywhere other than the root file system, and you have SELinux enabled in your environment, you must set the correct context for the mounted directories.

See the topic “SELinux requirements for mounting /opt/netapp or /opt/netapp/data on an NFS or CIFS share” on page 22 for information about setting the correct SELinux context.

VMware software and installation requirements

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

Operating system software

The following versions of VMware ESXi are supported:

- ESXi 6.0, 6.5, and 6.7

The following versions of vSphere are supported:

- VMware vCenter Server 6.0, 6.5, and 6.7

See the Interoperability Matrix for the complete and most current list of supported ESXi versions.

<https://datacentersupport.lenovo.com/>

The VMware ESXi server time must be the same as the NTP server time for the virtual appliance to function correctly. Synchronizing the VMware ESXi server time with the NTP server time prevents a time failure.

Installation requirements

VMware High Availability for the Unified Manager virtual appliance is supported.

If you deploy an NFS datastore on a storage system that is running ONTAP software, you must use the Lenovo NFS Plug-in for VMware VAAI to use thick provisioning.

If deployment fails using your High Availability-enabled environment because of insufficient resources, you may need to modify the Cluster Features Virtual Machine Options by disabling the VM Restart Priority, and leaving the Host Isolation Response powered on.

Linux software and installation requirements

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

Operating system software

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

- Red Hat Enterprise Linux or CentOS version 7.x based on x86_64 architecture

Red Hat Enterprise Linux 6.x is not supported starting with Unified Manager 9.4.

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

<https://datacentersupport.lenovo.com/>

Third-party software

The following third-party packages are required. These packages are automatically installed by the **yum** installer during installation, provided you have configured the repositories as mentioned in the following sections.

- MySQL Community Edition version 5.7.26 or later versions in the 5.7 family (from the MySQL repository)
- OpenJDK version 11.0.3 (from the Red Hat Extra Enterprise Linux Server repository)

Note: Oracle Java is not supported starting with Unified Manager 9.5.

- p7zip version 16.02 or later (from the Red Hat Extra Packages for Enterprise Linux repository)

Note: If you plan to upgrade any of the third-party software after Unified Manager has been running, you must shut down Unified Manager first. After the third-party software installation is complete, you can restart Unified Manager.

User authorization requirements

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

Installation requirements

The best practices for installing Red Hat Enterprise Linux or CentOS and the associated repositories on your system are listed below. Systems installed or configured differently, or deployed off premise (in the cloud), may require additional steps, and Unified Manager may not run properly in such deployments.

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

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

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

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

“Manually configuring the EPEL repository” on page 21

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

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

“Manually configuring the MySQL repository” on page 22

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

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

Port 443 requirement

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

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

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

```
# sudo yum install firewalld
```

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

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

Windows software and installation requirements

For the successful installation of Unified Manager on Windows, you must ensure that the system on which Unified Manager is being installed meets the software requirements.

Operating system software

Unified Manager runs only on a 64-bit English language Windows operating system. You can install Unified Manager on the following Windows platforms:

- Microsoft Windows Server 2016 Standard and Datacenter Edition
- Microsoft Windows Server 2019 Standard and Datacenter Edition

The server should be dedicated to running Unified Manager; no other applications should be installed on the server.

Third-party software

The following third-party packages are required:

- Microsoft Visual C++ 2015 Redistributable package version 14.0.24212
- Microsoft Visual C++ Redistributable Packages for Visual Studio 2013 version 12.0.40660
- MySQL Community Edition version 5.7.26, or later versions in the 5.7 family
- OpenJDK version 11.0.3
- p7zip version 18.05 or later

If these third-party packages are not installed, Unified Manager installs them as part of the installation.

Note: Starting with Unified Manager 9.5, OpenJDK is provided in the Unified Manager installation package and installed automatically. Oracle Java is not supported starting with Unified Manager 9.5.

If MySQL is pre-installed, you must ensure that:

- It is using the default port.
- The sample databases are not installed.
- The service name is "MYSQL".

Note: If you plan to upgrade any of the third-party software after Unified Manager has been running, you must shut down Unified Manager first. After the third-party software installation is complete you can restart Unified Manager.

Installation requirements

- Microsoft .NET 4.5.2, or greater, must be installed.
- You must reserve 2 GB of disk space for the temp directory to extract the installation files.
- You must reserve 2 GB of disk space in the Windows drive for caching the Unified Manager MSI files.
- The Microsoft Windows Server on which you want to install Unified Manager must be configured with a fully qualified domain name (FQDN) such that ping responses to the host name and FQDN are successful.
- You must disable Microsoft IIS worldwide web publishing service and ensure that ports 80 and 443 are free.

- You must make sure that the Remote Desktop Session Host setting for “Windows Installer RDS Compatibility” is disabled during the installation.
- UDP port 514 must be free, and must not be used by any other service.

Notes: The Unified Manager installation program configures the following exclusions in Windows Defender:

- Unified Manager data directory
- Unified Manager installation directory
- MySQL data directory

If your server has a different antivirus scanner installed you must configure these exclusions manually.

Supported browsers

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

Unified Manager has been tested with the following browsers; other browsers might work but have not been qualified.

- Mozilla Firefox ESR 60
- Google Chrome version 72 and 73

Note: Microsoft Internet Explorer is no longer supported.

For all browsers, disabling popup blockers helps ensure that software features display properly.

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

Protocol and port requirements

Using a browser, API client, or SSH, the required ports must be accessible to the Unified Manager UI and APIs. The required ports and protocols enable communication between the Unified Manager server and the managed storage systems, servers, and other components.

Connections to the Unified Manager server

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

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

Interface	Protocol	Port	Description
Unified Manager web UI	HTTP	80	Used to access the Unified Manager web UI; automatically redirects to the secure port 443.
Unified Manager web UI and programs using APIs	HTTPS	443	Used to securely access the Unified Manager web UI or to make API calls; API calls can only be made using HTTPS.
Maintenance console	SSH/SFTP	22	Used to access the maintenance console and retrieve support bundles.
Linux command line	SSH/SFTP	22	Used to access the Red Hat Enterprise Linux or CentOS command line and retrieve support bundles.
MySQL database	MySQL	3306	Used to enable ThinkSystem Storage Workflow Automation and OnCommand API Services access to Unified Manager.

Interface	Protocol	Port	Description
Syslog	UDP	514	Used to access subscription-based EMS messages from ONTAP systems and to create events based on the messages.
REST	HTTPS	9443	Used to access realtime REST API-based EMS events from authenticated ONTAP systems.

Note: The ports used for HTTP and HTTPS communication (ports 80 and 443) can be changed using the Unified Manager maintenance console.

Connections from the Unified Manager server

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

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

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

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

Completing the worksheet

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

Unified Manager installation information

The details required to install Unified Manager.

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

Unified Manager configuration information

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

Setting	Your value
Maintenance user email address	
NTP server (VMware only)	
SMTP server host name or IP address	
SMTP user name	
SMTP password	
SMTP port	25 (Default value)
Email from which alert notifications are sent	
Authentication server host name or IP address	
Active Directory administrator name or LDAP bind distinguished name	
Active Directory password or LDAP bind password	
Authentication server base distinguished name	
Identity provider (IdP) URL	
Identity provider (IdP) metadata	
SNMP trap destination host IP addresses	
SNMP port	

