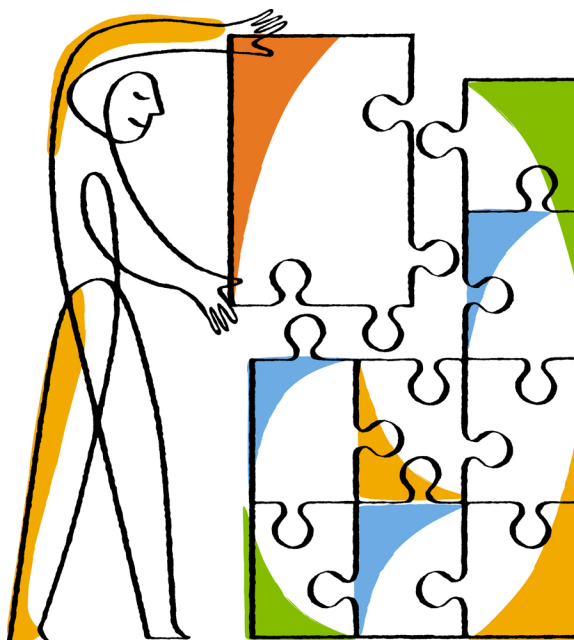




OnCommand® Unified Manager 6.0

Installation and Setup Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1(408) 822-6000
Fax: +1(408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-08054_A0
July 2013

Contents

Introduction to Unified Manager	5
What a virtual appliance does	5
What the maintenance user does	5
What AutoSupport does	6
Which OnCommand management software to use for each task type	6
When to use System Manager versus Unified Manager	7
System requirements	8
License requirements for Unified Manager	8
Virtual infrastructure requirements	8
Virtual appliance requirements	10
Software requirements	10
Supported versions of Data ONTAP	11
Browser requirements	11
Protocol and port requirements	11
Installing Unified Manager	13
Overview of the deployment sequence	13
Deploying Unified Manager	14
Downloading Unified Manager	15
Deploying the Unified Manager virtual appliance	15
Accessing the Unified Manager web UI	19
Performing the initial setup of the Unified Manager web UI	20
Configuring Unified Manager	22
Overview of the configuration sequence	22
Configuring your environment after deployment	23
Changing the Unified Manager host name	24
Configuring Unified Manager to send alert notifications	27
Adding clusters	35
Changing the local user password	35
Unified Manager 6.0 upgrade overview	37
Removing Unified Manager 6.0	38
Copyright information	39
Trademark information	40

How to send your comments 41

Index 42

Introduction to Unified Manager

You can deploy Unified Manager 6.0 only as a virtual appliance on a VMware host. This is different than previous versions of Unified Manager, which were installed on Windows or Linux servers.

Unified Manager 6.0 is built on a new server infrastructure that delivers scalability, supportability, and enhanced monitoring and notification capabilities. Cluster environments running Data ONTAP are visualized in the new graphical interface that provides at-a-glance status for capacity, availability, and protection of monitored systems. Unified Manager 6.0 supports monitoring of clustered Data ONTAP 8.1.1, 8.1.2, 8.1.3 and 8.2. Unified Manager 6.0 also supports the new and enhanced features in Data ONTAP 8.2 such as vaulting, nondisruptive operations, and Vservers with Infinite Volume.

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

Related information

NetApp Interoperability Matrix Tool: support.netapp.com/NOW/products/interoperability

What a virtual appliance does

A virtual appliance is a prebuilt software bundle containing an operating system and software applications that are integrated, managed, and updated as a package. Virtual appliances simplify the installation process.

Upon deployment, the virtual appliance creates a virtual machine containing Unified Manager, third-party applications, and all configuration information preinstalled on the virtual machine.

What the maintenance user does

Created during initial configuration, the maintenance user can create subsequent users and assign them roles. The maintenance user can also access the maintenance console and has the role of OnCommand administrator in the web UI.

The maintenance user can perform the following functions using the maintenance console:

- Configure network access
- Upgrade to newer versions of OnCommand Unified Manager
- Shut down virtual appliances (only from VMware console)
- Increase data disk or swap disk size
- Change the time zone
- Send on-demand AutoSupport messages to technical support from the maintenance console
- Send periodic AutoSupport messages to technical support from the web UI
- Enable or disable remote access to the diagnostic shell (only from VMware console)

- Generate support bundles to send to technical support

What AutoSupport does

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

Which OnCommand management software to use for each task type

Unified Manager 6.0 provides enhanced monitoring, alerting, and problem diagnosis for availability, capacity, and protection events in a cluster environment. Unified Manager works in conjunction with other products in the OnCommand suite to provide you with a complete monitoring and management experience.

To perform these management tasks for clustered Data ONTAP 8.2.x systems...	Use this OnCommand software...
Managing individual cluster elements	System Manager 3.0
Monitoring and alerting	Unified Manager 6.0
Reporting	OnCommand Report 2.x, Unified Manager 5.2
Performance monitoring and alerting	Unified Manager 5.2
Provisioning automation	Workflow Automation 2.2
Protection automation with client applications	NetApp Manageability SDK (Software Development Kit)
VMware discovery and monitoring	Not available
Monitoring performance and capacity of heterogeneous environments	OnCommand Balance 4.1.x
Storage capacity planning for heterogeneous environments	OnCommand Insight 6.4
SnapManager and SnapCreator integration	SnapManager and Unified Manager 5.2

When to use System Manager versus Unified Manager

As a general rule, you use System Manager to perform management tasks on individual cluster elements, such as volumes, aggregates, and so on; you use Unified Manager to monitor and escalate issues with multiple clusters and multiple cluster elements.

Use System Manager when you want to perform the following:

- Monitor real-time capacity and availability for a cluster
- Configure and manage individual cluster elements

Use Unified Manager when you want to perform the following:

- Monitor capacity availability and SnapMirror and SnapVault data protection relationships for multiple clusters and cluster elements
Unified Manager periodically polls clusters for information.
- Display storage trends
Unified Manager maintains a storage history that enables it to provide storage usage forecasting and planning information.
- Perform some management tasks on groups of cluster elements
For example, you can set thresholds, set alerts, and create resource pools.

System requirements

Before you deploy the Unified Manager virtual appliance, you must ensure that your storage system conforms to all supported platform requirements. Servers must meet specific software, hardware, CPU, and memory requirements.

