Active IQ® Unified Manager 9.6

Installation Guide

For VMware vSphere®

∏ NetApp®

Contents

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.

Related information

NetApp Interoperability Matrix Tool

What the Unified Manager server does

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

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

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.

Active IQ Unified Manager Installation Guide

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

Active IQ Unified Manager System Configuration Guide

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

Active IQ Unified Manager Workflow Guide 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.

Active IQ Unified Manager Workflow Guide 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.

Active IQ Unified Manager Reporting Guide

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.
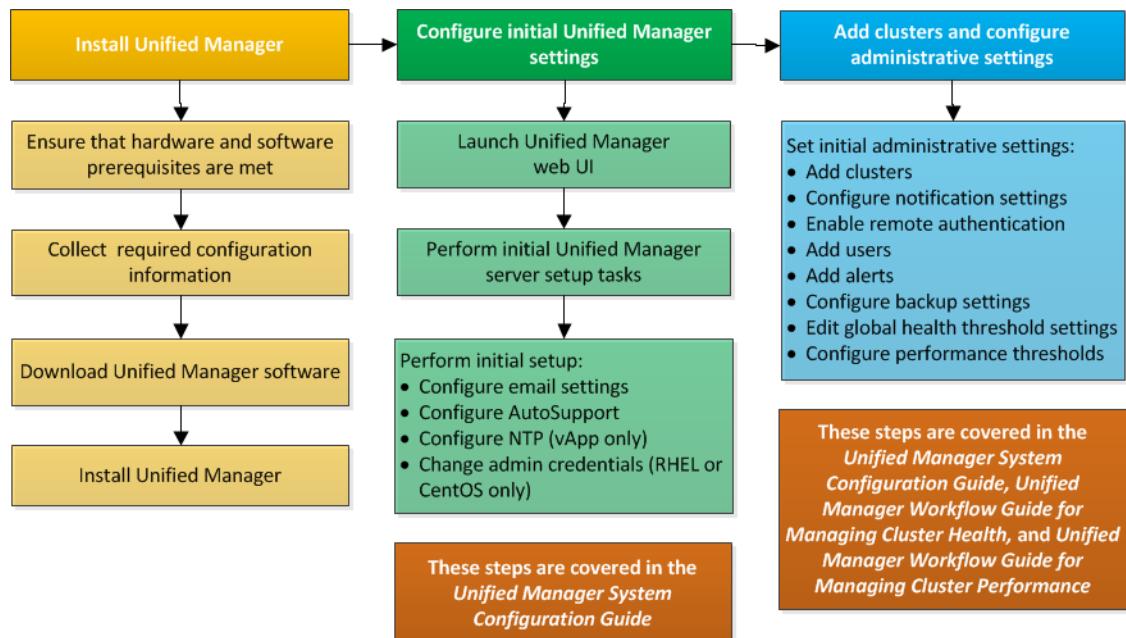
Requirements for installing Unified Manager

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

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

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

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

Related information
NetApp Interoperability Matrix Tool

Virtual infrastructure and hardware system requirements

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	• 5 GB (thin provisioned) • 152 GB (thick provisioned)

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. See the *Best Practices Guide* for more details.

Technical Report 4621: Unified Manager Best Practices Guide

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

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.

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.

mysupport.netapp.com/matrix

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 NetApp 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.

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. See the Interoperability Matrix for the complete list of supported browser versions.

mysupport.netapp.com/matrix

- 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 OnCommand Workflow Automation and OnCommand API Services access to Unified Manager.
Syslog	UDP	514	Used to access subscription-based EMS messages from ONTAP systems and to create events based on the messages.
REST	HTTPS	9443	Used to access realtime REST API-based EMS events from authenticated ONTAP systems.

> **Note:** The ports used for HTTP and HTTPS communication (ports 80 and 443) can be changed using the Unified Manager maintenance console. See the *Active IQ Unified Manager System Configuration Guide* for more information.

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	
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	
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)	

Installing, upgrading, and removing Unified Manager software

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

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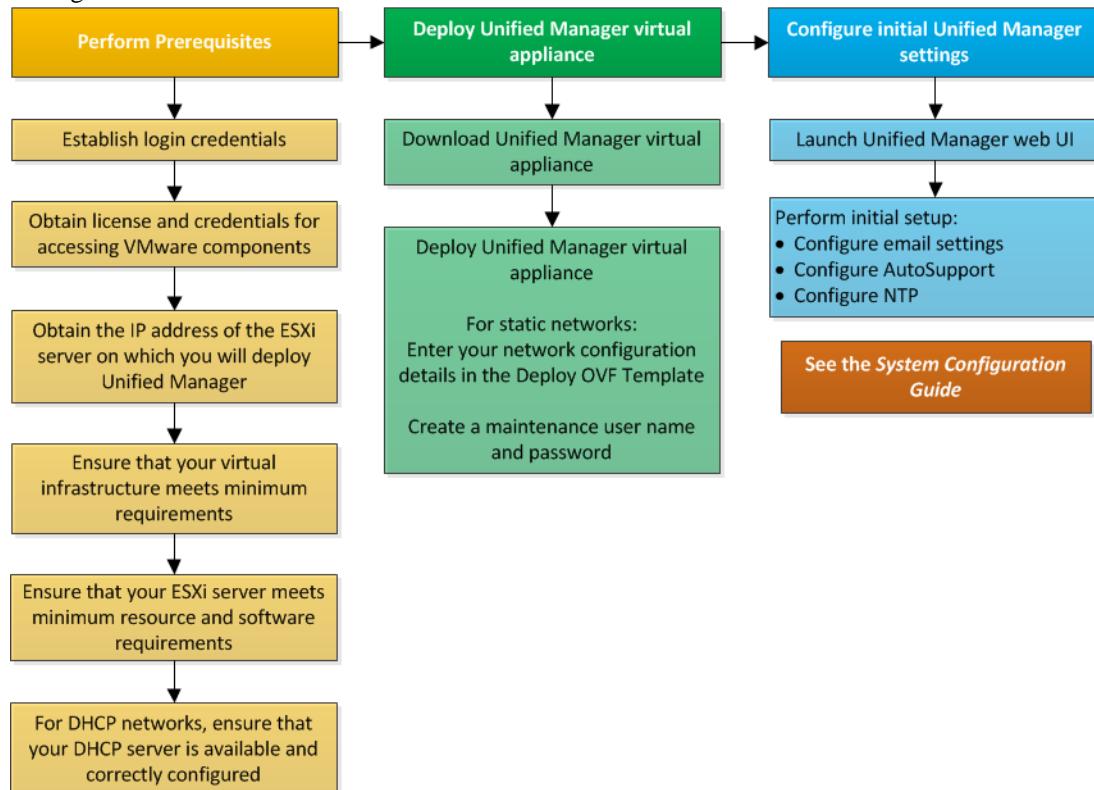
Deploying Unified Manager