Cluster information

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

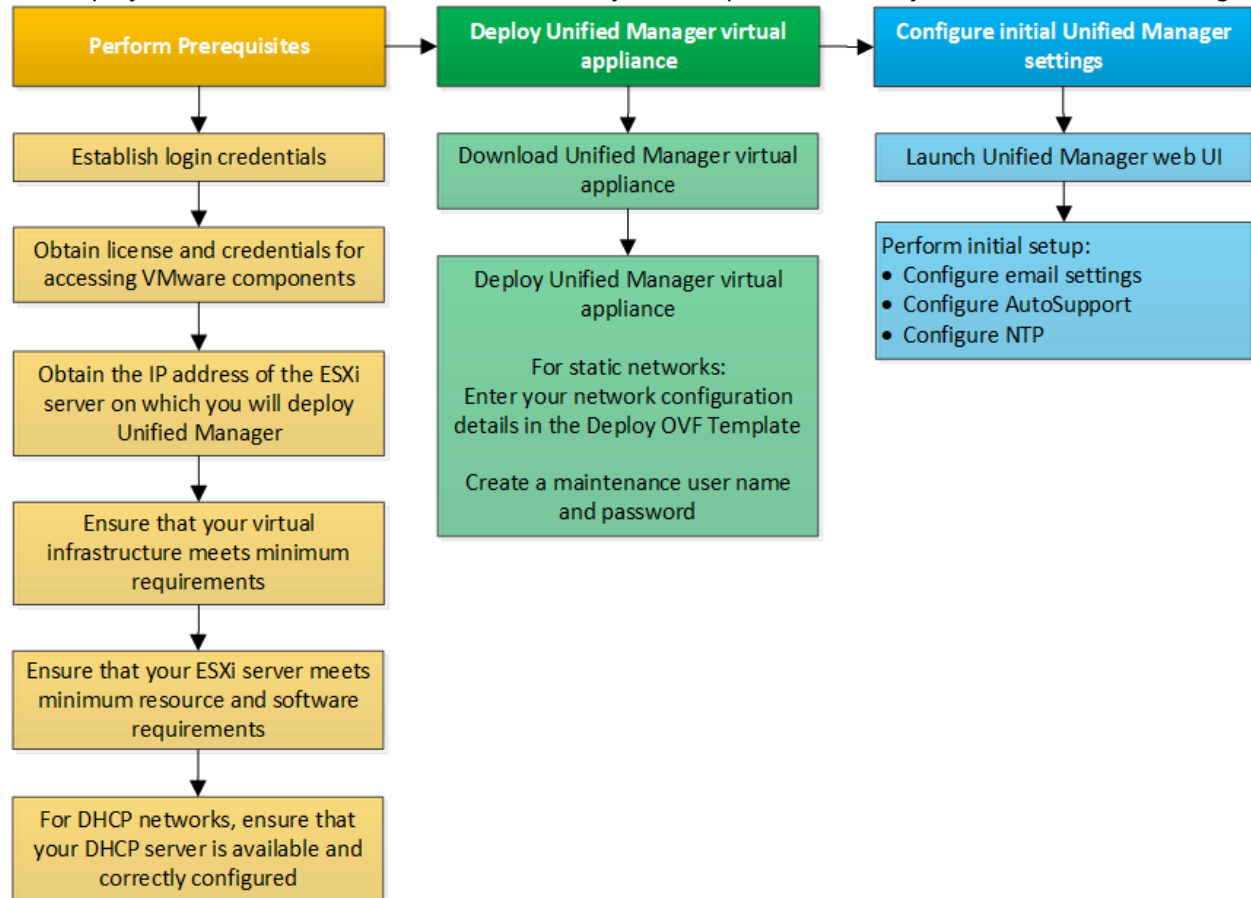
Cluster 1 of N	Your value
Host name or cluster-management IP address	
ONTAP administrator user name Note: The administrator must have been assigned the “admin” role.	
ONTAP administrator password	
Protocol (HTTP or HTTPS)	

Chapter 3. Installing, upgrading, and removing Unified Manager software on VMware vSphere

On VMware vSphere systems, you can install Unified Manager software, upgrade to a newer version of software, or remove the Unified Manager virtual appliance.

Overview of the deployment process on VMware

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



Deploying Unified Manager

Deploying Unified Manager includes downloading software, deploying the virtual appliance, creating a maintenance user name and password, and performing the initial setup in the web UI.

Before you begin

- You must have completed the system requirements for deployment.
 - Chapter 2 “System requirements” on page 3
- You must have the following information:
 - Login credentials for the Lenovo Support Site

- Credentials for accessing the VMware vCenter Server and vSphere Web Client (for vSphere version 6.5 or 6.7) or vSphere Client (for vSphere version 6.0)
- IP address of the ESXi server on which you are deploying the Unified Manager virtual appliance
- Details about the data center, such as storage space in the datastore and memory requirements
- IPv6 must be enabled on the host if you are planning to use IPv6 addressing.
- CD-ROM or ISO image of VMware Tools

About this task

You can deploy Unified Manager as a virtual appliance on a VMware ESXi server.

You must access the maintenance console by using the VMware console, and not by using SSH.

VMware Tools are not included in the Unified Manager .ova file, and must be installed separately.

After you finish

After finishing the deployment and initial setup, you can either add clusters, or configure additional network settings in the maintenance console, and then access the web UI.

Downloading the Unified Manager OVA file

You must download Unified Manager before you can deploy the virtual appliance.

Before you begin

You must have login credentials for the Lenovo Support Site.

About this task

The .ova file contains the Unified Manager software configured in a virtual appliance.

- Step 1. Log in to the Lenovo Support Site, and navigate to the Download page for Unified Manager on VMware vSphere.
<https://datacentersupport.lenovo.com>
- Step 2. Download and save the .ova file to a local directory or network directory that is accessible to your vSphere Client.
- Step 3. Verify the checksum to ensure that the software downloaded correctly.

Deploying the Unified Manager virtual appliance

You must deploy the Unified Manager virtual appliance after downloading it. You must use VMware vSphere Client to deploy the virtual appliance on an ESXi server.

Before you begin

You must have reviewed the system requirements. If changes are required to meet the system requirements, you must implement the changes before deploying the Unified Manager virtual appliance.

Chapter 2 “Requirements for installing Unified Manager ” on page 3

“VMware software and installation requirements” on page 4

If you use DHCP, you must ensure that the DHCP server is available, and that the DHCP and virtual machine (VM) network adapter configurations are correct. DHCP is configured by default.

If you use a static networking configuration, you must ensure that the IP address is not duplicated in the same subnet, and that the appropriate DNS server entries have been configured.

You must have the following information before deploying the virtual appliance:

- Credentials for accessing the VMware vCenter Server and vSphere Web Client (for vSphere version 6.5 or 6.7) or vSphere Client (for vSphere version 6.0)
- IP address of the ESXi server on which you are deploying the Unified Manager virtual appliance
- Details about the data center, such as availability of storage space
- If you are not using DHCP, you must have the IPv4 or IPv6 addresses for the networking devices to which you are planning to connect:
 - Fully qualified domain name (FQDN) of the host
 - IP address of the host
 - Network mask
 - IP address of the default gateway
 - Primary and secondary DNS addresses
 - Search domains
- CD-ROM or ISO image for the VMware Tools

About this task

VMware Tools are not included in the .ova file. You must install the VMware Tools separately.

When the virtual appliance is deployed, a unique self-signed certificate for HTTPS access is generated. When accessing the Unified Manager web UI, you might see a browser warning about untrusted certificates.

VMware High Availability for the Unified Manager virtual appliance is supported.

Step 1. In the vSphere Client, click **File → Deploy OVF Template**.

Step 2. Complete the Deploy OVF Template wizard to deploy the Unified Manager virtual appliance. On the Networking Configuration page:

Leave all the fields blank when using DHCP and IPv4 addressing.

Check the “Enable Auto IPv6 addressing” box, and leave all the other fields blank when using DHCP and IPv6 addressing.

If you want to use a static network configuration, you can complete the fields on this page and these settings are applied during deployment. You must ensure that the IP address is unique to the host on which it is deployed, that it is not already in use, and that it has a valid DNS entry.

Step 3. After the Unified Manager virtual appliance is deployed to the ESXi server, power on the VM by right-clicking the VM, and then selecting **Power On**.

If the Power On operation fails because of insufficient resources, you must add resources and then retry the installation.

Step 4. Click the **Console** tab.

The initial boot process takes a few minutes to complete.

Step 5. Follow the prompt to install the VMware Tools on the VM.

When using the vSphere Web Client with vSphere 6.5 you need to manually mount the VMware Tools ISO image. From the VM you need to select **Edit Settings → Virtual Hardware → CD/DVD drive x → Datastore ISO file** and then click **Browse** to select the file `linux.iso` as the mount image.

Step 6. To configure your time zone, enter your geographic area and your city or region as prompted in the VM Console window.

All the date information that is displayed uses the time zone that is configured for Unified Manager, regardless of the time zone setting on your managed devices. You should be aware of this when comparing time stamps. If your storage systems and the management server are configured with the same NTP server, they refer to the same instant in time, even if they appear differently. For example, if you create a Snapshot copy using a device that is configured using a different time zone than that of the management server, the time reflected in the time stamp is the management server time.

Step 7. If no DHCP services are available, or if there is an error in the details for the static network configuration, select one of the following options:

If you use...	Then do this...
DHCP	<p>Select Retry DHCP.</p> <p>If you plan to use DHCP, you should ensure that it is configured correctly.</p> <p>If you use a DHCP-enabled network, the FQDN and DNS server entries are given to the virtual appliance automatically. If DHCP is not properly configured with DNS, the host name “UnifiedManager” is automatically assigned and associated with the security certificate. If you have not set up a DHCP-enabled network, you must manually enter the networking configuration information.</p>
A static network configuration	<ol style="list-style-type: none">1. Select Enter the details for static network configuration. <p>The configuration process takes a few minutes to complete.</p> <ol style="list-style-type: none">2. Confirm the values that you entered, and select Y.

