



OnCommand® Unified Manager 7.0

Installation and Setup Guide

For VMware® Virtual Appliances

July 2016 | 215-11251_A0
doccomments@netapp.com

 **NetApp**®

Contents

Introduction to OnCommand Unified Manager	5
What a virtual appliance does	5
What the maintenance user does	5
What AutoSupport does	5
System requirements for deploying the Unified Manager virtual appliance	6
License requirements for Unified Manager	6
Virtual infrastructure requirements	6
Virtual appliance requirements	7
Software requirements	8
Supported versions of Data ONTAP	8
Supported browsers and platforms	8
Protocol and port requirements	8
Installing Unified Manager	10
Overview of the deployment sequence	10
Deploying Unified Manager	11
Downloading Unified Manager	12
Deploying the Unified Manager virtual appliance	12
Accessing the Unified Manager web UI	16
Performing the initial setup of the Unified Manager web UI	16
Configuring Unified Manager	18
Overview of the configuration sequence	18
Configuring your environment after deployment	19
Changing the Unified Manager host name	19
Adding clusters	22
Adding a cluster to a Performance Manager server	23
Managing storage objects using the Favorites option	24
Moving a cluster from one Performance Manager server to another	25
Configuring Unified Manager to send alert notifications	27
Configuring database backup settings	36
Restoring a database backup on a virtual machine	37
Changing the local user password	38
Integrating Performance Manager with Unified Manager	39
Connecting Performance Manager and Unified Manager	39
Creating a user with Event Publisher role privileges	40
Configuring a full integration connection between a Performance Manager server and Unified Manager	40
Configuring a partial integration connection between a Performance Manager server and Unified Manager	42
Deleting a connection between a Performance Manager server and Unified Manager	43

Setting up a connection between OnCommand Workflow Automation and Unified Manager	44
Creating a database user	44
Configuring a connection between OnCommand Workflow Automation and Unified Manager	45
Upgrading OnCommand Unified Manager	46
Downloading the Unified Manager 7.0 ISO image	46
Upgrading to Unified Manager 7.0 on VMware	47
Cannot log in to the web UI after upgrading OnCommand Unified Manager	48
Upgrading to Unified Manager 7.0 from Unified Manager 6.3 RC1	48
Removing Unified Manager	50
Troubleshooting Unified Manager installation on VMware virtual appliance	51
Error message displayed when maintenance user is not created during the virtual appliance deployment	51
Copyright information	52
Trademark information	53
How to send comments about documentation and receive update notifications	54
Index	55

Introduction to OnCommand Unified Manager

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

Unified Manager provides a graphical interface that displays the capacity, availability, protection, and performance status of the monitored storage systems.

Unified Manager 7.0 supports monitoring of ONTAP 9.0, 8.3.2, 8.3.1, 8.3.0, and 8.2.x systems. Unified Manager 7.0 also supports vaulting, nondisruptive operations, Storage Virtual Machines (SVMs) with Infinite Volumes, reporting, and MetroCluster configurations.

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 Unified Manager virtual appliance

Before you deploy the Unified Manager virtual appliance, you must ensure that your storage system meets all the requirements of the supported platforms. The Unified Manager server must meet specific software, hardware, CPU, and memory requirements.

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

Unified Manager 7.0 requires OnCommand Workflow Automation 3.1 or later to provision Storage Virtual Machines (SVMs) with Infinite Volumes with storage classes, and to configure SnapMirror and SnapVault data protection relationships. Workflow Automation 4.0 is recommended.

Unified Manager 7.0 requires OnCommand Performance Manager 2.1 or later to fully utilize the performance features that are displayed in the Unified Manager web UI. Performance Manager 7.0 is recommended.

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 requirements and CPU resource requirements before you can begin deployment of the Unified Manager virtual appliance.

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

The following table displays the minimum values that are 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.

Hardware configuration	Minimum requirement
Disk space required for thin provisioning	5 GB
Disk space required for thick provisioning If you deploy an NFS datastore on a storage system that is running ONTAP software, you must use the NetApp NFS Plug-in for VMware VAAI to use thick provisioning.	152 GB
Reserved RAM	12 GB
Required processors	4 virtual CPUs
Reserved CPU cycle capacity	9572 MHz

Important: You must ensure that the minimum CPU speed of 9572 MHz is met by the reservation of four CPU cores. Four 2500 MHz cores provide 10000 MHz, whereas four 2250 MHz cores provide only 9000 MHz, which is not enough for the virtual machine (VM) to boot. If four cores are not adequate, you must increase the number of CPU virtual sockets or CPU cores per socket to provide the required CPU cycles that are needed to run Unified Manager.

The following table displays the minimum values that are 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 15.

Alternate hardware configuration	Minimum requirement
Disk space required for thin provisioning	5 GB
Disk space required for thick provisioning If you deploy an NFS datastore on a storage system that is running ONTAP software, you must use the NetApp NFS Plug-in for VMware VAAI to use thick provisioning.	152 GB
Reserved RAM	8 GB
Required processors	2 virtual CPUs
Reserved CPU cycle capacity	4786 MHz

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

If deployment fails using your High Availability-enabled environment because of 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 the VM reservations for CPU and memory is possible, but not below the minimum values that are listed in the table.

