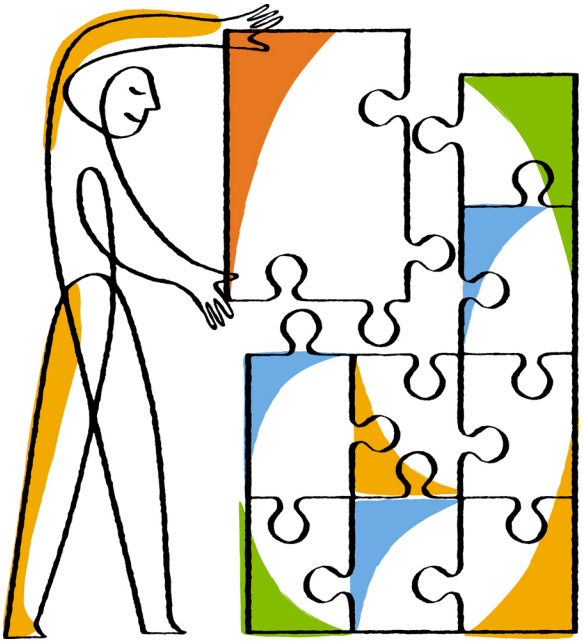
OnCommand® Unified Manager 6.2

Installation and Setup Guide

For VMware Virtual Appliances



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: 215-09222_B0
March 2015

Contents

Introduction to Unified Manager 5
What a virtual appliance does 5
What the maintenance user does 5
What AutoSupport does 6
System requirements for deploying the virtual appliance 7
License requirements for Unified Manager 7
Virtual infrastructure requirements 7
Virtual appliance requirements 9
Software requirements 9
Supported versions of Data ONTAP 9
Supported browsers and platforms 10
Protocol and port requirements 10
Installing Unified Manager 12
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 20
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
Adding clusters 28
Configuring Unified Manager to send alert notifications 29
Changing the local user password 38
Setting up a connection between Performance Manager and Unified Manager 40
Creating a user with Event Publisher role privileges 41
Configuring a connection between a Performance Manager server and Unified Manager 41

Deleting a connection between a Performance Manager server and Unified Manager 43
Setting up a connection between OnCommand Workflow Automation and Unified Manager 45
Creating a database user 45
Setting up a connection between OnCommand Workflow Automation and Unified Manager 46
Unified Manager 6.2 upgrade overview 48
Upgrading to Unified Manager 6.2 49
Downloading the Unified Manager 6.2 ISO image 49
Upgrading to OnCommand Unified Manager 6.2 50
Cannot log in to the web UI after upgrading to OnCommand Unified Manager 6.2 51
Removing Unified Manager 6.2 53
Troubleshooting Unified Manager installation on VMware virtual appliance 54
Error message displayed when maintenance user is not created during the virtual appliance deployment 54
Copyright information 55
Trademark information 56
How to send comments about documentation and receive update notification 57
Index 58

Introduction to Unified Manager

You can deploy Unified Manager 6.2 as a virtual appliance on a VMware host, or on a Linux server. This guide describes how to deploy Unified Manager as a virtual appliance.

Unified Manager 6.2 is built on a server infrastructure that delivers scalability, supportability, and enhanced monitoring and notification capabilities. Clustered environments running Data ONTAP are visualized in the new graphical interface that provides at-a-glance status for capacity, availability, protection, and performance views of monitored systems.

Unified Manager 6.2 supports monitoring of clustered Data ONTAP 8.3 and 8.2.x systems. Unified Manager 6.2 also supports vaulting, nondisruptive operations, Storage Virtual Machines (SVMs) with Infinite Volume, reporting, and MetroCluster configurations.

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

Related information

NetApp Interoperability Matrix Tool

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

If Unified Manager is installed as a virtual appliance, the maintenance user is created during initial configuration, the maintenance user can create subsequent users and assign them roles. The maintenance user has OnCommand administrator role in the web UI. If Unified Manager is installed as a virtual appliance, the maintenance user can also access the Unified Manager maintenance console.

If Unified Manager is installed as a virtual appliance, the maintenance user can perform the following functions using the maintenance console:

- Configure network access
- Upgrade to newer versions of Unified Manager

- Shut down virtual appliances (only from VMware console)
- Increase data disk or swap disk size
- Change the time zone
- Generate support bundles to send to technical support

What AutoSupport does

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

System requirements for deploying the virtual appliance

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 6.2 as a virtual appliance on an ESX server.

Unified Manager 6.2 requires OnCommand Workflow Automation 3.0 or later to provision SVMs with Infinite Volume with storage classes, or to configure SnapMirror and SnapVault data protection relationships.

Unified Manager requires OnCommand Performance Manager 1.1 to fully utilize performance features shown in the Unified Manager web UI.

For the most current information, see the Interoperability Matrix.