Step 8. At the prompt, enter a maintenance user name, and click **Enter**.
The maintenance user name must start with a letter from a-z, followed by any combination of -, a-z, or 0-9.

Step 9. At the prompt, enter a password, and click **Enter**.
The VM console displays the URL for the Unified Manager web UI.

Upgrading Unified Manager on VMware

You can upgrade to Unified Manager version 9.6 only from instances of 9.4 or 9.5.

About this task

During the upgrade process, Unified Manager is unavailable. You should complete any running operations before upgrading Unified Manager.

If Unified Manager is paired with an instance of workflow automation, and there are new versions of software available for both products, you must disconnect the two products and then set up a new connection after

performing the upgrades. If you are performing an upgrade to only one of the products, then you should log into Workflow Automation after the upgrade and verify that it is still acquiring data from Unified Manager.

Downloading the Unified Manager ISO image

Before upgrading to Unified Manager, you must first download the software.

Before you begin

You must have login credentials for the Lenovo Support Site.

- Step 1. Log in to the Lenovo Support Site and navigate to the Software Download page.
<https://datacentersupport.lenovo.com>
- Step 2. Download and save the .iso image file to a local directory or network directory that is accessible to your vSphere Client.
- Step 3. Verify the checksum to ensure that the software downloaded correctly.

Upgrading the Unified Manager virtual appliance

You can upgrade your Unified Manager software from previous Unified Manager releases.

Before you begin

- You must have downloaded the .iso file from the Lenovo Support Site.
- The system on which you are upgrading Unified Manager must meet the system and software requirements.
Chapter 2 “Virtual infrastructure requirements” on page 3
“VMware software and installation requirements” on page 4
- For vSphere 6.5 and 6.7 users, you must have installed the VMware Remote Console (VMRC).
- You must have the following information:
 - Login credentials for the Lenovo Support Site
 - Credentials for accessing the VMware vCenter Server and vSphere Web Client (for vSphere version 6.5 or 6.7) or vSphere Client (for vSphere version 6.0)
 - Credentials for the Unified Manager maintenance user

About this task

During the upgrade process, Unified Manager is unavailable. You should complete any running operations before upgrading Unified Manager.

If you have paired Workflow Automation and Unified Manager, you must manually update the host name in Workflow Automation.

- Step 1. In the vSphere Client, click **Home → Inventory → VMs and Templates**.
- Step 2. Select the virtual machine (VM) on which the Unified Manager virtual appliance is installed.
- Step 3. If the Unified Manager VM is running, navigate to **Summary → Commands → Shut Down Guest**.
- Step 4. Create a backup copy—such as a snapshot or clone—of the Unified Manager VM to create an application-consistent backup.
- Step 5. From the vSphere Client, power on the Unified Manager VM.
- Step 6. Select the Unified Manager upgrade image:

If you are using...	Then do this...
vSphere 6.0	<ol style="list-style-type: none"> 1. Click the CD/DVD Drive icon, and select Connect to ISO image on local disk. 2. Select the ActiveIQUnifiedManager-9.6-virtual-update.iso file, and click Open.
vSphere 6.5 or 6.7	<ol style="list-style-type: none"> 1. Launch the VMware Remote Console. 2. Click the CDROM icon, and select Connect to Disk Image File (.iso). 3. Select the ActiveIQUnifiedManager-9.6-virtual-update.iso file, and click Open.

- Step 7. Click the **Console** tab.
- Step 8. Log in to the Unified Manager maintenance console.
- Step 9. In the Main Menu, select **Upgrade**.
A message is displayed that Unified Manager will be unavailable during the upgrade process, and will resume after completion.
- Step 10. Type **y** to continue.
A warning is displayed, reminding you to back up the virtual machine on which the virtual appliance resides.
- Step 11. Type **y** to continue.
The upgrade process and the restart of Unified Manager services can take several minutes to complete.
- Step 12. Press any key to continue.
You are automatically logged out of the maintenance console.
- Step 13. Optional: Log in to the maintenance console, and verify the version of Unified Manager.

After you finish

You can log in to the web UI to use the upgraded version of Unified Manager. Note that you must wait for the discovery process to finish before performing any task in the UI.

Restarting the Unified Manager virtual machine

You can restart the Unified Manager virtual machine (VM) from the maintenance console. You must restart the VM after generating a new security certificate, or if there is a problem with the VM.

Before you begin

- The virtual appliance must be powered on.
- You must be logged in to the Unified Manager maintenance console as the maintenance user.

About this task

You can also restart the virtual machine from vSphere by using the VMware **Restart Guest** option.

- Step 1. In the maintenance console, select **System Configuration → Reboot Virtual Machine**.
- Step 2. Start the Unified Manager graphical user interface (GUI) from your browser, and log in.

Removing Unified Manager from VMware

You can uninstall Unified Manager by destroying the virtual appliance on which the Unified Manager software is installed.

Before you begin

- You must have credentials for accessing VMware vCenter Server and vSphere Web Client (for vSphere version 6.5 or 6.7) or vSphere Client (for vSphere version 6.0).
- The Unified Manager server must not have an active connection to a Workflow Automation server.

If there is an active connection, you must delete the connection by using the Administration menu.

- All clusters (data sources) must be removed from the Unified Manager server before you delete the virtual machine (VM).

Step 1. Use the Unified Manager maintenance console to verify that the Unified Manager server does not have an active connection to an external data provider.

Step 2. In the vSphere Client, click **Home → Inventory → VMs and Templates**.

Step 3. Select the VM that you want to destroy, and click the **Summary** tab.

Step 4. If the VM is running, click **Power → Shut Down Guest**.

Step 5. Right-click the VM that you want to destroy, and click **Delete from Disk**.

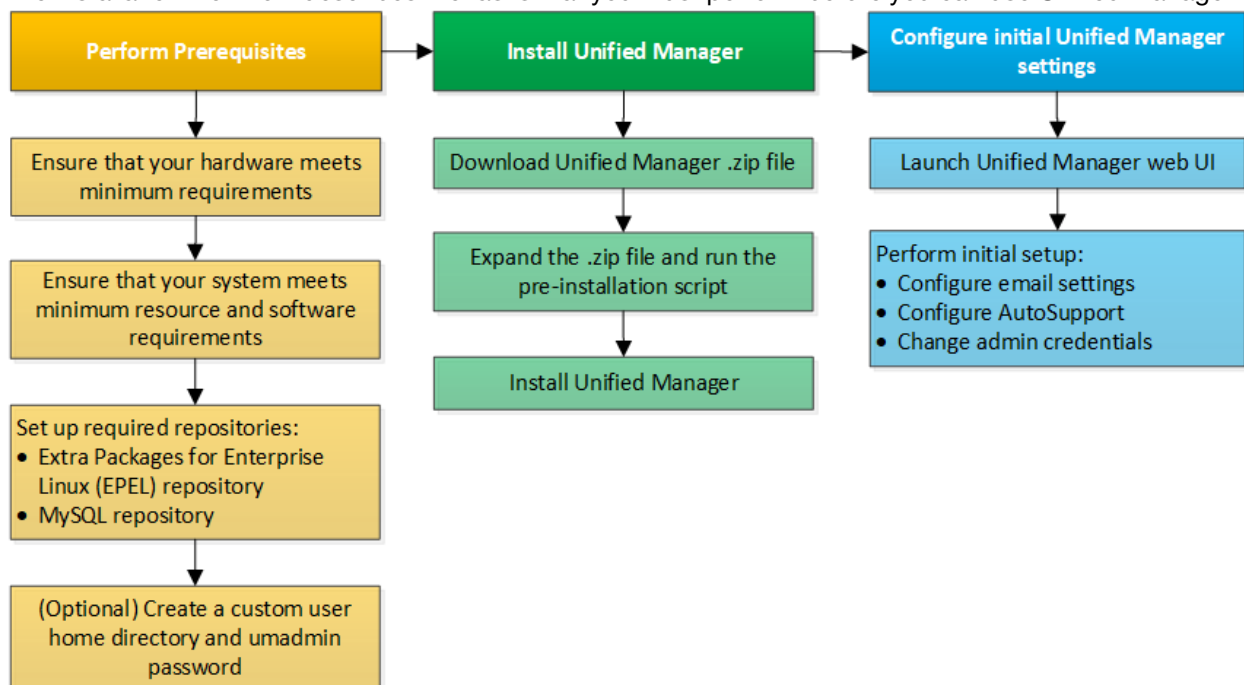
Chapter 4. Installing, upgrading, and removing Unified Manager software on Red Hat or CentOS

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

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

Overview of the installation process on Red Hat or CentOS

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



Setting up required software repositories

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

Manually configuring the EPEL repository

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

About this task

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

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

Manually configuring the MySQL repository

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

About this task

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

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

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

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

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

About this task

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

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

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

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

1. Run this command to check the context:
`ls -dZ /opt/netapp/data`

A sample output:

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

In this output, the context is **default_t** that must be changed to **mysqld_db_t**.