Virtual appliance requirements

The VMware ESXi server on which the virtual appliance is deployed must meet minimum resource requirements.

The following versions of VMware ESXi are supported:

- ESXi 5.5 and updates
- ESXi 6.0, 6.0 U1, and 6.0 U2

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

mysupport.netapp.com/matrix

The following versions of vSphere are supported:

- VMware vCenter Server 5.5 and updates

- VMware vCenter Server 6.0, 6.0 U1, and 6.0 U2

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

Software requirements

Before you use Unified Manager, you must ensure that you meet the software requirements.

Supported versions of Data ONTAP

Unified Manager 7.0 supports ONTAP 9.0, 8.3.2, 8.3.1, 8.3.0, and 8.2.x.

Supported browsers and platforms

To use the Unified Manager UI, 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 for the complete list of supported browser versions. mysupport.netapp.com/matrix

Supported browsers

- Microsoft Internet Explorer 11
- Google Chrome version 50 and 51
- Mozilla Firefox ESR 38 and 45

For IE, you must ensure that Compatibility View is disabled, and Document Mode is set to the default. See the Microsoft IE documentation for information about these settings.

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

Supported browser client platforms

- Windows 7, Windows 8, and Windows 10
- Red Hat Enterprise Linux 6.6, 6.7, 6.8, 7.0, 7.1, and 7.2 (64-bit)
- SUSE Linux Enterprise Server 11 SP2

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.
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 access to Unified Manager.
Syslog	UDP	514	Used to listen to and access EMS messages from ONTAP clusters and to create events based on the messages.
Unified Manager web UI and Reverse Proxy	TCP/IP	20443	Used by Unified Manager to listen to the reverse proxy.
Unified Manager web UI and Reverse Proxy	TCP/IP	8443	Used by the reverse proxy to listen to the port.

Connections from the Unified Manager server

You must configure your firewall to open 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.

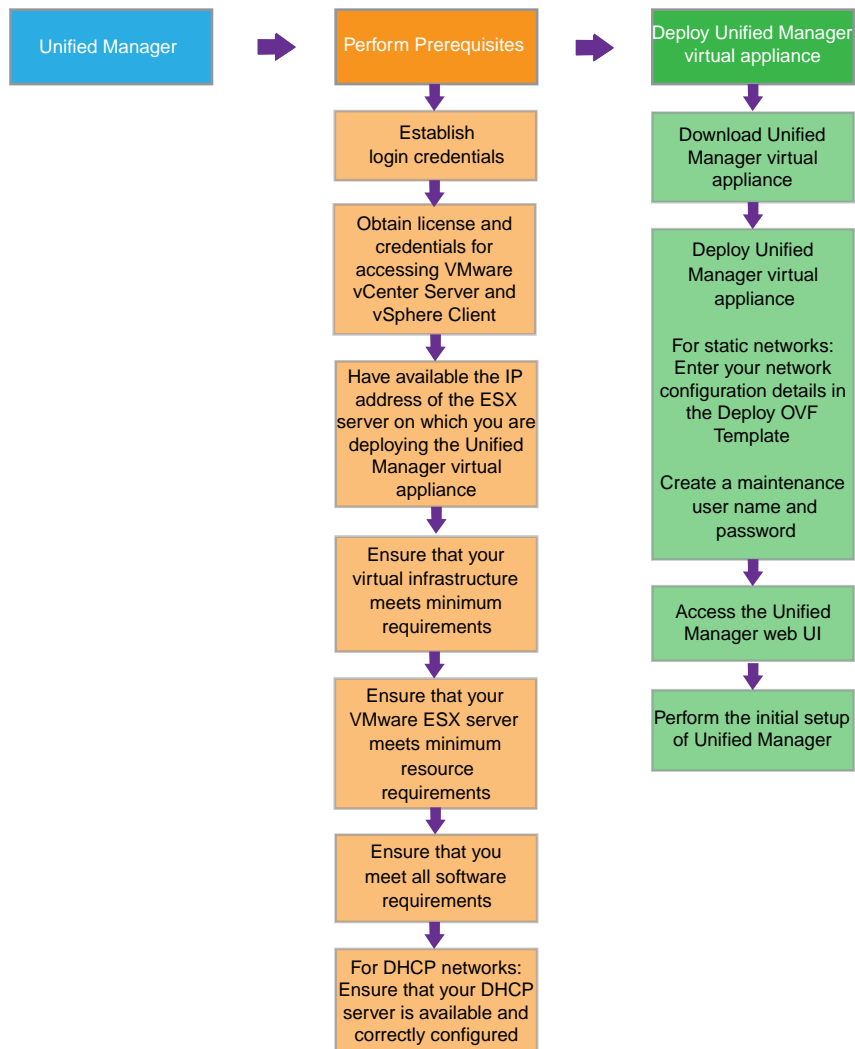
The Unified Manager server connects using the following protocols and ports to the managed storage systems, servers, and other components:

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.
	LDAPS	636	Used for secure communication.
Mail server	SMTP	25	Used to send alert notification emails.
SNMP trap sender	SNMPv1 or SNMPv3	162/UDP	Used to send alert notification SNMP traps.
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 11