Related information

NetApp Interoperability Matrix Tool

License requirements for Unified Manager

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

Virtual infrastructure requirements

Your virtual infrastructure must meet minimum memory and CPU resource 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 If you deploy an NFS datastore on a storage system running clustered Data ONTAP, you must use the NetApp NFS Plug-in for VMware VAAI to use thick provisioning.	152 GB
Memory needed for the Unified Manager virtual appliance	Minimum 12 GB
Processors needed for the Unified Manager virtual appliance	Four 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 If you deploy an NFS datastore on a storage system running clustered Data ONTAP, you must use the NetApp NFS Plug-in for VMware VAAI to use thick provisioning.	152 GB
Memory needed for the Unified Manager virtual appliance	Minimum 8 GB
Processors needed for the Unified Manager virtual appliance	Two 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 supported.

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

- Lower the 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.

Note: Lowering VM reservations for CPU and memory is possible, but not below the minimum values listed in the table.

Virtual appliance requirements

You can deploy the virtual appliance on a VMware ESX server, which must meet minimum requirements.

The following versions of VMware ESXi are supported:

- ESXi 5.1
- ESX 5.1 (update 1)
- ESX 5.5

The following versions of vSphere are supported:

- VMware vCenter Server 5.1
- VMware vCenter Server 5.5

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 ensure that you meet the software requirements.

Supported versions of Data ONTAP

Unified Manager 6.2 supports clustered Data ONTAP 8.1.3, 8.1.4, 8.2.0 8.2.1, and 8.3. To monitor protection relationships, you must use Data ONTAP 8.2 or later.

Supported browsers and platforms

To use the Unified Manager GUI, you must use a supported browser that runs on a supported client platform.

Unified Manager has been tested with the following browsers and client platforms; other browsers might work but have not been qualified. See the Interoperability Matrix at *mysupport.netapp.com/matrix* for the complete list of supported browser versions.

Supported browsers

- Microsoft Internet Explorer 10 (Standards mode) or later
- Google Chrome, versions 36 or later
- Mozilla Firefox, versions 24 ESR and 31 ESR or later
- Apple Safari version 7 or later

Supported browser client platforms

- Windows Vista, Windows 7, and Windows 8
- Red Hat Enterprise Linux version 6
- SUSE Linux Enterprise Server 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, because Unified Manager always runs on its default port, you can enter `https://<host>` instead of `https://<host:443>`. The default port numbers cannot be changed.

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

Interface	Protocol	Port	Description
Unified Manager web UI	HTTP	80	Used to access the Unified Manager web UI; automatically redirects to the secure port 443.

Interface	Protocol	Port	Description
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.
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.

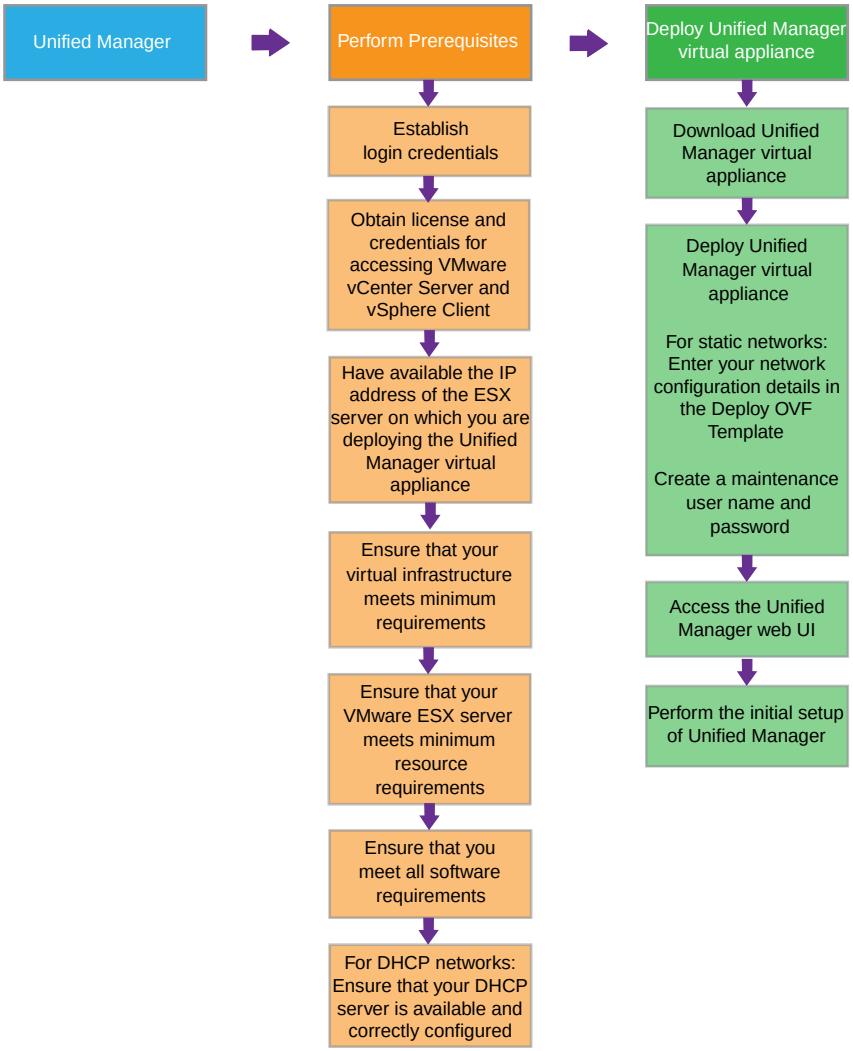
The Unified Manager server connects using the following protocols and ports to the managed storage systems, servers, and other components:

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 notification emails.
SNMP trap sender	SNMPv1 or SNMPv3	162/UDP	Used to send 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 add clusters and perform additional configuration tasks.