You can install Unified Manager 6.0 only as a virtual appliance on an ESX server. This is different than previous versions of Unified Manager, which were installed on Windows or Linux servers.

Unified Manager requires OnCommand Workflow Automation 2.1 to provision Vservers with Infinite Volume with storage classes for content repository support.

For the most current information, see the *OnCommand Unified Manager 6.0 Installation and Setup Guide* and the Interoperability Matrix Tool.

Related information

NetApp Interoperability Matrix Tool: support.netapp.com/NOW/products/interoperability

License requirements for Unified Manager

You must have appropriate licenses to use VMware vSphere for Enterprise. No additional licenses are required for the server.

Virtual infrastructure requirements

Your virtual infrastructure must meet minimum requirements before you can begin deployment.

Memory page swapping negatively impacts performance of the virtual appliance and the management application. Competing for CPU resources that are unavailable due to overall host utilization can degrade performance. Reserving the listed values for memory and CPU resources for the virtual appliance guarantees that the required minimum amount is always available to the virtual machine, and is required for running this virtual appliance.

The following table displays the minimum values required for memory and CPU resources in the default configuration. These values have been qualified for the virtual appliance to meet minimum acceptable performance levels.

Default hardware configuration	Requirement
Disk space needed for thin provisioning	Minimum 5 GB
Disk space needed for thick provisioning	152 GB

Default hardware configuration	Requirement
Memory needed for Unified Manager virtual appliance	Minimum 12 GB
Processors needed for Unified Manager virtual appliance	4 virtual CPUs
Process cycles (CPU speed) needed for the Unified Manager virtual appliance	Minimum 9572 MHz

The following table displays the minimum values required for memory and CPU resources in the alternate configuration. These values have been qualified for the virtual appliance to meet minimum acceptable performance levels. After the virtual appliance is deployed, you can modify the memory, the number of CPUs, and the CPU speed to use an alternate configuration. For more information, see [Modifying the default configuration to the alternate configuration](#) on page 19.

Alternate hardware configuration	Requirement
Disk space needed for thin provisioning	Minimum 5 GB
Disk space needed for thick provisioning	152 GB
Memory needed for Unified Manager virtual appliance	Minimum 8 GB
Processors needed for Unified Manager virtual appliance	2 virtual CPUs
Process cycles (CPU speed) needed for the Unified Manager virtual appliance	Minimum 4786 MHz

VMware High Availability for the Unified Manager virtual appliance is not supported. The virtual appliance can be deployed on a VMware server that is a member of a VMware High Availability environment, but utilizing the VMware High Availability functionality is not supported.

If deployment fails using your High Availability-enabled environment due to insufficient resources, you must modify the following default VMware settings:

- Lower VM Resources CPU & Memory settings
- Lower the vSphere HA Admission Control Policy to use less than the default percentage of CPU and Memory
- Modify the Cluster Features Virtual Machine Options by disabling the VM Restart Priority and leaving the Host Isolation Response powered on.

Virtual appliance requirements

The virtual appliance is deployed on a VMware ESX server, which must meet minimum resource requirements.

The following versions of ESX and ESXi are supported:

- ESX 4.0
- ESX 4.1
- ESXi 4.1
- ESXi 5.0
- ESXi 5.1

The following versions of vSphere are supported:

- VMware vCenter Server 4.0
- VMware vCenter Server 4.1
- VMware vCenter Server 5.0
- VMware vCenter Server 5.1

The VMware ESX server must use the same time as the NTP server so that the virtual appliance functions correctly. Synchronizing the VMware ESX server time with the NTP server time avoids a time failure.

Software requirements

Before you use Unified Manager, you must install Adobe Flash Player 10.0 or later. You can download the software from the Adobe downloads site.

Before you download Flash Player, you must ensure that file downloads are enabled on your web browser. If you are using Microsoft Internet Explorer, you must verify that the security settings for ActiveX controls are enabled.

You must install Adobe Flash Player for each browser type that you intend to use with Unified Manager, even if the browsers are on the same system. For example, if you have installed both Mozilla Firefox and Microsoft Internet Explorer on the same system and you might use both browsers to access the web UI, you must install Adobe Flash Player on both the browsers, as required.

Supported versions of Data ONTAP

Unified Manager 6.0 supports clustered Data ONTAP 8.1.1, 8.1.2, 8.1.3 and 8.2.

Browser requirements

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

Unified Manager 6.0 supports the following browsers and client platforms; other browsers might work but have not been qualified:

Supported browsers

- Internet Explorer, versions 8.0 (32-bit), 9.0, and 10.0
- Chrome, versions 25 and 26
- Mozilla Firefox, versions 19 and 20

Supported client platforms

- Windows Vista, Windows 7, and Windows 8
- RHEL version 6
- SLES version 11 SP2
- Macintosh OS X 10.8

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

You do not have to specify port numbers when connecting to the Unified Manager web UI, because default ports are always used. For example, you can enter `https://<host>` instead of `https://<host>:443`. The default port numbers cannot be changed.

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

Interface	Protocol	Port	Description
Unified Manager web UI	HTTP	80	Used to access the Unified Manager web UI; automatically redirects to the secure port 443
Unified Manager web UI and programs using APIs	HTTPS	443	Used to securely access the Unified Manager web UI or to make API calls; API calls can only be made using HTTPS

Interface	Protocol	Port	Description
Maintenance console	SSH/SFTP	22	Used to access the maintenance console and retrieve support bundles
MySQL database	MySQL	3306	Used to enable OnCommand Workflow Automation and OnCommand Report access to Unified Manager

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.