Deploying Unified Manager

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

Before you begin

- You must have completed the system requirements for deployment. [System requirements](#) on page 6
- You must have the following information:
 - Login credentials for the NetApp Support Site
 - Credentials for accessing the VMware vCenter Server and vSphere Client
 - IP address of the ESXi server on which you are deploying the Unified Manager virtual appliance
 - Details about the data center, such as storage space in the datastore and memory requirements
 - IPv6 must be enabled on the host if you are planning to use IPv6 addressing.
 - CD-ROM or ISO image of VMware Tools

About this task

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

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

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

After you finish

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

Steps

1. [Download Unified Manager](#) on page 12
You must download Unified Manager before you can deploy the virtual appliance.
2. [Deploy the Unified Manager virtual appliance](#) on page 12
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 16
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 16
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 Unified Manager virtual appliance](#) on page 6

Downloading Unified Manager

You must download the `OnCommandUnifiedManager-7.0.ova` file from the NetApp Support Site to deploy Unified Manager as a virtual appliance.

Before you begin

You must have login credentials for the NetApp Support Site.

About this task

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

Steps

1. Log in to the NetApp Support Site, and navigate to the Unified Manager Software Download page.
2. Download the `OnCommandUnifiedManager-7.0.ova` file.
3. Save the `.ova` file to a local directory or network directory that is accessible to your vSphere Client.
4. Verify the checksum to ensure that the software downloaded correctly.

Deploying the Unified Manager virtual appliance

You can deploy the Unified Manager virtual appliance after you download the `OnCommandUnifiedManager-7.0.ova` file from the NetApp Support Site. You must use the VMware vSphere Client to deploy the virtual appliance on an ESXi server. When you deploy the virtual appliance, a virtual machine is created.

Before you begin

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

[System requirements](#) on page 6

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

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

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

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

- Search domains
- CD-ROM or ISO image for the VMware Tools

About this task

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

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

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

You can change the default configuration of the virtual appliance after it has been deployed.

[Modifying the default configuration to the alternate configuration](#) on page 15

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 fields in the Properties tab in the Deploy OVF Template, and these 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.

[Virtual infrastructure requirements](#) on page 6
3. After the Unified Manager virtual appliance is deployed to the ESXi server, power on the VM by right-clicking the VM, and then selecting **Power On**.

If the Power On operation fails because of insufficient resources, you must modify the resource settings for memory and CPU resources. The resources must be reserved.
4. Click the **Console** tab.

The initial boot process takes a few minutes to complete. If a reset occurs during the initial boot process, the virtual appliance must be redeployed.
5. Follow the prompt to install the VMware Tools on the VM.
6. To configure your time zone, enter your geographic area and your city or region as prompted in the VM **Console** window.

All the date information that is displayed uses the time zone that is configured for Unified Manager, regardless of the time zone setting on your managed devices. You should be aware of this when comparing time stamps. If your storage systems and the management server are configured with the same NTP server, they refer to the same instant in time, even if they appear differently. For example, if you create a Snapshot copy using a device that is configured using a different time zone than that of the management server, the time reflected in the time stamp is the management server time.
7. If no DHCP services are available, or if there is an error in the details for the static network configuration, select one of the following options:

If you use...	Then do this...
DHCP	<p>Select Retry DHCP.</p> <p>If you plan to use DHCP, you should ensure that it is configured correctly.</p> <p>If you use a DHCP-enabled network, the FQDN and DNS server entries are given to the virtual appliance automatically. If DHCP is not properly configured with DNS, the host name “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.</p>
A static network configuration	<p>a. Select Enter the details for static network configuration. The configuration process takes a few minutes to complete.</p> <p>b. Confirm the values that you entered, and select Y.</p>

8. At the prompt, enter a maintenance user name, and click **Enter**.
The maintenance user name must start with a letter from a-z, followed by any combination of -, a-z, or 0-9.
9. At the prompt, enter a password, and click **Enter**.
The VM console displays the URL for the Unified Manager web UI.

After you finish

You can 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 6. 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.