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.

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 7.

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
- VMware Tools CD-ROM or ISO image

About this task

You can deploy Unified Manager 6.2 as a virtual appliance on a VMware ESX server.

You can also install Unified Manager 6.2 on a Linux server. For more information on installing Unified Manager on a Linux server, see the *OnCommand Unified Manager Installation and Setup Guide for Redhat Enterprise Linux*.

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

VMware Tools are not included in the .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.

Steps

1. Download Unified Manager on page 15
   You must download Unified Manager before you can deploy the virtual appliance.
2. Deploy the Unified Manager virtual appliance on page 15

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

3. Access the user interface on page 20
   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 highly recommended.

Related concepts

What the maintenance user does on page 5
System requirements for deploying the virtual appliance on page 7

Downloading Unified Manager

You must download Unified Manager from the NetApp Support Site.

Before you begin

You have login credentials for the NetApp Support Site.

About this task

The `OnCommandUnifiedManager-6.2.ova` file contains the Unified Manager software configured in a virtual appliance.

Steps

1. Download the `OnCommandUnifiedManager-6.2.ova` file from the NetApp Support Site.
2. Save the `OnCommandUnifiedManager-6.2.ova` file to a local 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 must deploy the Unified Manager virtual appliance after you download the `OnCommandUnifiedManager-6.2.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 7. 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 and that the appropriate DNS server entries have been configured.

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

- 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 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
- VMware Tools CD-ROM or ISO image

About this task

VMware Tools are not included in the .ova file and must be installed 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.

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 vSphere Client, click **File > Deploy OVF Template**.
2. Complete the **Deploy OVF Template** wizard to deploy the Unified Manager virtual appliance.

   If your environment is DHCP-enabled, but you want to use a static network configuration, you can complete the Properties tab in the Deploy OVF Template and those settings are applied during deployment. While entering details for a static network configuration, you must ensure that the IP address is unique to the host on which it is deployed. You must not use an IP address that is already in use, and the IP address must have a valid DNS entry.

   Note: The virtual appliance requires Reservation of Memory and CPU resources. For minimum requirements to run the Unified Manager virtual appliance, see the *Virtual infrastructure requirements* on page 7.

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 7.

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. Follow the prompt to install the VMware Tools on the virtual machine.
6. 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.

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

8. At the prompt, create and type a maintenance user name and click **Enter**.
9. 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

- Storage Virtual Machines (SVMs)
- Clusters
- Aggregates
- Disks
- Qtrees
- Network ports
- LUNs
- igroups
- CIFS shares
- Volumes
- LIFs
- Exports
- SnapMirror relationships
- SnapVault relationships
- Quotas

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. However, you must use the default configuration upon initial deployment.

Before you begin

- You must have considered your sizing requirements.
- 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 supported values for the alternate configuration.
  See *Virtual infrastructure requirements* on page 7. You must not use values lower than those specified in the table for the alternate configuration.

Steps

1. In the vSphere Client, select the VM on which the virtual appliance is located.

2. Right-click the virtual appliance, and then click **Edit Settings**.
3. Click the **Hardware** tab.
4. Click **Memory**, and then set memory size to 8 GB.
5. Click **CPUs**, and then 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 then set reservation to 4786 MHz.
8. Click **Memory**, and then 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 log in as the maintenance user.

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 highly recommended.

Before you begin

You must have performed the following operations:

- 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, the 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.