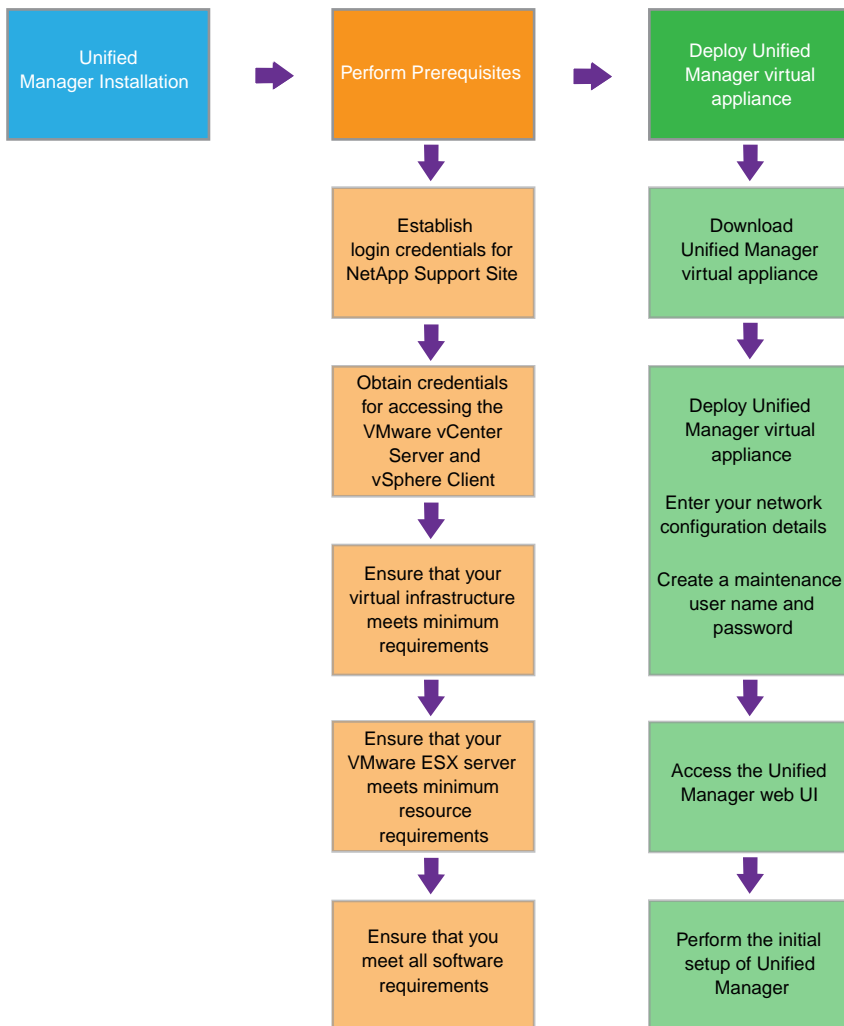
The Unified Manager server connects using the following protocols and ports to the managed storage systems, servers, and other components:

Destination	Protocol	Port	Description
Storage system	HTTPS	443	Used to monitor and manage storage systems
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
Mail server	SMTP	25	Used to send alert notification emails
SNMP trap listener	SNMPv1 or SNMPv3	162/UDP	Used to send alert notification SNMP traps
NTP server	NTP	123/UDP	Used to synchronize the time on the Unified Manager server with an external NTP time server

Installing Unified Manager

The installation workflow describes the tasks that you must perform before you can use Unified Manager. Because Unified Manager runs as a virtual appliance on a VMware host, you actually deploy it rather than install it. After completing the deployment tasks, you can either add clusters immediately or perform additional configuration tasks and then add clusters.

Overview of the deployment sequence



Related tasks

[Deploying Unified Manager](#) on page 14

Deploying Unified Manager

This workflow shows you how to deploy Unified Manager, which includes downloading software, deploying the virtual appliance, creating a maintenance user name and password, and performing the initial setup in the web UI. You can only deploy Unified Manager 6.0 as a virtual appliance on a VMware host. This is different than previous versions of Unified Manager which were installed on Windows or Linux servers.

Before you begin

You must have completed the system requirements for deployment. To ensure that your environment meets the minimum requirements, see [System requirements](#) on page 8.

You must have the following information:

- The login credentials for the NetApp Support Site
- Credentials for accessing the VMware vCenter Server and vSphere Client
- The IP address of the ESX Server on which you are deploying the Unified Manager virtual appliance
- Details about the data center, such as storage space in data store and memory requirements

About this task

You should access the maintenance console using the VMware console and not using SSH. For more information on the maintenance console, see the *OnCommand Unified Manager Administration Guide*.

After you finish

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

Steps

1. [Download Unified Manager](#) on page 15
You must download Unified Manager from the the NetApp Support Site.
2. [Deploy the Unified Manager virtual appliance](#) on page 15
You must deploy the Unified Manager virtual appliance after you download the `OnCommandUnifiedManager-6.0.ova` file from the NetApp Support Site. You must use VMware vSphere Client to deploy the virtual appliance on an ESX server. When you deploy the virtual appliance, a virtual machine is created.
3. [Access the user interface](#) on page 19

After you have deployed the virtual appliance, you can access the web UI to set up Unified Manager so that you can begin monitoring your clustered Data ONTAP systems.

4. *Perform the initial setup of the Unified Manager web UI* on page 20

To use Unified Manager, you must first configure the initial setup options, including the NTP server, the maintenance user email address, and the SMTP server host name and options. Enabling periodic AutoSupport is also recommended, but not mandatory.

Related concepts

What the maintenance user does on page 5

System requirements on page 8

Downloading Unified Manager

You must download Unified Manager from the the NetApp Support Site.

Before you begin

You must have login credentials for the NetApp Support Site.

About this task

The OnCommandUnifiedManager-6.0.ova file contains the Unified Manager software configured in a virtual appliance.

Steps

1. Download the OnCommandUnifiedManager-6.0.ova file from the NetApp Support Site.
2. Save the OnCommandUnifiedManager-6.0.ova file to a local or network directory that is accessible to your vSphere Client.

Deploying the Unified Manager virtual appliance

You must deploy the Unified Manager virtual appliance after you download the OnCommandUnifiedManager-6.0.ova file from the NetApp Support Site. You must use VMware vSphere Client to deploy the virtual appliance on an ESX server. When you deploy the virtual appliance, a virtual machine is created.

Before you begin

You must have completed the system requirements for deployment. To ensure that your environment meets the minimum requirements, see *System requirements* on page 8. If changes are required to meet system requirements, you must implement the changes before deployment of the Unified Manager virtual appliance.

If you use DHCP, you must have ensured that the DHCP server is available, and that the DHCP and VM network adapter configurations are correct. DHCP is configured by default.

If you use a static networking configuration, you must have ensured that the IP address is not duplicated in the same subnet.