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.
  System requirements
- You must have the following information:

  - Login credentials for the NetApp 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.

> **Related concepts**
> *Requirements for installing Unified Manager* on page 5
> Before you begin the installation process, ensure that the server on which you want to install Unified Manager meets the specific software, hardware, CPU, and memory requirements.

Steps

1. *Download Unified Manager* on page 11
You must download the Unified Manager `.ova` file from the NetApp Support Site to deploy Unified Manager as a virtual appliance.

2. *Deploy the Unified Manager virtual appliance* on page 11
You can deploy the Unified Manager virtual appliance after you download the `.ova` file from the NetApp Support Site. You must use the vSphere Web Client (for vSphere version 6.5 or 6.7) or vSphere Client (for vSphere version 6.0) to deploy the virtual appliance on an ESXi server. When you deploy the virtual appliance, a virtual machine is created.

Downloading the Unified Manager OVA file

You must download the Unified Manager `.ova` file from the NetApp Support Site to deploy Unified Manager as a virtual appliance.

Before you begin

You must have login credentials for the NetApp Support Site.

About this task

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

Steps

1. Log in to the NetApp Support Site, and navigate to the Download page for installing Unified Manager on VMware vSphere.

2. Download and save the `.ova` file to a local directory or network directory that is accessible to your vSphere Client.

3. Verify the checksum to ensure that the software downloaded correctly.

Deploying the Unified Manager virtual appliance

You can deploy the Unified Manager virtual appliance after you download the `.ova` file from the NetApp Support Site. You must use the vSphere Web Client (for vSphere version 6.5 or 6.7) or

vSphere Client (for vSphere version 6.0) to deploy the virtual appliance on an ESXi server. When you deploy the virtual appliance, a virtual machine is created.

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.

Virtual infrastructure requirements

VMware software and installation requirements

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.

Steps

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

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.

4. Click the **Console** tab.

The initial boot process takes a few minutes to complete.

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.

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.

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	Select **Retry DHCP**.
	If you plan to use DHCP, you should ensure that it is configured correctly.
	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.
A static network configuration	**a.** Select **Enter the details for static network configuration**. The configuration process takes a few minutes to complete. **b.** Confirm the values that you entered, and select **Y**.

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.

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

After you finish

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

Upgrading Unified Manager

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

Related tasks

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

Steps

1.
Before upgrading Unified Manager, you must download the Unified Manager ISO image from the
NetApp Support Site.

2.
You can upgrade from Unified Manager version 9.4 or 9.5 to 9.6.

Downloading the Unified Manager ISO image

Before upgrading Unified Manager, you must download the Unified Manager ISO image from the
NetApp Support Site.

Before you begin

You must have login credentials for the NetApp Support Site.

Steps

1. Log in to the NetApp Support Site and navigate to the Software Download page.

2. Download and save the `.iso` image file to a local directory or network directory that is
accessible to your vSphere Client.

3. Verify the checksum to ensure that the software downloaded correctly.

Upgrading the Unified Manager virtual appliance

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

Before you begin

- You must have downloaded the `.iso` file from the NetApp Support Site.
- The system on which you are upgrading Unified Manager must meet the system and software
requirements.
  Virtual infrastructure requirements
  VMware software and installation requirements
- 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 NetApp 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.

Steps

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

If you are using...	Then do this...
vSphere 6.0	**a.** Click the **CD/DVD Drive** icon, and select **Connect to ISO image on local disk**. **b.** Select the `ActiveIQUnifiedManager-9.6-virtual-update.iso` file, and click **Open**.
vSphere 6.5 or 6.7	**a.** Launch the VMware Remote Console. **b.** Click the **CDROM** icon, and select **Connect to Disk Image File (.iso)**. **c.** Select the `ActiveIQUnifiedManager-9.6-virtual-update.iso` file, and click **Open**.

7. Click the **Console** tab.
8. Log in to the Unified Manager maintenance console.
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.
10. Type **y** to continue.
    A warning is displayed, reminding you to back up the virtual machine on which the virtual appliance resides.
11. Type **y** to continue.
    The upgrade process and the restart of Unified Manager services can take several minutes to complete.
12. Press any key to continue.
    You are automatically logged out of the maintenance console.
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.

Steps

1. In the maintenance console, select **System Configuration** > **Reboot Virtual Machine**.

2. Start the Unified Manager graphical user interface (GUI) from your browser, and log in.

Related information

VMware vSphere PowerCLI Cmdlets Reference: Restart-VMGuest

Removing Unified Manager

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).

Steps

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.

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

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

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

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

Copyright and trademark

Copyright

Trademark