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

```
semanage fcontext -a -t mysql_db_t "/opt/netapp/data"
restorecon -R -v /opt/netapp/data
```

- b. If you have configured `/opt/netapp/data` in `/etc/fstab`, you must edit the `/etc/fstab` file. For the `/opt/netapp/data/` mount option, add the MySQL label as:
`context=system_u:object_r:mysql_db_t:s0`
 - c. Unmount and remount `/opt/netapp/data/` for enabling the context.
 - d. If you have a direct NFS mount, run the following command to set the context to **mysql_db_t**:
`0mount <nfsshare>:/<mountpoint> /opt/netapp/data -o context=system_u:object_r:mysql_db_t:s0`
3. Verify whether the context is set correctly: `ls -dZ /opt/netapp/data/`
`drwxr-xr-x. mysql root unconfined_u:object_r:mysql_db_t:s0 /opt/netapp/data/`

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

After setting the correct context for `/opt/netapp/data/`, ensure that the parent directory `/opt/netapp` does not have the SELinux context set to **file_t**.

1. Run this command to check the context: `ls -dZ /opt/netapp`

A sample output:

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

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

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

Installing Unified Manager on Red Hat Enterprise Linux or CentOS

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

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

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

Before you begin

- The system must meet the requirements described in “Virtual infrastructure and hardware system requirements” on page 3.
- You must be able to log in as the root user to the Red Hat Enterprise Linux or CentOS system.

About this task

The default Unified Manager installation performs the following tasks:

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

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

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

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

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

No security policies should restrict sudo privileges for the Unified Manager maintenance user or some Unified Manager operations will fail. Verify that you are able to run the following sudo command when logged in as the umadmin user after successful installation.

`sudo /etc/init.d/ocie status` This command should return the appropriate status of the ocie service without any issues.

Step 1. Log in as the root user to the server.

Step 2. Create the umadmin group account called “maintenance”:
`groupadd maintenance`

Step 3. Create the user account “umadmin” in the maintenance group under a home directory of your choice:
`adduser --home <home_directory> -g maintenance umadmin`

Step 4. Define the umadmin password:
`passwd umadmin`
The system prompts you to enter a new password string for the umadmin user.

After you finish

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

Downloading Unified Manager for Red Hat Enterprise Linux or CentOS

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

Before you begin

You must have login credentials for the Lenovo Support Site.

About this task

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

- Step 1. Log in to the Lenovo Support Site, and navigate to the Download page for Unified Manager on the Red Hat Enterprise Linux platform.
<https://datacentersupport.lenovo.com>
- Step 2. Download the Unified Manager .zip file to a directory on the target system.
- Step 3. Verify the checksum to ensure that the software downloaded correctly.

Installing Unified Manager on Red Hat Enterprise Linux or CentOS

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

Before you begin

- The system on which you want to install Unified Manager must meet the system and software requirements.
 “Hardware system requirements” on page 3
 “Linux software and installation requirements” on page 5
- You must have downloaded the Unified Manager .zip file from the Lenovo Support Site to the target system.
- You must have a supported web browser.
- Your terminal emulation software must have scrollbar enabled.

About this task

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

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

Required software and minimum version	Command to verify software and version
OpenJDK version 11.0.3	java -version
MySQL 5.7.26 Community Edition	rpm -qa grep -i mysql
p7zip 16.02	rpm -qa grep p7zip

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

Software to uninstall	Command to uninstall the software
MySQL Note: Uninstall any version of MySQL that is older than 5.7.26 Community Edition.	rpm -e <mysql_package_name> Note: If you receive dependency errors, you must add the --nodeps option to uninstall the component.
All other modules	yum remove module_name

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

unzip ActiveIQUnifiedManager-9.6.zip

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

Step 5. Verify that the following modules are available in the directory:

ls *.rpm

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

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

sudo ./pre_install_check.sh

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

Note: You must perform Step 7 on page 26 *only* if you are required to manually download the packages that are required for your installation. If your system has Internet access and all the required packages are available, go to Step 8 on page 26.

Step 7. Optional: For systems that are not connected to the Internet or that are not using the Red Hat Enterprise Linux repositories, perform the following steps to determine whether you are missing any required packages, and then download those packages:

a. On the system on which you are installing Unified Manager, view the list of available and unavailable packages:

yum install *.rpm --assumeno

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

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

yum install <package_name> --downloadonly --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.

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

yum install *.rpm

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

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

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

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

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

The message is similar to the following:

Active IQ Unified Manager installed successfully.

Use a web browser and one of the following URL(s) to configure and access the Unified Manager GUI.

`https://default_ip_address/` (if using IPv4)

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

`https://fully_qualified_domain_name/`

Log in to Unified Manager in a web browser by using following details:

username: umadmin

password: admin

Step 11. Record the IP address or URL, the assigned user name (umadmin), and the current password.

Step 12. If you created a umadmin user account with a custom home directory prior to installing Unified Manager, then you must specify the umadmin user login shell:

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

Users created during Unified Manager installation

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

umadmin

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

jboss

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

mysql

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

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

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

Changing the JBoss password on Linux

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

Before you begin

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

Step 1. Log in as root user on the system.

Step 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.

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

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

Step 4. When prompted, enter the old JBoss password.

The default password is D11h1aMu@79%.

Step 5. When prompted, enter the new JBoss password, and then enter it a second time for confirmation.

Step 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
```

Step 7. After all of the services are started, you can log in to the Unified Manager UI.

Setting up Unified Manager for high availability

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

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

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

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

Requirements for Unified Manager in VCS

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

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

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

You must also ensure that the FC link is active and that the LUNs created on the storage systems are accessible to both the cluster nodes.

- The shared data disk must have enough space (minimum 80 GB) for the Unified Manager database, reports, certificates, and script plug-in folders.
- A minimum of two network interfaces must be set up on each system: one for node-to-node communication and the other for node-to-client communication.

The name of the network interface used for node-to-client communication must be the same on both the systems.

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

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

- Additional RAM must be available for the SnapDrive and VCS applications.

Installing Unified Manager on VCS

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

Before you begin

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

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

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

About this task

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

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

Step 2. Install Unified Manager on the first node.
“Installing Unified Manager on Red Hat Enterprise Linux or CentOS” on page 23

Step 3. Repeat Steps 1 and 2 on the second node of the cluster.

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

Configuring Unified Manager with VCS using configuration scripts

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

Before you begin

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


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

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

About this task

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

- Step 1. Log in to the first node of the cluster.
You must have stopped all the Unified Manager services on the second node in the high availability setup.
- Step 2. Add the VCS installation directory `/opt/VRTSvcs/bin` to the PATH environmental variable.
- Step 3. If you are configuring an existing Unified Manager setup, create a Unified Manager backup and generate the support bundle.
- Step 4. Run the **ha_setup.pl** script:

```
perl ha_setup.pl --first -t vcs -g group_name -e eth_name -i cluster_ip -m net_mask -n fully_qualified_cluster_name -f mount_path -v volume_group -d disk_group -l install_dir -u user_name -p password
```
- Step 5. Use the Veritas Operation Manager web console or VCS Cluster Manager to verify that a failover group is created, and that the Unified Manager server services, mount point, virtual IP, network interface card (NIC), and volume group are added to the cluster group.
- Step 6. Manually move the Unified Manager service group to the secondary node and verify that cluster failover is working.
- Step 7. Verify that VCS has switched over to the second node of the cluster.
You must verify that the data mount, virtual IP, volume group, and NIC are online on the second node of the cluster.
- Step 8. Stop Unified Manager using Veritas Operation Manager.
- Step 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.
- Step 10. Verify that the Unified Manager server services are starting properly on the second node of the cluster.
- Step 11. Regenerate the Unified Manager certificate after running the configuration scripts to obtain the global IP address.
 - a. In the toolbar, click , and then click **HTTPS Certificate** from the Setup menu.
 - b. Click **Regenerate HTTPS Certificate**.The regenerated certificate provides only the cluster IP address, not the fully qualified domain name (FQDN). You must use the global IP address to set up Unified Manager for high-availability.
- Step 12. Access the Unified Manager UI using the following 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 that you create before and after failover. Both the nodes in the high-availability setup must be able to access the shared location.

Unified Manager service resources for VCS configuration

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

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

Category	Services
Storage resource	<ul style="list-style-type: none"> • <i>vol</i> • <i>mount</i>
Database resource	<ul style="list-style-type: none"> • <i>mysqld</i>
Network resource	<ul style="list-style-type: none"> • <i>nic</i> • <i>vip</i>
Unified Manager resource	<ul style="list-style-type: none"> • <i>ocie</i> • <i>ocieau</i>

Updating an existing Unified Manager setup for high availability

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

Before you begin

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

See the *Veritas Cluster Server 6.2.1 Installation Guide*.

- The newly added node must be configured to access the same shared location as that of the existing node in the high-availability setup.

Step 1. Log in to the new node of the cluster.

Step 2. Install Unified Manager on the node.
“Installing Unified Manager on Red Hat Enterprise Linux or CentOS” on page 23

Step 3. Configure the Unified Manager server using configuration scripts on the existing node with data.

Step 4. Initiate manual fail over to the second node.

Step 5. Run the `perl ha_setup.pl --join -t vcs -f mount_path` command on the second node of the cluster so that the Unified Manager server data points to the shared LUN.

Step 6. If ThinkSystem Storage Workflow Automation (WFA) is configured for Unified Manager, disable and then reconfigure the WFA connection.

Step 7. If SnapProtect is configured with Unified Manager, reconfigure SnapProtect with a new cluster IP address and the existing storage policies.

Step 8. Regenerate the custom reports and add these reports to Unified Manager with the new cluster IP address.

Upgrading Unified Manager on Red Hat Enterprise Linux or CentOS

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

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

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

Upgrading Unified Manager on Red Hat Enterprise Linux or CentOS

You can upgrade from Unified Manager version 9.4 or 9.5 to 9.6 by downloading and running the installation file on the Red Hat platform.

Before you begin

- The system on which you are upgrading Unified Manager must meet the system and software requirements.
“Hardware system requirements” on page 3
“Linux software and installation requirements” on page 5
- Starting with Unified Manager 9.5, Oracle Java is no longer supported. You must install, or upgrade, to the correct version of OpenJDK prior to upgrading Unified Manager.
“Upgrading JRE on Linux” on page 35
- Starting with Unified Manager 9.6, MySQL is not upgraded automatically during the Unified Manager upgrade. You must upgrade to the correct version of MySQL prior to beginning the upgrade to Unified Manager.
“Upgrading MySQL on Linux” on page 35
- You must have a subscription to the Red Hat Enterprise Linux Subscription Manager.
- To avoid data loss, you must have created a backup of the Unified Manager database in case there is an issue during the upgrade. It is also recommended that you move the backup file from the `/opt/netapp/data` directory to an external location.
- You should have completed any running operations, because Unified Manager is unavailable during the upgrade process.

About this task

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

- Step 1. Log in to the target Red Hat Enterprise Linux or CentOS server.
- Step 2. Download the Unified Manager bundle to the server.
“Downloading Unified Manager for Red Hat Enterprise Linux or CentOS” on page 24
- Step 3. Navigate to the target directory and expand the Unified Manager bundle:
`unzip ActiveIQUnifiedManager-9.6.zip`
The required RPM modules for Unified Manager are unzipped to the target directory.
- Step 4. Confirm the presence of the listed modules:
`ls *.rpm`
The following RPM modules are listed:
 - `ocie-au-<version>.x86_64.rpm`
 - `ocie-server-<version>.x86_64.rpm`
 - `ocie-serverbase-<version>.x86_64.rpm`
 - `netapp-application-server-<version>.x86_64.rpm`
 - `netapp-platform-base-<version>.x86_64.rpm`
 - `netapp-ocum-<version>.x86_64.rpm`

- Step 5. 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:
- View the list of available and unavailable packages:
`yum install *.rpm --assumeno`
 The items in the “Installing:” section are the packages that are available in the current directory, and the items in the “Installing for dependencies:” section are the packages that are missing on your system.
 - Download the missing packages on another system that has Internet access:
`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`
- Copy the missing packages from the Internet-connected system to your installation system.
- Step 6. If Unified Manager is configured for high availability, then using Veritas Operation Manager, stop all Unified Manager services on the first node.
- Step 7. Upgrade Unified Manager using the following script:
`upgrade.sh`
 This script automatically executes the RPM modules, upgrading the necessary supporting software and the Unified Manager modules that run on them. Additionally, the upgrade script checks whether there are any system configuration settings or any installed software that will conflict with the upgrade of Unified Manager. If the script identifies any issues, you must fix the issues prior to upgrading Unified Manager.
- 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 are upgraded in a specific order to a specific directory structure that are executed and configured automatically by the script.
- Step 8. For high availability installations, stop all Unified Manager services on the second node with Veritas Operation Manager.
- Step 9. For high availability installations, switch the service group to the second node in the high-availability setup and upgrade Unified Manager on the second node.
- Step 10. After the upgrade is complete, scroll back through the messages until you see the message displaying an IP address or URL for the Unified Manager web UI, the maintenance user name (umadmin), and the default password.
 The message is similar to the following:
 Active IQ Unified Manager upgraded successfully.
 Use a web browser and one of the following URLs to access the Unified Manager GUI:
- `https://default_ip_address/` (if using IPv4)
`https://[default_ip_address]/` (if using IPv6)
`https://fully_qualified_domain_name/`

After you finish

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

Upgrading the host OS from Red Hat Enterprise Linux 6.x to 7.x

If you previously installed Unified Manager on a Red Hat Enterprise Linux 6.x system and now need to upgrade to Red Hat Enterprise Linux 7.x, you must follow one of the procedures listed in this topic. In both cases you must create a backup of Unified Manager on the Red Hat Enterprise Linux 6.x system, and then restore the backup onto a Red Hat Enterprise Linux 7.x system.

About this task

The difference between the two options listed below is that in one case you are performing the Unified Manager restore onto a new RHEL 7.x server, and in the other case you are performing the restore operation onto the same server.

Because this task requires that you create a backup of Unified Manager on the Red Hat Enterprise Linux 6.x system, you should create the backup only when you are prepared to complete the entire upgrade process so that Unified Manager is offline for the shortest period of time. Gaps in collected data will appear in the Unified Manager UI for the period of time during which the Red Hat Enterprise Linux 6.x system is shut down and before the new Red Hat Enterprise Linux 7.x is started.

Upgrading the host OS using a new server

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

1. Install and configure a new server with Red Hat Enterprise Linux 7.x software.
“Red Hat software and installation requirements” on page 5
2. On the Red Hat Enterprise Linux 7.x system, install the same version of Unified Manager software that you have on the existing Red Hat Enterprise Linux 6.x system.
“Installing Unified Manager on Red Hat Enterprise Linux” on page 23
Do not launch the UI or configure any clusters, users, or authentication settings when the installation is complete. The backup file populates this information during the restore process.
3. On the Red Hat Enterprise Linux 6.x system, from the Administration menu in the web UI, create a Unified Manager backup and then copy the backup file (.7z file) and the contents of the database repository directory (`/database-dumps-repo` subdirectory) to an external location.
4. On the Red Hat Enterprise Linux 6.x system, shut down Unified Manager.
5. On the Red Hat Enterprise Linux 7.x system, copy the backup file (.7z file) from the external location to `/opt/netapp/data/ocum-backup/` and the database repository files to the `/database-dumps-repo` subdirectory under the `/ocum-backup` directory.
6. Enter the following command to restore the Unified Manager database from the backup file:
`um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>`
7. Enter the IP address or URL into your web browser to start the Unified Manager web UI, and then log in to the system.

Once you have verified that the system is operating properly you can remove Unified Manager from the Red Hat Enterprise Linux 6.x system.

Upgrading the host OS on the same server

Follow these steps if you do not have a spare system on which you can install RHEL 7.x software.

1. From the Administration menu in the web UI, create a Unified Manager backup and then copy the backup file (.7z file) and the contents of the database repository directory (`/database-dumps-repo` subdirectory) to an external location.

2. Remove the Red Hat Enterprise Linux 6.x image from the system and completely wipe the system.
3. Install and configure Red Hat Enterprise Linux 7.x software on the same system.
“Red Hat software and installation requirements” on page 5
4. On the Red Hat Enterprise Linux 7.x system, install the same version of Unified Manager software that you had on the Red Hat Enterprise Linux 6.x system.
“Installing Unified Manager on Red Hat Enterprise Linux” on page 23
Do not launch the UI or configure any clusters, users, or authentication settings when the installation is complete. The backup file populates this information during the restore process.
5. Copy the backup file (.7z file) from the external location to `/opt/netapp/data/ocum-backup/` and the database repository files to the `/database-dumps-repo` subdirectory under the `/ocum-backup` directory.
6. Enter the following command to restore the Unified Manager database from the backup file:
`um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>`
7. Enter the IP address or URL into your web browser to start the Unified Manager web UI, and then log in to the system.

Upgrading third-party products on Linux

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

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

Upgrading JRE on Linux

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

Before you begin

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

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

Upgrading MySQL on Linux

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

Before you begin

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

About this task

You can only upgrade to minor updates of MySQL 5.7, for example, 5.7.22 to 5.7.26. You cannot upgrade to major versions of MySQL, for example, version 5.8.

- Step 1. Log in as a root user on the Unified Manager host machine.
- Step 2. Download the latest MySQL Community Server .rpm bundle on the target system.
- Step 3. Untar the bundle to a directory on the target system.
- Step 4. You will get multiple .rpm packages in the directory after untarring the bundle, but Unified Manager only needs the following rpm packages:
 - mysql-community-client-5.7.x
 - mysql-community-libs-5.7.x
 - mysql-community-server-5.7.x
 - mysql-community-common-5.7.x
 - mysql-community-libs-compat-5.7.xDelete all other .rpm packages. Installing all packages in an rpm bundle will not cause any problems.
- Step 5. Stop the Unified Manager service and the associated MySQL software in the order shown:

```
service ocieau stop
service ocie stop
service mysqld stop
```
- Step 6. Invoke the upgrade of MySQL by using the following command:

```
yum install *.rpm
```

```
yum install *.rpm
```

*.rpm refers to the .rpm packages in the directory where you downloaded the newer version of MySQL.
- Step 7. Start Unified Manager in the order shown:

```
service mysqld start
service ocie start
service ocieau start
```

Restarting Unified Manager in Red Hat Enterprise Linux or CentOS

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

Before you begin

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

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

```
service ocieau stop
service ocie stop
service mysqld stop
```

When installed in a high-availability setup, stop the Unified Manager service by using either VCS Operations Manager or VCS commands.
- Step 3. Start Unified Manager in the order shown:

```
service mysqld start
service ocie start
service ocieau start
```

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

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

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

Before you begin

- You must have root user access to the server from which you want to remove Unified Manager.
- Security-Enhanced Linux (SELinux) must be disabled on the Red Hat machine. Change the SELinux runtime mode to “Permissive” by using the **setenforce 0** command.
- All clusters (data sources) must be removed from the Unified Manager server before removing the software.

About this task

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

- Step 1. Log in as root user to the cluster node owning the cluster resources on which you want to remove Unified Manager.
- Step 2. Stop all Unified Manager services using VCS Operations Manager or VCS commands.
- Step 3. Stop and remove Unified Manager from the server:

```
rpm -e netapp-ocum ocie-au ocie-server netapp-platform-base netapp-application-server ocie-serverbase
```

This step removes all the associated Lenovo RPM packages. It does not remove the prerequisite software modules, such as Java, MySQL, and p7zip.
- Step 4. Switch to the other node by using the VCS Operations Manager.
- Step 5. Log in to the second node of the cluster.
- Step 6. Stop all the services, and then and remove Unified Manager from the second node:

```
rpm -e netapp-ocum ocie-au ocie-server netapp-platform-base netapp-application-server ocie-serverbase
```
- Step 7. Prevent the service group from using VCS Operations Manager or VCS commands.
- Step 8. Optional: If appropriate, remove the supporting software modules, such as Java, MySQL, and p7zip:

```
rpm -e p7zip mysql-community-client mysql-community-server mysql-community-common mysql-community-libs java-x.y
```

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.

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.

Step 1. Log in as the root user to the Red Hat Enterprise Linux server.

Step 2. Delete the umadmin user:
`userdel umadmin`

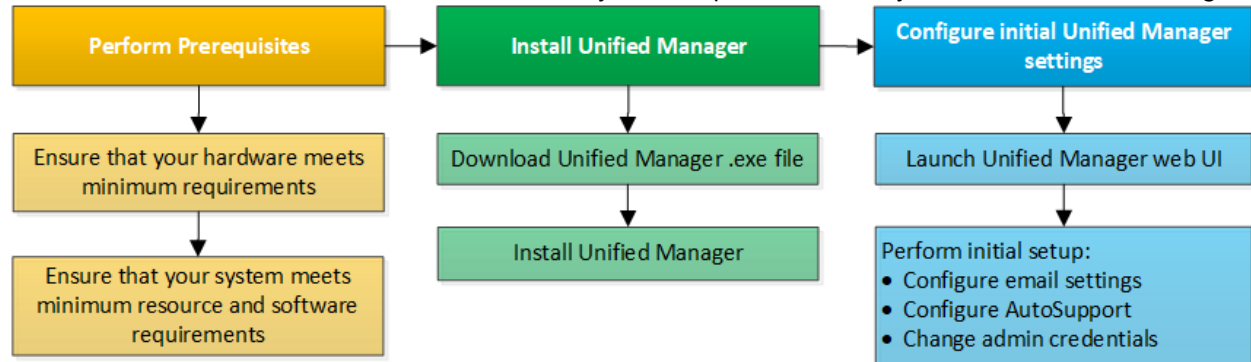
Step 3. Delete the maintenance group:
`groupdel maintenance`

Chapter 5. Installing, upgrading, and removing Unified Manager software on Windows

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

Overview of the installation process on Windows

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



Installing Unified Manager on Windows

It is important that you understand the sequence of steps to download and install Unified Manager on Windows. Before you install Unified Manager on Windows, you can decide if you want to configure Unified Manager for high availability.

Installing Unified Manager on a Windows system

You can install Unified Manager on Windows to monitor and troubleshoot data storage capacity, availability, performance, and protection issues.

Before you begin

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

“Hardware system requirements” on page 3

“Windows software and installation requirements” on page 7

Note: Starting with Unified Manager 9.5, OpenJDK is provided in the installation package and installed automatically. Oracle Java is not supported starting with Unified Manager 9.5.

- You must have Windows administrator privileges.
- You must have a supported web browser.
- The Unified Manager maintenance user password must be between 8 and 20 characters, must contain upper-case letters or lower-case letters, numerals, and special characters.
- The following special characters are not allowed in the password string for the maintenance user or for the MySQL root user: " ' ` % , = & < > | ^ \ / () [] ;

The following special characters are allowed: ~ ! @ # \$ * - ? . : + { }

- Step 1. Log in to Windows using the default local administrator account.
- Step 2. Log in to the Lenovo Support Site, and locate the Download page for Unified Manager on the Windows platform.
<https://datacentersupport.lenovo.com>
- Step 3. Download the Unified Manager Windows installation file from the Lenovo Support Site to a target directory in the Windows system.
- Step 4. Navigate to the directory where the installation file is located.
- Step 5. Right-click and run the Unified Manager installer executable (.exe) file as an administrator. Unified Manager detects missing or pre-installed third-party packages and lists them. If the required third-party packages are not installed in the system, Unified Manager installs them as part of the installation.
- Step 6. Click **Next**.
- Step 7. Enter the user name and password to create the maintenance user.
- Step 8. In the Database Connection wizard, enter the MySQL root password if already installed.
- Step 9. Click **Change** to specify a new location for the Unified Manager installation directory and MySQL data directory.
If you do not change the installation directory, Unified Manager is installed in the default installation directory.
- Step 10. Click **Next**.
- Step 11. In the Ready to Install Shield wizard, click **Install**.
- Step 12. After the installation is complete, click **Finish**.

Result

The installation creates multiple directories:

- Installation directory
This is the root directory for Unified Manager, which you specified during installation. Example: C:\Program Files\NetApp\
- MySQL data directory
This is the directory where the MySQL databases are stored, which you specified during installation. Example: C:\ProgramData\MySQL\MySQLServerData\
- Java directory
This is the directory where OpenJDK will be installed. Example: C:\Program Files\NetApp\JDK\
- Unified Manager application data directory (appDataDir) This is the directory where all the application-generated data is stored. This includes logs, support bundles, backup, and all other additional data. Example: C:\ProgramData\NetApp\OnCommandAppData\

Performing an unattended installation of Unified Manager on Windows

You can install Unified Manager on Windows without user intervention by using the command-line interface. You can complete the unattended installation by passing the parameters in key-value pairs.

- Step 1. Log in to the Windows command-line interface by using the default local administrator account.
- Step 2. Navigate to the location where you want to install Unified Manager, and choose one of the following options:

Option	Instructions
If third-party packages are pre-installed	<p>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\\<i>Installation directory</i>\" MYSQL_DATA_DIR=\\<i>MySQL data directory</i>\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qn /l*v <i>CompletePathForLogFile</i>"</p> <p>Example:</p> <p>ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR="C:\Program Files\NetApp\" MYSQL_DATA_DIR="C:\ProgramData\MySQL\MySQLServer\" MAINTENANCE_PASSWORD=***** MAINTENANCE_USERNAME=admin /qn /l*v C:\install.log"</p>
If third-party packages are not installed	<p>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\\<i>Installation directory</i>\" MYSQL_DATA_DIR=\\<i>MySQL data directory</i>\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qr /l*v <i>CompletePathForLogFile</i>"</p> <p>Example:</p> <p>ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR="C:\Program Files\NetApp\" MYSQL_DATA_DIR="C:\ProgramData\MySQL\MySQLServer\" MAINTENANCE_PASSWORD=***** MAINTENANCE_USERNAME=admin /qr /l*v C:\install.log"</p>

The /qr option enables quiet mode with a reduced user interface. A basic user interface is displayed, which shows the installation progress. You will not be prompted for inputs. If third-party packages such as JRE, MySQL, and 7zip are not pre-installed, you must use the /qr option. Installation fails if the /qn option is used on a server where third-party packages are not installed.

Note: The /qn option enables quiet mode with no user interface. No user interface or details are displayed during installation. You must not use the /qn option when third-party packages are not installed.

Step 3. Log in to the Unified Manager web user interface by using the following URL:
<https://IP address>

Setting up Unified Manager in a failover clustering environment

You can configure high availability for Unified Manager using failover clustering. The high-availability setup provides failover capability.

In this setup, only one node owns all the cluster resources. When one node goes down or any of the configured services fail to come online, the failover cluster 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 and you do not have to perform any actions.

A failover cluster configured with the Unified Manager server consists of two nodes, 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.

Requirements for Unified Manager in a failover clustering environment

Before installing Unified Manager in a failover clustering environment, you must ensure that the cluster nodes are properly configured to support Unified Manager.

You must ensure that the failover cluster configuration meets the following requirements:

- Both the cluster nodes must be running the same version of Microsoft Windows Server.
- The same version of Unified Manager must be installed using the same path on both the cluster nodes.
- Failover clustering must be installed and enabled on both the nodes.

See Microsoft documentation for instructions.

- You must have used Fibre Channel switched fabric or iSCSI-based storage for creating shared data disk as the storage back-end.
- Optional: Using SnapDrive for Windows, a shared location must be created that is accessible to both the nodes in the high-availability setup.
- You must have the Perl installed with XML::LibXML and File::chdir modules for scripts to work.
- There must be only two nodes in the cluster setup.
- The “node and disk majority” quorum type must be used for failover clustering.
- You must have configured a shared IP address with a corresponding FQDN to be used as the cluster global IP address to access Unified Manager.
- The password for Unified Manager maintenance user on both the nodes must be same.
- You must have used only IPv4 IP address.

Installing Unified Manager on MSCS

For configuring high availability, you must install Unified Manager on both the Microsoft Cluster Server (MSCS) cluster nodes.

Step 1. Log in as the domain user on both the nodes of the cluster.

Step 2. Set up high availability by choosing one of the following options:

If you want to...	Then do this...
Configure high availability on an existing Unified Manager installation	Add another server to be paired with the existing server: <ol style="list-style-type: none"> 1. Upgrade the existing Unified Manager server to the latest software version. 2. Create a backup of the existing Unified Manager installation, and store the backup to a mounted LUN. 3. Install Unified Manager on the second node. “Installing Unified Manager on a Windows system” on page 39 4. Restore the backup of the existing Unified Manager installation onto the second node.
Configure high availability on a new Unified Manager installation	Install Unified Manager on both the nodes. “Installing Unified Manager on a Windows system” on page 39

Configuring Unified Manager server with MSCS using configuration scripts

After installing Unified Manager on both cluster nodes, you can configure Unified Manager with Failover Cluster Manager using configuration scripts.

Before you begin

You must have created a shared LUN that is of a sufficient size to accommodate the source Unified Manager data.

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

Step 2. Create a role in Windows 2016 or Windows 2019 using Failover Cluster Manager:

- Launch Failover Cluster Manager.
- Create the empty role by clicking **Roles → Create Empty Role**.
- Add the global IP address to the role by right-clicking **Role → Add Resources → More Resources → IP address**.

Note: Both nodes must be able to ping this IP address because Unified Manager is launched using this IP address after high availability is configured.

- Add the data disk to the role by right-clicking **Role → Add Storage**.

Step 3. Run the **ha_setup.pl** script on the first node:

```
perl ha_setup.pl --first -t mscs -g group_name -i ip_address -n fully_qualified_domain_cluster_name -f shared_location_path -k data_disk -u user_name -p password
```

Example

```
C:\Program Files\NetApp\ocum\bin>perl .\ha_setup.pl --first -t mscs -g umgroup -i "IP Address"
-n spr38457002.eng.company.com -k "Cluster Disk 2" -f E:\ -u admin -p wx17yz
```


The script is available at *Install_Dir\NetApp\ocum\bin*.

- You can obtain the value of the -g, -k, and -i options using the **cluster res** command.
- The -n option must be the FQDN of the global IP address that can be pinged from both nodes.

- Step 4. Verify that the Unified Manager server services, data disk, and cluster IP address are added to the cluster group by using the Failover Cluster Manager web console.
- Step 5. Stop all Unified Manager server services (MySQL, ocie, and ocieau) by using the **services.msc** command.
- Step 6. Switch the service group to the second node in Failover Cluster Manager.
- Step 7. Run the command **perl ha_setup.pl --join -t mscs -f *shared_location_path*** on the second node of the cluster to point to the Unified Manager server data to the LUN.

Example

```
perl ha_setup.pl --join -t mscs -f E:\
```

- Step 8. Bring all the Unified Manager services online using Failover Cluster Manager.
- Step 9. Manually switch to the other node of the Microsoft Cluster Server.
- Step 10. Verify that the Unified Manager server services are starting properly on the other node of the cluster.
- Step 11. Regenerate the Unified Manager certificate after running configuration scripts to obtain the global IP address.
- a. In the toolbar, click , and then click **HTTPS Certificate** from the Setup menu.
 - b. Click **Regenerate HTTPS Certificate**.

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

- Step 12. Access the Unified Manager UI using the following 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 nodes in the high-availability setup must be able to access the shared location.

Changing the JBoss password on Windows

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

Before you begin

- You must have Windows admin privileges for the system on which Unified Manager is installed.
- You must have the password for the MySQL root user.

- You must be able to access the Lenovo-provided password.bat script in the directory \Program Files\NetApp\essentials\bin.

Step 1. Log in as the admin user on the Unified Manager host machine.

Step 2. Use the Windows Services console to stop the following Unified Manager services:

- NetApp Active IQ Acquisition Service (Ocie-au)
- NetApp Active IQ Management Server Service (Oncommandsvc)

Step 3. Launch the password.bat script to begin the password change process:
C:\Program Files\NetApp\essentials\bin> password.bat resetJBossPassword

Step 4. When prompted, enter the MySQL root user password.

Step 5. When prompted, enter the current JBoss user password.
The default password is D11h1aMu@79%.

Step 6. When prompted, enter the new JBoss user password, and then enter it again for confirmation. Confirmation messages appear as the changes are made, and then you are prompted one last time for the new JBoss user password.

Step 7. Enter the new JBoss user password one more time.

Step 8. When the script completes, start the Unified Manager services by using the Windows Services console:

- NetApp Active IQ Management Server Service (Oncommandsvc)
- NetApp Active IQ Acquisition Service (Ocie-au)

Step 9. After all of the services are started, you can log in to the Unified Manager UI.

Upgrading Unified Manager on Windows

You can upgrade Unified Manager 9.4 or 9.5 to 9.6 by downloading and running the installation file on the Windows platform.

Before you begin

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

“Hardware system requirements” on page 3

“Windows software and installation requirements” on page 7

Note: Starting with Unified Manager 9.5, OpenJDK is provided in the installation package and installed automatically. Oracle Java is not supported starting with Unified Manager 9.5.

Note: Starting with Unified Manager 9.4, Microsoft .NET 4.5.2 or greater is required. Make sure you have the correct version of .NET installed before starting the upgrade.

- You must have Windows administrator privileges.
- You must have valid credentials to log in to the Lenovo Support Site.
- 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 must have adequate disk space available to perform the upgrade.

The available space on the installation drive must be 2.5 GB larger than the size of the data directory. The upgrade will stop and display an error message indicating the amount of space to be added if there is not enough free space.

About this task

During the upgrade process, Unified Manager is unavailable. You should complete any running operations before upgrading Unified Manager.

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

- Step 1. Log in to the Lenovo Support Site, and locate the Download page for Unified Manager Installation Guide.
<https://datacentersupport.lenovo.com>
- Step 2. Download the Unified Manager Windows installation file to a target directory in the Windows system.
- Step 3. If Unified Manager is configured for high availability, stop all the Unified Manager services on the first node by using Microsoft Cluster Server, and then start the MySQL service from **services.msc**.
- Step 4. Right-click and run the Unified Manager installer executable (.exe) file as an administrator. Unified Manager prompts you with the following message:
This setup will perform an upgrade of Unified Manager. Do you want to continue?
- Step 5. Click **Yes**, and then click **Next**.
- Step 6. Enter the MySQL root password that was set during installation, and click **Next**.
- Step 7. After the upgrade is successful, if the system is configured for high availability, start all the Unified Manager services from the Failover Cluster Manager and follow the remaining tasks.
- Step 8. From the command prompt, run the **ha_setup.pl** script to configure the new services in the failover cluster and the files that are present in the shared location.

Example