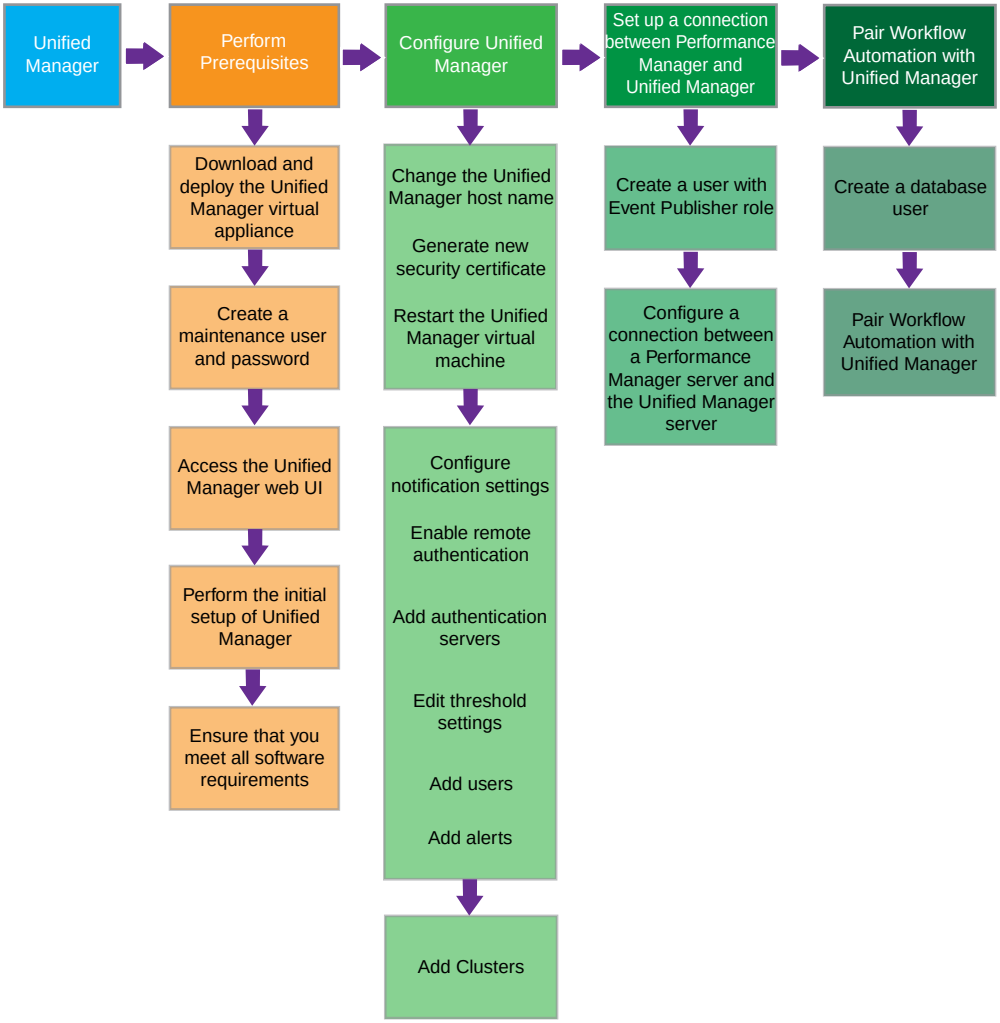
After you finish

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 and install Unified Manager, 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 installed Unified Manager and completed the Unified Manager initial setup.
- You must have the OnCommand Administrator role.

About this task

After you complete the Unified Manager initial setup, you can add 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 29

  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 and viewing the discovery status* on page 28

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

Related concepts

Installing Unified Manager on page 12

Changing the Unified Manager host name

The network host is assigned a name when the virtual appliance is first deployed . You can change the host name after deployment. If you change the host name, you must 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 is 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 have to generate a new certificate if you change the host name. However, it is the best practice to update the certificate so that the host name in the certificate matches the actual host name.

If you change the host name in Unified Manager, you must manually update the host name in Workflow Automation. The host name is not updated automatically.

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

Steps

1. *Edit the network settings* on page 25

   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 have the OnCommand Administrator role.

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.

About this task

Attention: If connections that enable performance monitoring are currently configured between the Unified Manager server and one or more Performance Manager servers, executing this task invalidates those connections and deactivates any further performance monitoring updates from Performance Manager servers to the Unified Manager web UI. You must reactivate those connections after completing 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 takes effect. You can use the **System Configuration** option in the NetApp maintenance console.

After you finish

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

If you need to reactivate performance monitoring updates from Performance Manager servers to the Unified Manager server, you must delete the connections that were invalidated by this task and reconfigure new connections.

Viewing the HTTPS security certificate

You can compare the HTTPS certificate details with 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.

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 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 VMware **Restart Guest** option.

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.

Related information

VMware vSphere PowerCLI Cmdlets Reference: Restart-VMGuest

Adding clusters

You can add a cluster to Unified Manager to monitor the cluster and obtain information such as its health, capacity, and configuration so you can find and resolve any issues that might arise. You can also view the cluster discovery status from the Manage Data Sources page.

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. This host name must resolve to the cluster-management IP address.
    The cluster-management IP address must be the cluster-management LIF of the administrative Storage Virtual Machine (SVM). If you use a node-management LIF, the operation fails.
  - Data ONTAP administrator user name and password
    The Data ONTAP administrator must be assigned the ONTAPI and SSH administrator roles.
  - Type of protocol (HTTP or HTTPS) that can be configured on the cluster and the port number of the cluster
- You must have the OnCommand Administrator or Storage Administrator role.

About this task

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

Steps

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

   By default, the HTTPS protocol is selected.
4. Click **Add**.
5. If HTTPS is selected, perform the following steps:
   a. In the **Authorize Host** dialog box, click **View Certificate** to view the certificate information about the cluster.
   b. Click **Yes**.

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

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

6. Optional: View the cluster discovery status by performing the following steps:
   a. Click the **Data Sources** link from the discovery status message displayed in the **Clusters** .
   b. Review the cluster discovery status from the **Manage Data Sources** page.

Result

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

Related information

NetApp KB Article 1014389: How to renew an SSL certificate in clustered Data ONTAP

Configuring Unified Manager to send alert notifications

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

Before you begin

You must have the OnCommand Administrator role.

About this task

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

Steps

1. *Configure notification settings* on page 30

   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 31

   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 32

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

4. *Edit global threshold settings* on page 33

   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 36

   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 36

   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 OnCommand Administrator or Storage Administrator role.

Steps

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

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

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

Enabling remote authentication

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

Before you begin

You must have the OnCommand Administrator role.