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

- Credentials for accessing the VMware vCenter server and vSphere Client
- IP address of the ESX server on which you are deploying the Unified Manager virtual appliance
- Details about the data center, such as availability of storage space
- Static network configuration information (if not using DHCP):
 - Host fully qualified domain name (FQDN)
 - Host IP address
 - Network mask
 - IP address of the default gateway
 - Primary and secondary DNS addresses
 - Search domains

About this task

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.

If you are using a static network configuration, you should verify that the appropriate DNS server entries have been configured.

VMware High Availability for the Unified Manager virtual appliance is not supported.

If your environment is DHCP-enabled, but you want to use a static network configuration, you can install the virtual appliance using DHCP and then change the configuration to a static network configuration. For more information, see [Editing the network settings](#) on page 24.

You can change the default configuration of the virtual appliance after it has been deployed. See [Modifying the default configuration to the alternate configuration](#) on page 19.

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.

Note: This virtual appliance requires Reservation of Memory and CPU resources. For minimum requirements to run the Unified Manager virtual appliance, reference the [Virtual infrastructure requirements](#) on page 8.

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

If the Power On operation fails due to insufficient resources, you must have sufficient resources in the ESX server where the virtual appliance is deployed. If you do not have sufficient resources,

you can modify the resource settings for Memory and CPUs. The resources must be Reserved. See [Virtual infrastructure requirements](#) on page 8.

4. Click the **Console tab.**

The initial boot process takes a few minutes to complete.

If a reset occurs during the first boot process, the virtual appliance must be redeployed.

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

All date information displayed uses the time zone 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 both your storage systems and the management server are configured with the same time sync server, they refer to the same instant in time, even if they appear differently. For example, if you make a Snapshot copy using a device configured using a different time zone than the management server, the time reflected in the time stamp is the management server time.

6. Proceed to step 10 if DHCP is configured correctly and the virtual appliance obtains a DHCP address.

If you use a DHCP-enabled network, the fully-qualified domain name and DNS server entries are given to the virtual appliance automatically. If DHCP is not properly configured with DNS, the host name “OnCommand” 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.

7. If no DHCP services are available or if you use a static network configuration, select one of the following options:

If you use...	Then Select...
DHCP	Retry DHCP
	If you plan to use DHCP, you should ensure that it is configured correctly.
A static network configuration	Set up a static network configuration

8. If you use a static network configuration, enter your network configuration details in the VM console.

The IP address used must be unique to the host on which it is deployed. You should not use an IP address that is already in use.

The configuration process takes a few minutes to complete.

9. Confirm the values you entered and select **Y.**

10. At the prompt, create and type a maintenance user name and click **Enter.**

11. At the prompt, create and type a password and click **Enter.**

The VM console displays the URL for the Unified Manager web UI.

After you finish

You can either access the web UI to perform the initial setup of Unified Manager, or you can configure additional network settings in the maintenance console and then access the web UI.

The monitoring capacities of the default and alternate configurations

Before modifying your configuration, you should take into consideration how many storage objects you need to monitor.

Unified Manager can monitor up to 24 clusters in each deployment instance and can include as many or as few member nodes per cluster as necessary.

The following table displays the total number of storage objects that each configuration can monitor:

Configuration type	Approximate number of storage objects
Default configuration	230,000 - 940,000
Alternate configuration	0 - 230,000

Storage objects can include the following:

- Disk shelves
- Cluster nodes
- Vservers
- Clusters
- Aggregates
- Disks
- Qtrees
- Network ports
- LUNs
- iGroups
- CIFS shares
- Volumes
- LIFs
- Exports
- SnapMirror relationships
- SnapVault relationships

Modifying the default configuration

You can modify the default configuration based on the size of your environment and your sizing requirements, enabling you to preserve your resources. You must use the default configuration upon initial deployment.

Before you begin

- You must have considered your sizing requirements. See [Considerations before modifying your configuration](#) on page 18.
- You must have credentials for accessing the VMware vCenter server and vSphere Client.
- You must have shut down the virtual appliance.
- You must know the values supported values for the alternate configuration. See [Virtual infrastructure requirements](#) on page 8.

Steps

1. In the vSphere Client, select the VM on which the virtual appliance is located.
2. Right-click the virtual appliance and click **Edit Settings**.
3. Click the **Hardware** tab.
4. Click **Memory** and set memory size to 8 GB.
5. Click **CPUs** and set the number of virtual sockets to 2.
Do not change the value for number of cores per socket.
6. Click the **Resources** tab.
7. Click **CPUs** and set reservation to 4786 MHz.
8. Click **Memory** and verify that the Reservation is set to 8192 MB.
9. Click **OK**.
10. Start the virtual machine.

Accessing the Unified Manager web UI

After you have deployed the virtual appliance, you can access the web UI to set up Unified Manager so that you can begin monitoring your clustered Data ONTAP systems.

Before you begin

- The Unified Manager virtual appliance must be deployed.
- If this is the first time you are accessing the web UI, you must have created a maintenance user name and password.

Steps

1. Start the Unified Manager web UI from your browser by using the displayed link.

The link is in the following format: `https://IP_address` or `https://Fully Qualified Domain Name`.

2. Log in to the Unified Manager web UI using your maintenance user credentials.

Performing the initial setup of the Unified Manager web UI

To use Unified Manager, you must first configure the initial setup options, including the NTP server, the maintenance user email address, and the SMTP server host name and options. Enabling periodic AutoSupport is also recommended, but not mandatory.

Before you begin

You must have performed the following operations before performing the initial setup:

- Deployed the Unified Manager virtual appliance
- Accessed the web UI using the URL provided in the maintenance console after deployment
- Entered the maintenance user name and password created during deployment

About this task

The OnCommand Unified Manager Initial Setup dialog box appears only when you first access the web UI. If you want to change any options, you can use the Setup Options dialog box, which is accessible from the Administration menu.

Steps

1. In the **OnCommand Unified Manager Initial Setup** dialog box, choose **Yes** to enable AutoSupport capabilities and click **Continue**.

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

2. Type the NTP server, maintenance user email address, the SMTP server host name, and any additional SMTP options, and click **Save**.

The **Get Started** area appears.

3. (Optional) To add clusters for monitoring, click **Add Cluster**.