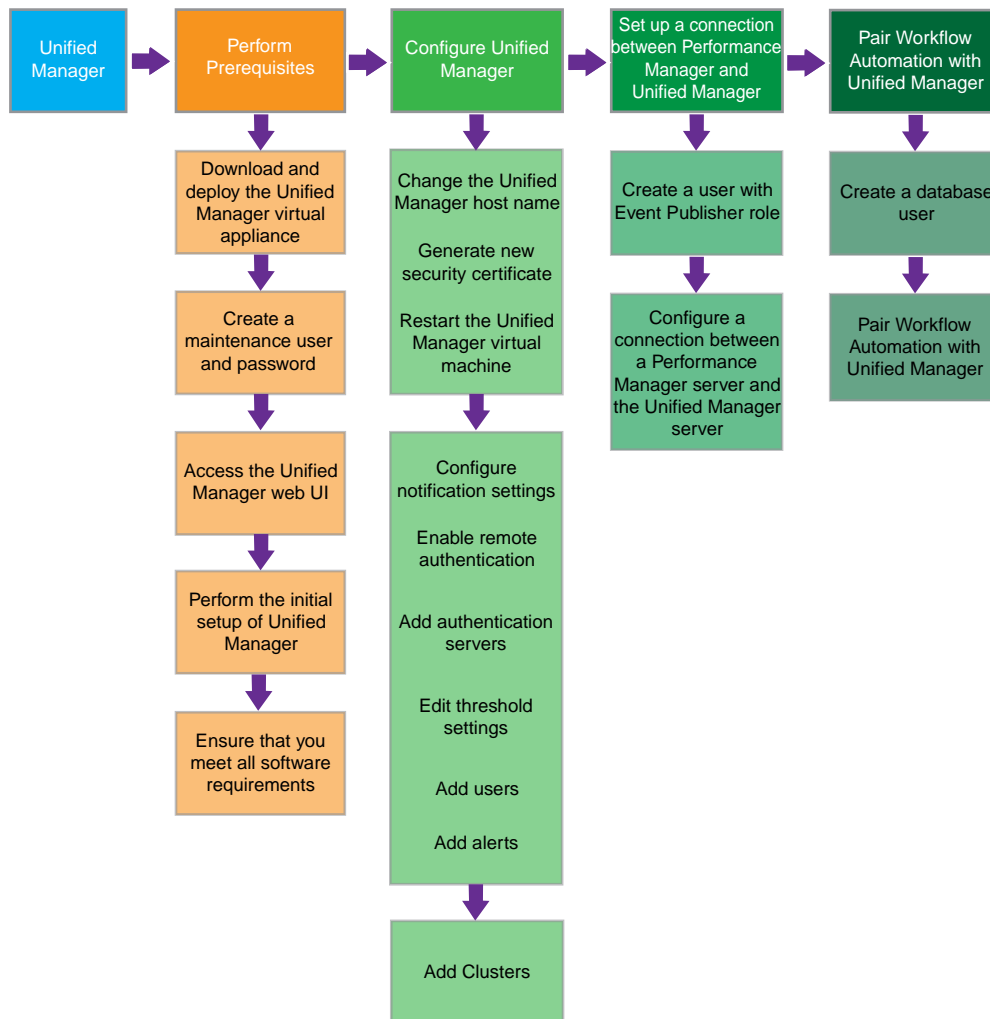
After you finish

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 19.

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 19

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 after the initial setup, you must add clusters 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 before or after adding clusters.

Choices

- [Changing the Unified Manager host name](#) on page 19

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 clusters are added to Unified Manager, you can monitor them, but you cannot receive notifications about events in your cluster environment until you configure several options (for example, the email address from which notifications are sent, and the users who should receive the alerts). You might also want to modify the default threshold settings at which events are generated.

Related concepts

[Installing Unified Manager](#) on page 10

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 logged 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 Unified Manager web UI. If you configured a static IP address for your network during deployment, then you would have designated a name for the network host. If you configured the network using DHCP, the host name should be taken from the DNS. 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 OnCommand Workflow Automation (WFA). The host name is not updated automatically in WFA.

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

Steps

1. [Generate an HTTPS security certificate](#) on page 20

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.

2. [View the HTTPS security certificate](#) on page 21

You must verify that the correct information is displayed after generating a new security certificate.

3. [Restart the Unified Manager virtual machine](#) on page 21

After you regenerate the HTTPS certificate, you must restart the Unified Manager virtual machine.

Generating an HTTPS security certificate

You might generate a new HTTPS security certificate for multiple reasons, including when you want to sign with a different Certificate Authority or when 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 to the Unified Manager web UI. You must reactivate those connections after completing this task.

Steps

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

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

Restarting the Unified Manager virtual machine

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

Before you begin

- The virtual appliance must be powered on.
- You must be logged in to the 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. In the maintenance console, select **System Configuration** > **Reboot Virtual Machine**.
2. Start the Unified Manager graphical user interface (GUI) from your browser, and log in.

Related information

VMware vSphere PowerCLI Cmdlets Reference: Restart-VMGuest

Adding clusters

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


Before you begin

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

About this task

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

Steps

1. Click  > **Dashboard**.
2. From the **Managed Clusters** page, click **Add Cluster**.
3. In the **Add Cluster** page, specify the required values, such as the host name or IP address (IPv4 or IPv6) of the cluster, user name, password, protocol for communication, and port number.
By default, the HTTPS protocol is selected.
You can change the cluster-management IP address from IPv6 to IPv4 or from IPv4 to IPv6. The new IP address is reflected in the cluster grid and the cluster configuration page after the next monitoring cycle is complete.
4. In the **Link Performance Manager** section, select the name of the Performance Manager instance to which you want the cluster to be assigned.
You can associate an instance of Performance Manager either while adding a cluster or while modifying the cluster configuration.
5. Click **Save**.
6. If HTTPS is selected, perform the following steps:
 - a. In the **Authorize Host** dialog box, click **View Certificate** to view the certificate information about the cluster.

- b. Click **Yes**.

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

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

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

Adding a cluster to a Performance Manager server

You add a cluster to a Performance Manager server so that you can monitor cluster performance. You can add the cluster to Performance Manager at the same time as you add it to Unified Manager using the Add Cluster page, or you can add the cluster to Performance Manager later, using the Edit Cluster page.

Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- The Performance Manager server where you want to add the cluster must be installed with Performance Manager version 2.1 software, or later, and running.
- During the installation of Performance Manager software, you specified that you would connect the Performance Manager server with a specific Unified Manager server, and you are currently logged in to this Unified Manager server.
- The user name and password used to access the cluster must have the *admin* role with Application access set to *ontapi*, *ssh*, and *http*.