About this task

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

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

Steps

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

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

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

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

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

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

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

Disabling nested groups from remote authentication

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

Before you begin

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

About this task

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

Steps

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

Adding authentication servers

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

Before you begin

- The following information must be available:
  - Host name or IP address of the authentication server
  - Port number of the authentication server

- You must have enabled remote authentication and configured your authentication service so that the management server can authenticate remote users or groups in the authentication server.
- You must have the OnCommand Administrator role.

About this task

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

Steps

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

Result

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

After you finish

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

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 34

  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 34

  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 35

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

Configuring global aggregate threshold values

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

Before you begin

You must have the OnCommand Administrator or Storage Administrator role.

About this task

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

Steps

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

Configuring global volume threshold values

You can configure the global threshold values for all volumes to track any threshold breach. Appropriate events are generated for threshold breaches, and you can take preventive measures based

on these events. You can configure the global values based on the best practice settings for thresholds that apply to all monitored volumes.

Before you begin

You must have the OnCommand Administrator or Storage Administrator role.

About this task

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

Steps

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

Editing unmanaged relationship lag threshold settings

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

Before you begin

You must have the OnCommand Administrator or Storage Administrator role.

About this task

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

Steps

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

Adding a user

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

Before you begin

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

About this task

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

Steps

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

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

Adding an alert

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

Before you begin

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

- You must have the OnCommand Administrator role..

About this task

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

Steps

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

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

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

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

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

- Alert name: Test
- Resources: includes all volumes whose name contains “abc” and excludes all the volumes whose name contains “xyz”

- Events: includes all critical events
- 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 **`abc`** in the **Name contains** field to display the volumes whose name contains abc.
   b. Select <<**All Volumes whose name contains 'abc'**>> from the Available Resources area and move it to the Selected Resources area.
   c. Click **Exclude** and enter **`xyz`** in the **Name contains** field and then click **Add**.
3. Click **Events** and select Critical from the **Event Severity** field.
4. Select **All Critical Events** from the Matching Events area and move it to the Selected Events area.
5. Click **Recipients** and enter **`sample@domain.com`** in the **Alert these users** field.
6. Select **Remind every 15 minutes** to set the frequency to notify the user every 15 minutes.
   You can configure an alert to repeatedly send notification to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.
7. Click **Save**.

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 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**.

Setting up a connection between Performance Manager and Unified Manager

This workflow shows you how to set up your connection between Performance Manager and Unified Manager. This enables you to monitor the performance issues that are detected by the Performance Manager server through the Unified Manager web UI.

Before you begin

- Unified Manager is installed.
- Performance Manager is installed.
- You must have the OnCommand Administrator role in Unified Manager.
- You must have maintenance user log in access to Performance Manager.

About this task

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

Note: A connection configured between a Performance Manager server and a Unified Manager server requires either that both servers be deployed and running as virtual machines on VMware virtual infrastructure or that both servers be installed and running on Red Hat Enterprise Linux. Connections across installation types are not supported.

Steps

1. Create a user with the event publisher role on page 41
   You must first create a user with the event publisher role to begin connecting the Unified Manager server to an OnCommand Performance Manager server.
2. Set up a connection between Performance Manager and Unified Manager on page 41
   You can connect an OnCommand Performance Manager server with the Unified Manager server to display performance issues in the Unified Manager web UI.
3. Delete a connection between Performance Manager and Unified Manager on page 43
   You can delete a connection between an OnCommand Performance Manager server and the Unified Manager server if you no longer want to display performance issues discovered by a specific Performance Manager server in the Unified Manager web UI.

Related information

NetApp Documentation: OnCommand Performance Manager for Clustered Data ONTAP

Creating a user with Event Publisher role privileges

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

Before you begin

You must have the OnCommand Administrator role in Unified Manager.

About this task

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

Steps

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

After you finish

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

Configuring a connection between a Performance Manager server and Unified Manager

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

Before you begin

- You must have created a local user with Event Publisher privileges on the Unified Manager in the connection you want to create.

- You must have an authorized login ID.
  - Performance Manager, if installed as a virtual appliance, requires you have a user ID and password authorized to log in to the maintenance console of the Performance Manager server for which you want to display performance data in the Unified Manager web UI.
- You must be prepared to specify the following information about Unified Manager:
  - Unified Manager server name or IP address
  - Unified Manager server port (must always be 443)
  - Event Publisher user name (the name of the local Unified Manager user assigned Event Publisher privileges)
  - Event Publisher password (the password of the local Unified Manager user assigned Event Publisher privileges)
- Your Unified Manager and Performance Manager installation platforms must match.
  - Unified Manager, if installed as a virtual appliance, can only connect with Performance Manager servers also installed as virtual appliances.
- The clusters that are to be managed by Performance Manager and Unified Manager must be added to both Performance Manager and Unified Manager.

About this task

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

Steps

1. Log in via SSH as the maintenance user to the Performance Manager host to set up the Performance Manager and Unified Manager connection.
   - If Performance Manager is installed as a virtual appliance, log in as the maintenance user to the maintenance console of the Performance Manager server for which you want to create the Unified Manager connection.
2. In the maintenance console, type the number of the menu option labeled “Unified Manager Connection” and then type the number of the menu option labeled “Add/Modify Unified Manager Server Connection.”
3. When prompted, supply the requested Unified Manager server name or IP address and Unified Manager server port information.