Adding a cluster enables Unified Manager to monitor your cluster components, but alert notifications are not sent until they are configured.

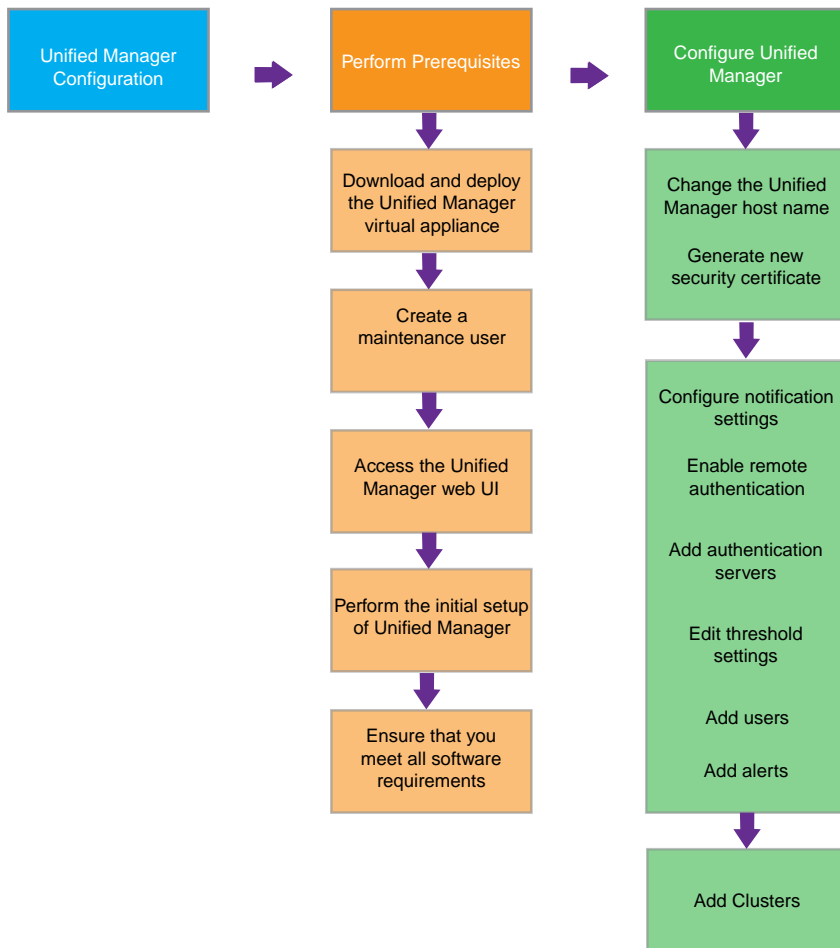
After you finish

If you choose not to immediately add clusters, you can configure additional options, such as alerts and thresholds, and then add clusters for monitoring. See [*Configuring Unified Manager*](#) on page 23.

Configuring Unified Manager

After deploying the Unified Manager virtual appliance and completing the initial setup to access the web UI, you can add clusters immediately or perform additional configuration tasks before adding clusters, such as changing the host name, adding alerts, and adding users. The configuration workflow describes the tasks you might want to perform after completing the installation.

Overview of the configuration sequence



Related tasks

[Configuring your environment after deployment](#) on page 23

Configuring your environment after deployment

After you deploy the Unified Manager virtual appliance, there are several configuration tasks that you might want to perform before you start monitoring your clusters, such as changing the host name, adding alerts, and adding users.

Before you begin

- You must have deployed the virtual appliance and completed the OnCommand Unified Manager Initial Setup.
- You must be logged in as the OnCommand Administrator to complete all tasks in this workflow.

About this task

After you completed the OnCommand Unified Manager Initial Setup, you were presented with the option of adding clusters. If you did not add clusters at that time, you must add them before you can start monitoring cluster objects. You can add clusters at any time. However, there are some configuration changes that you might want to make to Unified Manager prior to, or after, adding clusters.

Choices

- [Changing the Unified Manager host name](#) on page 24

When you deployed Unified Manager, an SSL certificate was generated for HTTPS access. A host name was associated with the certificate, allowing you to use the host name to access the Unified Manager web UI. You might want to change this host name after deployment.

- [Configuring Unified Manager to send alert notifications](#) on page 27

After the clusters have been added to Unified Manager, you can monitor them, but you cannot receive notifications about events in your cluster environment until you configure several options, such as the email address from which notifications are sent, the users to receive the alerts, and so forth. You might also want to modify the default threshold settings at which events are generated.

- [Adding clusters](#) on page 35

You must manually add clusters to Unified Manager before you can monitor them.

Related concepts

[Installing Unified Manager](#) on page 13

Changing the Unified Manager host name

When the virtual appliance is first deployed, the network host is assigned a name. You can change the host name after deployment. If you change the host name, you should also regenerate the HTTPS certificate.

Before you begin

You must be signed in to Unified Manager as the maintenance user or have the OnCommand Administrator role assigned to you to perform these tasks.

About this task

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 would have designated a name for the network host. If you configured the network using DHCP, the host name should be taken from the DNS. If DHCP or DNS are not properly configured, the host name “OnCommand” is automatically assigned and associated with the security certificate.

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

If you access the web UI by using the server's IP address instead of the host name, you do not need to generate a new certificate if you change the host name. However, it is highly recommended that you do update the certificate, so that the host name in the certificate matches the actual host name.

The new certificate does not take effect until Unified Manager is restarted.

Steps

1. [Edit the network settings](#) on page 24

You can change the host name from the Configure Network Settings dialog box, accessed from the Administration menu.

2. [Generate an HTTPS security certificate](#) on page 26

If you want to use the new host name to access the Unified Manager web UI, you must regenerate the HTTPS certificate to associate it with the new host name.

3. [View the HTTPS security certificate](#) on page 26

You should verify that the correct information is displayed after generating a new security certificate, then restart Unified Manager.

4. [Restart the Unified Manager virtual machine](#) on page 27

If you regenerate the HTTPS certificate, then you must restart the virtual machine.

Editing the network settings

You might want to edit network settings if an IP address changes due to the migration of a virtual machine (VM) to a different ESX server in a different domain, when maintenance is performed on

your network equipment, if you switch from a DHCP to a static network configuration, or if you switch from a static network to a DHCP configuration.