About this task

A cluster should be managed by only one instance of Performance Manager.

The process of adding a cluster to Performance Manager varies depending on whether you are adding the first cluster to the Performance Manager server or clusters already exist on that server. When adding the first cluster, you must perform Performance Manager initialization tasks. Both procedures are described in the following steps.

A single instance of Performance Manager supports a specific number of clusters and storage objects. If Performance Manager is monitoring an environment that exceeds the supported configuration, it might have difficulty collecting and analyzing configuration and performance data from the clusters. See the *OnCommand Performance Manager Release Notes* for the number of clusters, nodes, and volumes that Performance Manager can reliably support.

Steps

1. Use a web browser to log in to the Unified Manager web UI, using the IP address or URL and an appropriate user name and password.
2. From the **Managed Clusters** list, select the cluster you want to add, and then click  > **Edit**.
The Edit Cluster page is displayed in the right pane.
3. From the **Link Performance Manager** section, select the Performance Manager server that will monitor the cluster.
4. Click **Save**.

Note: If you receive an error message that the cluster add operation failed because of an HTTPS certificate error, ensure that you rebooted the Performance Manager server after pairing Performance Manager with Unified Manager.

5. If you selected the HTTPS protocol, perform the following steps:
 - a. In the **Authorize Host** dialog box, click **View Certificate** to view the certificate information of the cluster.
 - b. Click **Yes** to authorize Performance Manager to communicate with the cluster.

The result depends on whether the Performance Manager server is initialized:

- If the server is already initialized, the cluster is added to the server. After the initial cluster inventory and data collection has completed, which might take up to 30 minutes, performance statistics are displayed in the UI.
 - If the server is not initialized, a new browser window is displayed.
6. Follow the instructions in the new browser window to set up email and AutoSupport:
 - a. Specify an initial email recipient to which email alerts will be sent, and the SMTP server that will handle email communications.
 - b. Specify whether AutoSupport is enabled to send information about your Performance Manager installation to technical support.
 7. Click **Save and Complete Initialization**.
 8. Return to the **Edit Cluster** page in the original browser window.
 9. Click **Save**.

Result

After all of the objects are discovered, Performance Manager gathers historical performance data for the previous 24 hours. This enables you to view a full day of historical performance information for a cluster immediately after it is added. After the historical data is collected, real-time cluster performance data is collected, by default, every five minutes.

Managing storage objects using the Favorites option

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

Tasks you can perform from the Favorites dashboard

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

Viewing the Favorites list

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

Adding storage objects to the Favorites list

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

Removing storage objects from the Favorites list

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

Adding storage objects to Favorites list

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

About this task

You can add up to 20 clusters, aggregates, or volumes to the Favorites list.

Steps

1. Go to the **Details** page of the storage object that you want to mark as a favorite.
2. Click the star icon to add the storage object to the Favorites list.

Adding a cluster to the Favorites list

1. Click Clusters.
2. From the Clusters page, click the cluster that you want to add to the Favorites list.
3. On the Cluster details page, click the star icon.

Moving a cluster from one Performance Manager server to another

The number of clusters that a single instance of Performance Manager can support depends on the number on the number of nodes, volumes, and other storage objects within each cluster. When too many clusters and storage objects are being monitored by a single instance of Performance Manager, you might need to move some clusters to a different instance of Performance Manager.

Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- The Performance Manager server where you want to add the cluster is installed with Performance Manager version 2.1 software, or later, and it is running.
- During the installation of Performance Manager software, you specified that you would connect the Performance Manager server with a specific Unified Manager server, and you are currently logged in to this Unified Manager server.


About this task

Moving a cluster consists of removing the cluster from one instance of Performance Manager and adding the cluster to another instance of Performance Manager.

Attention: This task is disruptive, because all cluster performance data, including historical data, storage services, and all associated events, is deleted from the original Performance Manager server.

The process of adding a cluster to the new Performance Manager server varies depending on whether you are adding the first cluster to the Performance Manager server or if one cluster has already been added to the server. When adding the first cluster, you must perform Performance Manager initialization tasks.

Steps

1. From the **Managed Clusters** list, select the cluster you want to move and click  > **Edit**.
The Edit Cluster page displays in the right pane.
 2. From the **Link Performance Manager** section, select the option **None** from the **Select Application Instance** list.
 3. Click **Save**.
 4. Click **Yes** in response to the warning message that all performance data for this cluster will be lost after removing the cluster.
 5. From the **Link Performance Manager** section, select the new Performance Manager server that will monitor the cluster.
 6. Click **Save**.
 7. If you have selected the HTTPS protocol, perform the following steps:
 - a. In the **Authorize Host** dialog box, click **View Certificate**.
 - b. Click **Yes** to authorize Performance Manager to communicate with the cluster.
- Depending on whether the Performance Manager server is initialized, the following actions occur:
- If the server is already initialized, the cluster is added to the server.
After the initial cluster inventory and data collection is complete, which might take up to 30 minutes, performance statistics display in the UI.
 - If the server is not initialized, a new browser window displays.
8. Follow the instructions in the new browser window to set up email and AutoSupport:
 - a. Specify an initial email recipient to which email alerts will be sent, and the SMTP server that will perform email communications.
 - b. Specify whether AutoSupport is enabled to send information about your Performance Manager installation to technical support.
 9. Click **Save and Complete Initialization**.
 10. Return to the **Edit Cluster** page in the original browser window.
 11. Click **Save**.