   The maintenance console checks the validity of the specified Unified Manager server name or IP address and Unified Manager server port, and, if necessary, prompts you to accept the Unified

Manager server trust certificate to support the connection. The default Unified Manager server port 443 must be used.

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

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

Result

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

Note: Until an initial performance incident is discovered the Unified Manager Dashboard remains unchanged.

Deleting a connection between a Performance Manager server and Unified Manager

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

Before you begin

You must have a user ID authorized to log in to the maintenance console of the Performance Manager server.

Steps

1. Log in as the maintenance user to the maintenance console of the Performance Manager server.
2. In the maintenance console, type the number of the menu option labeled “Unified Manager Connection”.
3. Type the number of the menu option labeled “Delete Unified Manager Server Connection”.
4. When prompted whether you want to delete the connection, type **y** to delete the connection or type **n** to cancel.

Result

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

Setting up a connection between OnCommand Workflow Automation and Unified Manager

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

Before you begin

You must have installed Unified Manager.

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

You must have the OnCommand Administrator or Storage Administrator role.

Steps

1. Create a database user on page 45
   You can create a database user to begin pairing Workflow Automation with Unified Manager.
2. Set up Workflow Automation in Unified Manager on page 46
   You can pair Workflow Automation with Unified Manager to define workflows for your storage classes.

Creating a database user

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

Before you begin

You must have the OnCommand Administrator role.

About this task

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

Steps

1. Click **Administration > Manage Users**.
2. In the **Manage Users** page, click **Add**.

3. In the **Add User** dialog box, select **Database User** in the **Type** drop-down list.
4. Type a name and password for the database user.
5. In the **Role** drop-down list, select the appropriate role.

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

6. Click **Add**.

Setting up a connection between OnCommand Workflow Automation and Unified Manager

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

Before you begin

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

Steps

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

You must use Unified Manager server port 443.

5. Click **Save and Close**.
6. If you use a self-signed certificate, click **Yes** to authorize the security certificate.

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

Related information

NetApp Documentation: OnCommand Workflow Automation (current releases)

Unified Manager 6.2 upgrade overview

You can deploy Unified Manager 6.2 as a virtual instance, but there is no upgrade path from Unified Manager 5.x. You can upgrade, however, from Unified Manager 6.0 to later versions.

Both Unified Manager 5.x and Unified Manager 6.x can monitor clustered Data ONTAP systems concurrently. However, if Unified Manager 5.x and Unified Manager 6.x are both polling the same clusters, the increased overhead might result in slower response times.

Note: Unified Manager 6.2 does not automatically discover alerts that you configured for Unified Manager 5.x. Therefore, when you upgrade Unified Manager 6.2, you must reconfigure all alerts.

If you must transition Data ONTAP FlexVol volumes and configurations operating in 7-Mode environments to hardware that is running clustered Data ONTAP 8.2.0 or 8.2.1, you must use the 7-Mode Transition Tool 2.0.

Related tasks

Removing Unified Manager 6.2 on page 53
Deploying Unified Manager on page 14

Related information

7-Mode Transition Tool 2.0 Data and Configuration Transition Guide

Upgrading to Unified Manager 6.2

This workflow shows you how to upgrade from a previous version of Unified Manager 6.x to Unified Manager 6.2.

Before you begin

The virtual machine on which the virtual appliance resides is backed up by a VMware snapshot, to avoid data loss.

You must be logged in as the maintenance user.

You have the following information:

- Login credentials for the NetApp Support Site
- Credentials for accessing the VMware vCenter server and vSphere Client

About this task

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

Because Unified Manager 6.2 is deployed as a virtual instance, there is no upgrade path from OnCommand Unified Manager 5.x.

Steps

1. Download the Unified Manager 6.2 ISO image on page 49
   Before upgrading to Unified Manager 6.2, you must first download the software.
2. Upgrade to Unified Manager 6.2 on page 50
   You can upgrade to Unified Manager 6.2 from 6.x.

Downloading the Unified Manager 6.2 ISO image

Before upgrading to Unified Manager 6.2, you must download the Unified Manager 6.2 ISO image from the NetApp Support Site.

Before you begin

You must have login credentials for the NetApp Support Site.

About this task

The image file contains the software updates required for upgrading to Unified Manager 6.2.

Steps

1. Download the `OnCommandUnifiedManager-6.2-virtual-update.iso` file from the NetApp Support Site.
2. Save the image file to a local or network directory that is accessible to your vSphere Client.
3. Verify the checksum to ensure that the software downloaded correctly.

Related information

NetApp Support

Upgrading to OnCommand Unified Manager 6.2

To upgrade from a previous version of OnCommand Unified Manager 6.x to OnCommand Unified Manager 6.2, you must first download the `OnCommandUnifiedManager-6.2-virtual-update.iso` file from the NetApp Support Site.

Before you begin

You must have the following information:

- Credentials for accessing the VMware vCenter Server and vSphere Client
- Credentials as the maintenance user

About this task

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

Because OnCommand Unified Manager 6.x is deployed as a virtual instance, there is no upgrade path from OnCommand Unified Manager 5.x.