Before you begin

- You might need one or more of the following: host name or FQDN, IP address, DHCP, network mask, gateway, primary and secondary DNS addresses, and search domains.
- If you are changing your network settings from DHCP-enabled to static network configuration, you should have done the following:
 - Ensured that the IP address and gateway are reachable.
 - Ensured that the IP address does not contain a duplicate address.
 - Verified that the primary and secondary DNS addresses are ready and available to send and receive network traffic.
- You must be authorized to perform all the steps of this task; your administrator can confirm your authorization in advance.

About this task

When you switch to a DHCP configuration, the previous host name is replaced by the name specified by your DHCP server.

The self-signed SSL certificate generated during deployment is associated with the host name (or FQDN) and the IP address. If you change either of these values and want to use that new host name or IP address to connect to Unified Manager, then you must generate a new certificate. The new certificate does not take effect until the Unified Manager virtual machine is restarted.

Steps

1. Click **Administration > Configure Network Settings**.
2. In the **Configure Network Settings** dialog box, modify the host and network settings, as required.

Tip: You can enter multiple comma-separated values in the Secondary DNS Address and Search Domains fields.
3. Click **Update**.

After you finish

After you have modified the settings of your network configuration, you can use the updated configuration to access Unified Manager.

Generating an HTTPS security certificate

You might generate a new HTTPS security certificate for multiple reasons, including if you want to sign with a different Certificate Authority or if the current security certificate has expired. The new certificate replaces the existing certificate.

Before you begin

You must have the OnCommand Administrator role to perform this task.

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Management Server > HTTPS**.
3. Click **Regenerate HTTPS Certificate**.

Important: You must restart the Unified Manager virtual machine before the new certificate will take effect. This can be done from the System Configuration option in the NetApp maintenance console or from the VM console.

After you finish

After generating a new certificate, you can verify the new certificate information by viewing the HTTPS certificate.

Viewing the HTTPS security certificate

You can compare the HTTPS certificate details to the retrieved certificate in your browser to ensure that your browser's encrypted connection to Unified Manager is not being intercepted. You can also view the certificate to verify the content of a regenerated certificate or to view alternate URL names from which you can access Unified Manager.

Before you begin

You must have the OnCommand Administrator role to perform this task.

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Management Server > HTTPS**.
3. Click **View HTTPS Certificate**.

The Subject DN field should display the same host name or fully qualified domain name (FQDN) that is displayed in the Configure Network Settings dialog box. The IP addresses should also be the same in the certificate and in the network settings.

To view more detailed information about the security certificate, you can view the connection certificate in your browser.

Restarting the Unified Manager virtual machine

You can restart the virtual machine from the maintenance console. You might need to restart after generating a new security certificate or if there is a problem with the virtual machine.

Before you begin

The virtual appliance must be powered on.

You must be logged in to the NetApp maintenance console as the maintenance user.

About this task

You can also restart the virtual machine from vSphere by using the Restart Guest option. See the VMware documentation for more information.

Steps

1. Access the maintenance console.
2. Select **System Configuration > Reboot Virtual Machine**.
3. Start the Unified Manager GUI from your browser and log in.

Configuring Unified Manager to send alert notifications

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

Before you begin

You must be signed in to the web UI as the OnCommand Administrator.

About this task

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

You can complete the following tasks to properly configure your environment and to add alerts.

Steps

1. [*Configure notification settings*](#) on page 28

If you want alert notifications sent when certain events occur in your environment, you must supply an email address from which the alert notification can be sent. If your configuration uses

an SMTP server for email authentication, then you must provide the user name and password for the server. If you want to use SNMP traps, you can select that option and provide the necessary information.

2. [Enable remote authentication](#) on page 29

If you want remote LDAP or Active Directory users to access the Unified Manager instance and receive alert notifications, then you must enable remote authentication.

3. [Add authentication servers](#) on page 29

If you enable remote authentication, then you must identify authentication servers.

4. [Edit global threshold settings](#) on page 30

You can modify the threshold settings for aggregates, volumes, and certain types of protection relationships. These settings determine when an event should be generated, which can affect when an alert notification is sent.

5. [Add users](#) on page 32

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

6. [Add alerts](#) on page 33

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

Configuring notification settings

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

Before you begin

The following information must be available:

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

You must have the role of OnCommand Administrator to change notification settings.

Steps

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

3. In the **Notification Setup Options** dialog box, configure the appropriate settings.

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

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

Enabling remote authentication

You can enable remote authentication (LDAP, Active Directory) to enable the management server to communicate with your authentication servers and to enable users of the authentication servers to use Unified Manager and manage the storage objects and data.

Before you begin

You must have the role of OnCommand Administrator to enable remote authentication.

About this task

If remote authentication is disabled, remote users or groups will no longer be able to access Unified Manager.

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Management Server > Authentication**.
3. Select **Enable Remote Authentication**.
4. Optional: Add authentication servers and test the authentication.
5. Click **Save and Close**.

Adding authentication servers

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

Before you begin

- The following information must be available:
 - Host name or IP address of the authentication server
 - Port number of the authentication server
- You must have enabled remote authentication and configured your authentication service so that the management server can authenticate remote users or groups in the authentication server.
- You must be authorized to perform all the steps of this task; your administrator can confirm your authorization in advance.

About this task

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

Steps

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

Result

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

After you finish

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

Editing global threshold settings

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

About this task

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

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

Choices

- [Configuring global aggregate threshold values](#) on page 31
You can edit the threshold settings for capacity, growth, and Snapshot copies for all aggregates to track any threshold breach.
- [Configuring global volume threshold values](#) on page 31

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

- [Editing unmanaged relationship lag thresholds](#) on page 32

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

Configuring global aggregate threshold values

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

Before you begin

You must be authorized to perform all the steps of this task; your administrator can confirm your authorization in advance.

About this task

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

Steps

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

Configuring global volume threshold values

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

Before you begin

You must be authorized to perform all the steps of this task; your administrator can confirm your authorization in advance.

About this task

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

Steps

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

Editing unmanaged relationship lag threshold settings

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

Before you begin

You must be authorized to perform all the steps of this task; your administrator can confirm your authorization in advance.