The cluster is added to the server. After the initial cluster inventory and data collection is complete, performance statistics display in the UI.

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 27
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 28
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 30
If you enable remote authentication, then you must identify authentication servers.
4. [Edit global threshold settings](#) on page 32
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 34
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 34
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  > **Health**.
2. Click **Administration** > **Setup Options**.
3. In the **Setup Options** dialog box, click **General Settings** > **Notification**.
4. 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 (IPv4 or IPv6) of the SMTP server instead of the host name.

Enabling remote authentication

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

Before you begin


You must have the OnCommand Administrator role.

About this task

If remote authentication is disabled, remote users cannot access Unified Manager.

Remote authentication is supported over LDAP and LDAPS (Secure LDAP). Unified Manager uses 389 as the default port for non-secure communication, and 636 as the default port for secure communication.

Steps

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

For Authentication type...	Enter the following information...
Active Directory	<ul style="list-style-type: none"> • Authentication server administrator name in one of following formats: <ul style="list-style-type: none"> ◦ <i>domainname\username</i> ◦ <i>username@domainname</i> ◦ <i>Bind Distinguished Name</i> (using the appropriate LDAP notation) • Administrator password • Base distinguished name (using the appropriate LDAP notation)
Open LDAP	<ul style="list-style-type: none"> • Bind distinguished name (in the appropriate LDAP notation) • Bind password • Base distinguished name

If the 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.

If you select the Use Secure Connection option for the authentication server, then Unified Manager communicates with the authentication server using the Secure Sockets Layer (SSL) protocol.

7. Optional: Add authentication servers, and test the authentication.
8. 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 can 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. Select **Enable Remote Authentication**.
4. In the **Authentication Service** field, select **Others**.
5. In the **Member** field, change the member information from “member:1.2.840.113556.1.4.1941:” to “member”.

6. 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 (HA) 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  > **Health**.
2. Click **Administration > Setup Options**.
3. In the **Setup Options** dialog box, click **Management Server > Authentication**.
4. Enable or disable the **Use secure connection authentication** option:

If you want to...	Then do this...
Enable it	<ol style="list-style-type: none"> a. In Enable Remote Authentication area, select the Use Secure Connection option. b. In the Servers area, click Add. c. In the Add Authentication Server dialog box, enter the authentication name or IP address (IPv4 or IPv6) of the server. d. In the Authorize Host dialog box, click View Certificate. e. In the View Certificate dialog box, verify the certificate information, and then click Close. f. In the Authorize Host dialog box, click Yes. <p>Note: When you enable the Use Secure Connection authentication option, Unified Manager communicates with the authentication server and displays the certificate. Unified Manager uses 636 as default port for secure communication and port number 389 for non-secure communication.</p>

If you want to...	Then do this...
Disable it	<ol style="list-style-type: none"> a. In the Enable Remote Authentication area, clear the Use Secure Connection option. b. In the Servers area, click Add. c. In the Add Authentication Server dialog box, specify either the host name or IP address (IPv4 or IPv6) of the server, and the port details. d. Click Add.

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

5. Perform a test authentication to confirm that you can authenticate users in the authentication server that you added.

Testing the configuration of authentication servers

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


Before you begin

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

About this task

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

Steps

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

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

Editing global threshold settings

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

About this task

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

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

Choices

- [Configuring global aggregate threshold values](#) on page 32
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 33
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 33
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  > **Health**.
2. Click **Administration** > **Setup Options**.
3. In the **Setup Options** dialog box, click **Thresholds** > **Aggregates**.
4. Configure the appropriate threshold values for capacity, growth, and Snapshot copies.

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

Editing lag threshold settings for unmanaged protection relationships

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 task are applied globally to all unmanaged protection relationships. The settings cannot be specified and applied exclusively to one unmanaged protection relationship.

Steps

1. Click  > **Health**.
2. Click **Administration** > **Setup Options**.
3. In the **Setup Options** dialog box, click **Thresholds** > **Relationships**.
4. In the **Lag** area of the **Lag Thresholds for Unmanaged Relationships** dialog box, increase or decrease the global default lag warning or error lag time percentage as required.
5. 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 that belong to an authentication server. You can assign roles to these users and, based on the privileges of the roles, users can manage the storage objects and data with Unified Manager, or view the 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 the direct members of that group can authenticate to Unified Manager.

Steps

1. Click  > **Health**.
2. Click **Administration** > **Manage Users**.
3. On the **Manage Users** page, click **Add**.
4. 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 that is unique to that user. You must avoid specifying email addresses that are shared by multiple users.

5. 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. You can specify the frequency with which you want to be notified and associate a script to the alert.


Before you begin

- You must have configured notification settings such as the user 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 the user names or email addresses of the users that you want to notify.
- You must have added scripts to Unified Manager by using the Manage Scripts page.
- You must have the OnCommand Administrator or Storage Administrator role.

About this task

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

Steps

1. Click  > **Health**.
2. Click **Administration > Manage Alerts**.
3. In the **Manage Alerts** page, click **Add**.
4. 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 in 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 that you specify, the list of available resources displays only those resources that match the filter rule. The text string that you specify is case-sensitive.