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, select the VM on which the virtual appliance for OnCommand Unified Manager 6.0 or 6.1 is installed.
2. Shut down Unified Manager.
3. Create a backup copy, such as a snapshot or clone of the Unified Manager VM, to create an application-consistent backup.
4. Power on the Unified Manager VM.

5. Click the **CD/DVD Drive** icon and select **Connect to ISO image on local disk**.
6. Select the `OnCommandUnifiedManager-6.2-virtual-update.iso` file and click **Open**.
7. Click the **Console** tab.
8. Log in to the maintenance console.
9. In the **Main Menu**, select **Upgrade**.

   A message displays that Unified Manager will be unavailable during the upgrade process and will resume after completion.
10. Type **y** to continue.

    A warning appears that reminds 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 number.

Result

You can log in to the web UI to use the upgraded version of Unified Manager.

After the upgrade, you must wait for the discovery process to finish before performing any task in the UI.

Cannot log in to the web UI after upgrading to OnCommand Unified Manager 6.2

Issue

You cannot log in to the UI because of a Java exception in `ocumserver-debug.log`.

Cause

When you use Unified Manager 6.2 and open a browser connection to the Unified Manager server, cookies are created. If you then upgrade from an earlier version of Unified Manager 6.x to Unified Manager 6.2, the server services are restarted and this results in the client session timing out.

Corrective action

1. Delete the browser cookies and browser cache for the existing server connection created after the start of the browser session.

2. Log in to the Unified Manager 6.2 web UI using the same credentials.

Removing Unified Manager 6.2

You can uninstall Unified Manager 6.2 by destroying the virtual appliance on which the Unified Manager software is installed.

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**.

Troubleshooting Unified Manager installation on VMware virtual appliance

During or shortly after installation of Unified Manager on a VMware virtual appliance, you might encounter some issues that require further attention.

Error message displayed when maintenance user is not created during the virtual appliance deployment

If a maintenance user is not created during the VMware virtual appliance deployment, then Unified Manager displays an error message, indicating that at least one user is required to log in to Unified Manager.

Actions

Follow these steps to resolve the issue:

1. Open the VMware virtual appliance console.
2. Follow the prompts to create a maintenance user.
3. Close the VMware virtual appliance console.
4. Close the Unified Manager user interface dialog box.
5. Log in to Unified Manager.

Copyright information

Copyright © 1994–2015 NetApp, Inc. All rights reserved. Printed in the U.S.

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

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

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

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

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

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

Trademark information

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

Cisco and the Cisco logo are trademarks of Cisco in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

How to send comments about documentation and receive update notification

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

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

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

You can also contact us in the following ways:

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

Index

.ova file
    deploying *15*
    downloading *15*

6.2 release of Unified Manager
    introduction to *5*

A

accessing
    Unified Manager web UI *20*
Active Directory
    using to enable remote authentication *31*
adding
    alerts *36*
    authentication servers *32*
    clusters *28*
aggregates
    configuring global threshold values for *34*
alerts
    adding *36*
    configuring your environment for *29*
    creating *36*
alternate configuration
    monitoring capacities *18*
authentication
    adding servers *32*
authentication, remote
    disabling nested groups *32*
    enabling *31*
AutoSupport
    what it does *6*

B

browsers
    supported *10*

C

cannot log in to the web UI after upgrade
    troubleshooting *51*
certificates
    generating HTTPS security certificates *26*
    viewing HTTPS security *26*
Chrome
    browser requirements *10*
client software
    supported versions *10*
clustered Data ONTAP systems
    See clusters
clusters
    adding *28*
    viewing discovery status *28*
comments
    how to send feedback about documentation *57*
configurations
    modifying virtual appliance default *19*
    monitoring capacities *18*
configuring
    aggregate global threshold values *34*
    DNS *25*
    network settings *25*
    notification settings *30*
    thresholds *33*
    Unified Manager *22*
    volume global threshold values *34*
    your environment *23*
connection
    setting up between Performance Manager and Unified Manager *40*
connection setup
    between Unified Manager and Workflow Automation *45*
CPU requirements
    table of *7*
creating
    alerts *36*

D

Data ONTAP
    supported versions *9*
database user roles
    Integration Schema, Report Schema *45*
database users
    creating *36*, *45*
default configuration
    monitoring capacity *18*
default configurations

modifying virtual appliance *19*
deleting
connection between Performance Manager and Unified Manager *43*
deploying
Unified Manager *14*
Unified Manager virtual appliance *15*
deployment
Unified Manager *12*
deployment issues
maintenance user not created *54*
DHCP
enabling *25*
discovery
viewing the status of clusters *28*
DNS
configuring *25*
documentation
how to receive automatic notification of changes to *57*
how to send feedback about *57*

E

editing
network settings *25*
unmanaged relationship lag threshold settings *35*
enabling
DHCP *25*
environment
setup *23*
ESX requirements
virtual appliance *9*
ESXi requirements
virtual appliance *9*

F

feedback
how to send comments about documentation *57*
Firefox
browser requirements *10*