```
C:\Program Files\NetApp\ocum\bin> perl .\ha_setup.pl --upgrade --first -t mscs -g kjaggrp -i  
"New IP Address1" -n scs8003.englab.company.com -k "Cluster Disk 2" -f E:\ -u user -p userpass
```

- Step 9. Stop all the Unified Manager services (ocie, ocieau, and MySQL) in the first node by using Microsoft Cluster Server.
- Step 10. Start the MySQL service on the second node from **services.msc**.
- Step 11. Switch the service group to the second node in the high-availability setup.
- Step 12. Upgrade Unified Manager on the second node.
- Step 13. At the command prompt, enter Y to continue, or enter any other character to abort.
The upgrade and restart processes of the Unified Manager services can take several minutes to complete.
- Step 14. Start all the Unified Manager services on both the nodes using Microsoft Cluster Server.
- Step 15. From the command prompt, run the **ha_setup.pl** script with the --upgrade option.

Example

```
perl ha_setup.pl --upgrade --join -t mscs -f E:\
```

- Step 16. Log in to the Unified Manager web UI, and verify the version number.

After you finish

Note: To perform a silent upgrade of Unified Manager, run the following command:
`ActiveIQUnifiedManager-9.6.exe /s /v"MYSQL_PASSWORD=netapp21! /qn /l*v C:\install.log`

Upgrading third-party products on Windows

You can upgrade third-party products, such as JRE and MySQL, on Unified Manager when installed on Windows systems.

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

Upgrading JRE on Windows

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

Before you begin

You must have Windows admin privileges for the system on which Unified Manager is installed.

- Step 1. Log in as the admin user on the Unified Manager host machine.
- Step 2. Download the appropriate version of Java (64-bit) from the JDK site to the target system. For example, download `openjdk-11_windows-x64_bin.zip` from <http://jdk.java.net/11/>.
- Step 3. Use the Windows Services console to stop the following Unified Manager services:
 - NetApp Active IQ Acquisition Service (Ocie-au)
 - NetApp Active IQ Management Server Service (Oncommandsvc)
- Step 4. Expand the zip file.
- Step 5. Copy the directories and files from the resulting `jdk` directory (for example, `jdk-11.0.2` to the location where Java is installed. Example: `C:\Program Files\NetApp\JDK\`
- Step 6. Start the Unified Manager services by using the Windows Services console:
 - NetApp Active IQ Management Server Service (Oncommandsvc)
 - NetApp Active IQ Acquisition Service (Ocie-au)

Upgrading MySQL on Windows

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

Before you begin

- You must have Windows admin privileges for the system on which Unified Manager is installed.
- You must have the password for the MySQL root user.

- Step 1. Log in as the admin user on the Unified Manager host machine.
- Step 2. Download the appropriate version of MySQL to the target system.
- Step 3. Use the Windows Services console to stop the following Unified Manager services:
 - NetApp Active IQ Acquisition Service (Ocie-au)
 - NetApp Active IQ Management Server Service (Oncommandsvc)
 - MYSQL

- Step 4. Click the .msi package to invoke the upgrade of MySQL and follow the instructions on the screen to complete the upgrade.
- Step 5. Start the Unified Manager services by using the Windows Services console:
- MYSQL
 - NetApp Active IQ Management Server Service (Oncommandsvc)
 - NetApp Active IQ Acquisition Service (Ocie-au)

Restarting Unified Manager on Windows

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

Before you begin

You must have Windows administrator privileges.

- Step 1. Log in to Windows using the default local administrator account.
- Step 2. Stop the Unified Manager services:

From the...	Stop the services in following order...
Command line	<ol style="list-style-type: none">1. <code>sc stop ocie-au</code>2. <code>sc stop Oncommandsvc</code>
Microsoft Service Manager	<ol style="list-style-type: none">1. NetApp Active IQ Acquisition Service (Ocie-au)2. NetApp Active IQ Management Server Service (Oncommandsvc)

When installed in a high-availability setup, stop the Unified Manager service by using either Microsoft Service Manager or the command line.

- Step 3. Start the Unified Manager services:

From the...	Start the services in following order...
Command line	<ol style="list-style-type: none">1. <code>sc start Oncommandsvc</code>2. <code>sc start ocie-au</code>
Microsoft Service Manager	<ol style="list-style-type: none">1. NetApp Active IQ Management Server Service (Oncommandsvc)2. NetApp Active IQ Acquisition Service (Ocie-au)

When installed in a high-availability setup, start Unified Manager service by using either Microsoft Service Manager or the command line.

Uninstalling Unified Manager from Windows

You can uninstall Unified Manager from Windows by using the Programs and Features wizard, or by performing an unattended uninstallation from the command-line interface.

Before you begin

- You must have Windows administrator privileges.
- All clusters (data sources) must be removed from the Unified Manager server before uninstalling the software.

Step 1. When installed in a high-availability setup, remove the HA service group resources and delete the HA service group before uninstalling Unified Manager from both nodes.

Step 2. Uninstall Unified Manager by choosing one of the following options:

To uninstall Unified Manager from the...	Then...
Programs and Features wizard	<ol style="list-style-type: none"> 1. Navigate to Control Panel → Program and Features. 2. Select Active IQ Unified Manager, and click Uninstall.
Command line	<ol style="list-style-type: none"> 1. Log in to the Windows command line using administrator privileges. 2. Navigate to the Active IQ Unified Manager directory, and run the following command: <code>msiexec /x {A78760DB-7EC0-4305-97DB-E4A89CDFF4E1} /qn /l*v %systemdrive%\UmUnInstall.log</code>

If User Account Control (UAC) is enabled on the server, and you are logged in as a domain user, you must use the command-line uninstallation method. Unified Manager is uninstalled from your system.

Step 3. Uninstall the following third-party packages and data that are not removed during the Unified Manager uninstallation:

- Third-party packages: JRE, MySQL, Microsoft Visual C++ 2015 Redistributable, and 7zip
- MySQL application data generated by Unified Manager
- Application logs and contents of application data directory

Appendix A. Contacting Support

You can contact Support to obtain help for your issue.

You can receive hardware service through a Lenovo Authorized Service Provider. To locate a service provider authorized by Lenovo to provide warranty service, go to <https://datacentersupport.lenovo.com/serviceprovider> and use filter searching for different countries. For Lenovo support telephone numbers, see <https://datacentersupport.lenovo.com/supportphonenumberlist> for your region support details.

Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

*Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property*

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

LENOVO, LENOVO logo, and THINKSYSTEM are trademarks of Lenovo. All other trademarks are the property of their respective owners. © 2019 Lenovo.