If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule, and the alert is not generated for events related to the excluded resource.
 - c. Click **Events**, and select the events based on the event name or event severity type for which you want to trigger an alert.
 - d. Click **Actions**, and select the users that you want to notify, choose the notification frequency, and assign a script to be executed when an alert is generated.

Note: If you modify the email address that is specified for the user and reopen the alert for editing, the Name field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you 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.
5. 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 volumes whose name contains “xyz”
- Events: includes all critical events
- Actions: includes “sample@domain.com”, a “Test” script, and the user has to be notified every 15 minutes

Perform the following steps in the Add Alert dialog box:

1. Click **Name**, and enter **Test** in the **Alert Name** field.
2. Click **Resources**, and in the Include tab, select **Volumes** from the drop-down list.
 - a. Enter **abc** in the **Name contains** field to display the volumes whose name contains “abc”.
 - b. Select <<**All Volumes whose name contains 'abc'**>> from the Available Resources area, and move it to the Selected Resources area.

- c. Click **Exclude**, and enter **xyz** in the **Name contains** field, and then click **Add**.
- 3. Click **Events**, and select **Critical** from the Event Severity field.
- 4. Select **All Critical Events** from the Matching Events area, and move it to the Selected Events area.
- 5. Click **Actions**, and enter **sample@domain.com** in the Alert these users field.
- 6. Select **Remind every 15 minutes** to notify the user every 15 minutes.
You can configure an alert to repeatedly send notifications to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.
- 7. In the Select Script to Execute menu, select **Test** script .
- 8. Click **Save**.


Configuring database backup settings

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

Before you begin

- You must have the Operator, OnCommand Administrator, or Storage Administrator role.

Steps

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

Daily

If you select this option, you must enter a time in 24-hour format for creating the backup. For example, if you specify 18:30, then a backup is created daily at 6:30 PM.

Weekly

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

7. Click **Save and Close**.

Restoring a database backup on a virtual machine

In case of data loss or data corruption, you can use the restore feature to restore Unified Manager to the previous stable state with minimal loss. You can restore the Unified Manager database on a virtual machine by using the Unified Manager maintenance console.

Before you begin

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

About this task

Backup compatibility is platform and version dependent. You can restore a backup from a virtual appliance to another virtual appliance, and from a virtual appliance to a Red Hat Enterprise Linux system.

Steps

1. In the vSphere client, locate the Unified Manager virtual machine, and then select the **Console** tab.
2. Click in the console window, and then log in to the maintenance console using your user name and password.
3. In the **Main Menu**, enter the number for the **System Configuration** option.
4. In the **System Configuration Menu**, enter the number for the **Restore Database from bundle** option.
5. When prompted, enter the absolute path of the backup file.

Example

```
Bundle to restore from: opt/netapp/data/ocum-backup/
UM_6.4.N151112.0947_backup_unix_11-22-2015-11-41.7z
```

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

After you finish

After you restore the backup, if the OnCommand Workflow Automation server does not work, perform the following steps:

1. On the Workflow Automation server, change the IP address of the Unified Manager server to point to the latest machine.
2. On the Unified Manager server, reset the database password if the acquisition fails in step 1.

Note: When OnCommand Performance Manager is paired with a Unified Manager server, and you restore the backup to a different system, you must update Performance Manager with the new IP address for the Unified Manager server.

Changing the local user password

You can change your login password to prevent potential security risks. If you have configured Unified Manager in a VCS environment, then you must change the password for both cluster nodes. Both cluster nodes must have same password.

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. You must use the Unified Manager maintenance console to change the maintenance user password. To change the remote user password, you must 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**.

Integrating Performance Manager with Unified Manager

A connection between a Performance Manager server and a Unified Manager server enables you to use the Unified Manager web UI to monitor the performance issues that are detected by Performance Manager.

You configure the connection between a Performance Manager server and a Unified Manager server through the menu option labeled “Unified Manager Integration” in the Performance Manager maintenance console.

Connecting Performance Manager and Unified Manager

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

Before you begin

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

About this task

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

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

Integration of the two products does not require that they are installed on the same host operating system. Any combination of host operating systems is allowed. For example, Performance Manager installed on Red Hat Enterprise Linux can be integrated with Unified Manager installed on Windows.

Steps

1. [Create a user with the event publisher role](#) on page 40
You must create a user with the event publisher role before connecting the Unified Manager server to a Performance Manager server.
2. [Set up a full integration connection between Performance Manager and Unified Manager](#) on page 40
You can connect a Performance Manager server with the Unified Manager server to send performance events to Unified Manager and to integrate the products under a common URL.
3. [Set up a partial integration connection between Performance Manager and Unified Manager](#) on page 42
You can connect a Performance Manager server with the Unified Manager server to send performance events to Unified Manager.

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, 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 event notification is posted in the Unified Manager web UI.

Steps

1. Log in to Unified Manager and navigate to the **Health** dashboard.
2. Click **Administration > Manage Users**.
3. In the **Manage Users** page, click **Add**.
4. In the **Add User** dialog box, select **Local User** for `type` and **Event Publisher** for `role`, and then enter the other required information.
5. Click **Add**.