G

groups, nested
disabling remote authentication of *32*

H

hardware
requirements *7*
host names
changing *24*
HTTPS
viewing the security certificate *26*
HTTPS certificates
generating new security certificates *26*

I

information
how to send feedback about improving documentation *57*
infrastructure requirements
table of *7*
installation
configuring initial setup *20*
deploying the virtual appliance *15*
downloading *15*
Unified Manager *12*
installing
accessing the GUI *20*
Unified Manager *14*
Internet Explorer
browser requirements *10*
ISO image
downloading before performing upgrade *49*
issue resolution
what AutoSupport does *6*

L

lag threshold settings
editing for unmanaged relationships *35*
license requirements
VMware vSphere *7*
Linux
supported versions *10*
local users
changing password for *38*
creating *36*

M

machines, virtual
restarting from the maintenance console *27*
Macintosh

supported versions *10*
maintenance console
console, maintenance
restarting the virtual machine from *27*
restarting the virtual machine from *27*
role of maintenance user *5*
maintenance user
not created during deployment *54*
purpose *5*
memory requirements
table of *7*
messages, AutoSupport
how used for troubleshooting *6*
migrating to clustered Data ONTAP
where to go for more information *48*
modifying
unmanaged relationship lag threshold settings *35*

N

nested groups
disabling remote authentication of *32*
network settings
configuring *25*
customizing the host name *24*
editing *25*
notification
adding alerts *36*
configuring settings *30*

O

OnCommand Workflow Automation
setting up a connection with Unified Manager *45*
setting up connection with Unified Manager *46*
Open LDAP
using to enable remote authentication *31*

P

passwords
changing local user *38*
Performance Manager
configuring a connection to a Unified Manager server *41*
deleting a connection to a Unified Manager server *43*
setting up a connection to Unified Manager *40*
performance monitoring
configuring connections between Performance Manager and Unified Manager *41*
deleting connections between Performance Manager and Unified Manager *43*
disabling *43*
enabling *41*
physical storage
adding clusters *28*
platforms
supported *10*
ports
requirements *10*
privileges
creating a user with the Event Publisher role *41*

R

relationships, unmanaged
editing lag thresholds settings for *35*
releases of Unified Manager
introduction to 6.2 *5*
remote authentication
disabling nested groups *32*
enabling *31*
remote groups
adding *36*
remote users
adding *36*
removing
Unified Manager *53*
reports
creating a database user with the Report Schema role *45*
requirements
Data ONTAP, supported versions *9*
deploying *7*
hardware *7*
software *9*
virtual appliance *9*
virtual infrastructure *7*
VMware vSphere license *7*
role, Event Publisher
creating a user having *41*
roles
assigning to users *36*

S

security certificates
generating, HTTPS *26*
viewing HTTPS *26*
servers

required ports *10*
setting up
aggregate global threshold values *34*
notification settings *30*
SMTP server *30*
SNMP *30*
thresholds *33*
volume global threshold values *34*
setting up a connection
between Performance Manager and Unified Manager *40*
settings, lag threshold
editing for unmanaged relationships *35*
setup
post-deployment *23*
setup, connection
between Performance Manager and Unified Manager *40*
software requirements
compliance with *9*
suggestions
how to send feedback about documentation *57*
supported
browser and platform *10*

T

threshold settings, lag
editing for unmanaged relationships *35*
thresholds
configuring *33*
global values for aggregates *34*
global values for volumes *34*
troubleshooting
maintenance user is not created *54*
virtual appliance installation issues *54*
web UI login issue after upgrade *51*
what AutoSupport does *6*
twitter
how to receive automatic notification of documentation changes *57*

U

UI
accessing *20*
Unified Manager
accessing the web UI *20*
configuring *22*
configuring the virtual appliance *20*
deploying *12*, *14*
downloading *15*
downloading the ISO image before upgrading *49*
installing *12*, *14*
introduction to 6.2 *5*
running 6.x concurrently with 5.x *48*
uninstalling 6.2 *53*
upgrading to 6.2 *49*
upgrading to 6.2 from 6.x *50*
uninstalling
Unified Manager *53*
unmanaged relationships
editing lag thresholds settings for *35*
upgrade issues
cannot log in to web UI after, troubleshooting *51*
upgrade process
Unified Manager 6.2 *49*
Unified Manager 6.x to 6.2 *50*
upgrading
downloading the ISO image before *49*
upgrading to 6.2
overview *48*
user roles
assigning *36*
users
adding *36*
changing password for local *38*
creating *36*
creating having the Event Publisher role *41*
maintenance *5*
users, database
creating *45*

V

vApp
system requirements for deploying *7*
See also virtual appliance
viewing
discovery status of clusters *28*
virtual appliance
configuring initial setup *20*
deploying *15*
requirements *9*
system requirements for deploying *7*
what it does *5*
virtual appliance (vApp)
destroying *53*
virtual appliance default configurations
modifying *19*

virtual infrastructure requirements *7*
virtual machines
    restarting from the maintenance console *27*
volumes
    configuring global threshold values for *34*
vSphere requirements
    virtual appliance *9*

W

Windows
    supported versions *10*
Workflow Automation
    creating a database user with the Integration Schema role *45*
    setting up a connection with Unified Manager *45*
    setting up connection with Unified Manager *46*