Steps

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

Adding a user

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

Before you begin

- To add a remote user or group, you must have enabled remote authentication and configured your authentication server.
- You must be logged in as the OnCommand Administrator to perform this task.

About this task

If you add a group from active directory, then all direct members and nested subgroups can authenticate to Unified Manager. If you add a group from OpenLDAP or Other authentication services, then only direct members of that group can authenticate to Unified Manager.

Steps

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

Adding an alert

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

Before you begin

- You must have configured the notification settings such as email address, SMTP server, and SNMP trap host so that the Unified Manager server can use these settings to send notifications to users when an event is generated.
- The following information must be available: resources and events for which you want to trigger the alert, and user names or email addresses of users you want to notify.
- You must have the role of OnCommand Administrator to add an alert.

About this task

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

Steps

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

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

Note: The text string that you specify is case-sensitive.

If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule, and the alert is not generated for events related to the excluded resource.

Tip: To select more than one resource, press the Ctrl key while you make your selections.

- c) Click **Events** and select the events based on the event name or event severity type for which you want to trigger an alert.

Tip: To select more than one event, press the Ctrl key while you make your selections.

- d) Click **Recipients** and select the users that you want to notify when the alert is generated and the notification frequency.

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

You can also choose to notify users through SNMP traps.

4. Click **Save**.

Example for adding an alert

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

- Alert name: Test
- Resources: includes all volumes whose name contains “vol0” and excludes all the volumes whose name contains “xyz”
- Events: includes all critical events
- Recipients: includes “sample@domain.com” and the user has to be notified every 15 minutes

Perform the following steps in the Add Alert dialog box:

1. Click **Name** and enter **Test** in the **Alert Name** field.
2. Click **Resources** and in the Include tab, select Volumes from the drop-down list.
 - a. Enter **vol0** in the **Name contains** field to display the volumes whose name contains vol0.
 - b. Select <<**All Volumes whose name contains 'vol0'**>> from the Available Resources area and move it to the Selected Resources area.
 - c. Click **Exclude** and enter **xyz** in the **Name contains** field and then click **Add**.
3. Click **Events** and select Critical from the **Event Severity** field.
 - a. Select **All Critical Events** from the Matching Events area and move it to the Selected Events area.
4. Click **Recipients** and enter **sample@domain.com** in the **Alert these users** field.
5. Select **Remind every 15 minutes** to set the frequency to notify the user every 15 minutes. You can configure an alert to repeatedly send notification to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.

6. Click **Save.**

Adding clusters

You can add an existing cluster to Unified Manager to monitor the cluster and obtain information such as its health, capacity, and configuration.

Before you begin

- The following information must be available:
 - Host name or cluster management IP address
The host name is the FQDN or short name that Unified Manager uses to connect to the cluster.
The cluster management IP address must be the cluster-management LIF of the admin Vserver. If you use a node-management LIF, the operation fails.
 - User name and password to access the cluster
 - Type of protocol that can be configured on the cluster and the port number of the cluster
- You must be authorized to perform all the steps of this task; your administrator can confirm your authorization in advance.

Steps

1. Click **Storage > Clusters**.
2. On the **Clusters** page, click **Add**.
3. In the **Add Cluster** dialog box, specify the values as required and then click **Add**.

Result

The cluster is added to the Unified Manager database after the default monitoring interval of approximately 15 minutes.

Changing the local user password

You can change your login password to prevent potential security risks.

Before you begin

You must be logged in as a local user.

About this task

The passwords for the maintenance user and for the remote user cannot be changed from the web UI. To change the maintenance user password, use the OnCommand Unified Manager Maintenance Console. To change the remote user password, contact your password administrator.

Steps

1. Log in to Unified Manager.
2. Click *user_name* > **Change Password**.

The **Change Password** option is not displayed if you are a remote user.

3. In the **Change Password** dialog box, enter the details as required.
4. Click **Save**.

Unified Manager 6.0 upgrade overview

Because Unified Manager 6.0 is deployed only as a virtual instance, there is no upgrade path from Unified Manager 5.x; you just deploy Unified Manager 6.0.

You can install Unified Manager 5.x on physical servers and on virtual machines. In contrast, you deploy Unified Manager 6.0 only as a virtual instance. Therefore, both Unified Manager 5.x and Unified Manager 6.0 can monitor clustered Data ONTAP systems concurrently.

However, if Unified Manager 5.x and Unified Manager 6.0 are both polling the same clusters, the increased overhead might result in slower response times.

Note: Unified Manager 6.0 does not automatically discover and use relationships and alerts that you configured for Unified Manager 5.x. Therefore, when you deploy Unified Manager 6.0, you must reconfigure all backup and mirror relationships and all alerts.

For information about migrating Data ONTAP 7G and 7-Mode FlexVol volumes and configuration to hardware that is running clustered Data ONTAP 8.2, see the 7-Mode Transition Tool 1.0 *Data and Configuration Transition Guide For Transitioning to Clustered Data ONTAP 8.2*.

Related tasks

[Removing Unified Manager 6.0](#) on page 38

[Deploying Unified Manager](#) on page 14

Removing Unified Manager 6.0

You can uninstall Unified Manager 6.0 by destroying the virtual appliance on which the Unified Manager software runs.

Before you begin

You must have downloaded and deployed the virtual appliance.

You must have credentials for accessing VMware vCenter Server and vSphere Client.

Steps

1. In vSphere Client, click **Home > Inventory > VMs and Templates**.
2. Select the VM that you want to destroy.
3. Click the **Summary** tab.
4. If the VM is running, click **Commands > Shut Down Guest**.
5. Right-click the VM that you want to destroy and click **Delete from Disk**.

Copyright information

Copyright © 1994–2013 NetApp, Inc. All rights reserved. Printed in the U.S.

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

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

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

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

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

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

Trademark information

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Mars, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

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

Index

.ova file
 deploying [15](#)
 downloading [15](#)

6.0 release of Unified Manager
 introduction to [5](#)

A

accessing
 Unified Manager web UI [19](#)
adding
 alerts [33](#)
 authentication servers [29](#)
 clusters [35](#)
 remote groups [32](#)
 remote users [32](#)
aggregates
 configuring global threshold values for [31](#)
alerts
 adding [33](#)
 configuring your environment for [27](#)
 creating [33](#)
alternate configuration
 monitoring capacities [18](#)
assigning
 user roles [32](#)
authentication
 adding servers [29](#)
 enabling remote [29](#)
AutoSupport
 what it does [6](#)

B

browsers
 requirements [11](#)

C

certificates
 generating HTTPS security certificates [26](#)
 viewing HTTPS security certificates [26](#)
Chrome

 browser requirements [11](#)
clustered Data ONTAP systems
 adding [35](#)
clustered system management tasks
 choosing the correct OnCommand management
 software to perform [6](#)
clusters
 adding [35](#)
configurations
 monitoring capacities [18](#)
configuring
 aggregate global threshold values [31](#)
 DNS [24](#)
 network settings [24](#)
 notification settings [28](#)
 thresholds [30](#)
 Unified Manager [22](#)
 volume global threshold values [31](#)
 your environment [23](#)
CPU requirements
 table of [8](#)
creating
 alerts [33](#)
 database users [32](#)
 local users [32](#)

D

Data ONTAP
 supported versions [11](#)
Data ONTAP 8.2.x tasks
 choosing the correct OnCommand management
 software to perform [6](#)
database users
 creating [32](#)
default configuration
 modifying [19](#)
 monitoring capacity [18](#)
deploying
 Unified Manager [13](#), [14](#)
 Unified Manager virtual appliance (Vapp) [15](#)
DHCP
 enabling [24](#)
DNS
 configuring [24](#)

E

- editing
 - network settings [24](#)
 - unmanaged relationship lag threshold settings [32](#)
- enabling
 - DHCP [24](#)
- environment
 - setup [23](#)
- ESX requirements
 - virtual appliance [10](#)
- ESXi requirements
 - virtual appliance [10](#)

F

- Firefox
 - browser requirements [11](#)

H

- hardware
 - requirements [8](#)
- host name
 - changing [24](#)
- HTTPS
 - generating new security certificates [26](#)
 - viewing the security certificate [26](#)

I

- infrastructure requirements
 - table of [8](#)
- installation
 - downloading [15](#)
- installing
 - accessing the GUI [19](#)
 - configuring initial setup [20](#)
 - deploying the virtual appliance (Vapp [15](#)
 - Unified Manager [13](#), [14](#)
- Internet Explorer
 - browser requirements [11](#)

L

- license requirements
 - VMware vSphere [8](#)
- local users
 - creating [32](#)

M

- maintenance console
 - restarting the virtual machine [27](#)
 - restarting Unified Manager [27](#)
 - role of maintenance user [5](#)
- maintenance user
 - what it does [5](#)
- memory requirements
 - table of [8](#)
- migrating to clustered Data ONTAP
 - where to go for more information [37](#)
- modifying
 - unmanaged relationship lag threshold settings [32](#)

N

- network settings
 - configuring [24](#)
 - customizing the host name [24](#)
 - editing [24](#)
- notification
 - adding alerts [33](#)
 - configuring settings [28](#)

O

- OnCommand management software
 - System Manager versus Unified Manager [7](#)
 - which software to use for each task type [6](#)
- OnCommand Unified Manager
 - configuring the virtual appliance [20](#)
 - downloading [15](#)
 - running 6.0 concurrently with 5.x [37](#)
- oncommand.6.0.ova file
 - deploying [15](#)
 - downloading [15](#)

P

- passwords
 - changing [35](#)
- physical storage
 - adding clusters [35](#)
- ports
 - requirements [11](#)

R

- relationships
 - unmanaged, editing lag thresholds settings for [32](#)
- releases of Unified Manager
 - introduction to 6.0 [5](#)
- remote authentication
 - enabling [29](#)
- remote groups
 - adding [32](#)
- remote users
 - adding [32](#)
- removing
 - Unified Manager 6.0 [38](#)
- requirements
 - browser [11](#)
 - Data ONTAP, supported versions [11](#)
 - hardware [8](#)
 - software [10](#)
 - system [8](#)
 - virtual appliance [10](#)
 - VMware vSphere licenses [8](#)
- roles
 - assigning to users [32](#)

S

- security certificates
 - generating, HTTPS [26](#)
 - viewing, HTTPS [26](#)
- servers
 - required ports [11](#)
- setting up
 - aggregate global threshold values [31](#)
 - notification settings [28](#)
 - SMTP server [28](#)
 - SNMP [28](#)
 - thresholds [30](#)
 - volume global threshold values [31](#)
- setup
 - post-deployment [23](#)
- software requirements [10](#)
- System Manager
 - comparison to Unified Manager [7](#)
- system requirements
 - Unified Manager [8](#)

T

- task types

- choosing the correct OnCommand management software to perform [6](#)
- tasks
 - choosing the correct OnCommand management software to perform [6](#)
- thresholds
 - configuring [30](#)
 - editing settings for unmanaged relationships [32](#)
 - global values for aggregates [31](#)
 - global values for volumes [31](#)
- types of users
 - maintenance user [5](#)

U

- UI
 - accessing [19](#)
- Unified Manager
 - accessing the web UI [19](#)
 - comparison to System Manager [7](#)
 - configuring [22](#)
 - deploying [13, 14](#)
 - downloading [15](#)
 - installing [13, 14](#)
 - introduction to 6.0 [5](#)
 - uninstalling 6.0 [38](#)
- uninstalling
 - Unified Manager 6.0 [38](#)
- unmanaged relationships
 - editing lag thresholds settings for [32](#)
- upgrading to 6.0
 - overview [37](#)
- user roles
 - assigning [32](#)
- user tasks
 - choosing the correct OnCommand management software to perform [6](#)
- users
 - adding [32](#)
 - changing passwords [35](#)
 - creating [32](#)
 - maintenance user [5](#)

V

- vApp
 - See* virtual appliance
- Vapp
 - See* virtual appliance
- virtual appliance

- requirements [10](#)
- what it does [5](#)
- virtual appliance (Vapp)
 - configuring initial setup [20](#)
 - deploying [15](#)
 - destroying [38](#)
- virtual appliance default configuration
 - modifying [19](#)
- virtual machine
 - restarting [27](#)
- volumes
 - configuring global threshold values for [31](#)
- vSphere requirements
 - virtual appliance [10](#)