After you finish

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

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

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

Before you begin

- You intend to configure a full integration connection.
- The Unified Manager server must be installed with version 6.4 or later software.
- The versions of Unified Manager and Performance Manager must be compatible. The Interoperability Matrix contains the list of compatible versions.
mysupport.netapp.com/matrix
- You must have a user ID authorized to log in to the maintenance console of the Performance Manager server.
- You must be prepared to specify the following information about the Unified Manager server:
 - Unified Manager server name or IP address
If using an FQDN, the last part cannot be a single letter; for example, `vm.company.a` is invalid.

- Unified Manager Administrator user name and password
- Unified Manager Event Publisher user name and password

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

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

About this task

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

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

Steps

1. Log in using SSH as the maintenance user to the Performance Manager host to access the maintenance console.
 - If Performance Manager is installed as a virtual appliance, log in as the maintenance user on the Performance Manager server.

The Performance Manager maintenance console prompts are displayed.
2. Type the number of the menu option labeled **Unified Manager Integration**.
3. If prompted, enter the maintenance user password again.
4. Select **Full Integration > Enable Full Integration**.
5. When prompted, supply the Unified Manager server name or IP address (IPv4 or IPv6).

The maintenance console checks the validity of the specified Unified Manager server name or IP address (IPv4 or IPv6) and Unified Manager server port and, if necessary, prompts you to accept the Unified Manager server trust certificate to support the connection.
6. When prompted, supply the Administrator user name and password.
7. When prompted, supply the Event Publisher user name and password.
8. When prompted, supply the unique name for this instance of Performance Manager.

This name enables you to easily identify the Performance Manager server you want to manage when there are many instances integrated with Unified Manager.
9. Type **y** to confirm that the connection settings are correct, or type **n** if the settings are incorrect and you want to discard your changes.
10. If Performance Manager is installed as a virtual appliance, the virtual machine restarts automatically.

Result

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

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

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

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

Before you begin

- You intend to configure a partial integration connection.
- The version of Unified Manager must be compatible with the version of Performance Manager. See the Interoperability Matrix for the list of compatible versions. mysupport.netapp.com/matrix
- You must have created a local user with Event Publisher privileges on Unified Manager server.
- You must have a user ID that is authorized to log in to the maintenance console of the Performance Manager server.
- You must have the following information:
 - Unified Manager server name or IP address
 - Unified Manager server port number (must be 443)
 - Event Publisher user name
 - Event Publisher password

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

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

About this task

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

Steps

1. Log in using SSH as the maintenance user to the Performance Manager host.
 - If Performance Manager is installed as a virtual appliance, log in as the maintenance user to the maintenance console of the Performance Manager server.

The Performance Manager maintenance console prompts are displayed.
2. Type the number of the menu option that is labeled **Unified Manager Integration**.
3. If prompted, enter the maintenance user password again.
4. Select **Partial Integration > Add Unified Manager Server Connection**.
5. When prompted, enter the Unified Manager server name or IP address (IPv4 or IPv6) and the Unified Manager server port information.

The maintenance console checks the validity of the specified Unified Manager server name or IP address (IPv4 or IPv6), and the 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.

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

Result

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

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

Deleting a connection between a Performance Manager server and Unified Manager

If you no longer want to display performance issues that are discovered by a specific Performance Manager server in the Unified Manager web UI, you can delete the connection between that server and Unified Manager.

Before you begin

You must have credentials to log in to the maintenance console of the Performance Manager server.

About this task

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

If you are planning to delete a Performance Manager instance that has an existing connection to Unified Manager, you must delete the connection before deleting the instance.

Steps

1. Log in as the maintenance user to the maintenance console of the Performance Manager server.
The Performance Manager maintenance console prompts are displayed.
2. In the maintenance console, type the number of the menu option that is labeled **Unified Manager Integration**.
3. If prompted, enter the maintenance user password again.
4. Select **Partial Integration > Delete Unified Manager Server Connection**.
5. When prompted whether you want to delete the connection, type **y** to delete the connection.

Result

Performance events that are 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 configure protection features such as SnapMirror and SnapVault, and to issue commands for managing SnapMirror relationships.

Before you begin

- You must have installed Unified Manager.
- You must have installed OnCommand Workflow Automation version 3.1 or later.
- You must have the OnCommand Administrator or Storage Administrator role.

Steps

1. [Create a database user](#) on page 44
You can create a database user to begin pairing Workflow Automation with Unified Manager.
2. [Set up Workflow Automation in Unified Manager](#) on page 45
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**.


Configuring a connection between OnCommand Workflow Automation and Unified Manager

You can configure a secure connection between Workflow Automation (WFA) and Unified Manager. Connecting to Workflow Automation enables you to use protection features such as SnapMirror and SnapVault configuration workflows, as well as commands for managing SnapMirror relationships.

Before you begin

- You must have the name of the database user that you created in Unified Manager to support WFA 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 Workflow Automation setup.
- You must have the OnCommand Administrator or Storage Administrator role.

Steps

1. Click  > **Health**.
2. Click **Administration** > **Setup Options**.
3. In the **Setup Options** dialog box, click **Add-ons** > **Workflow Automation**.
4. 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 Workflow Automation connections.
5. In the **Workflow Automation Credentials** area of the **Set Up OnCommand Workflow Automation** dialog box, type the host name or IP address (IPv4 or IPv6), and the user name and password for the Workflow Automation setup.
You must use the Unified Manager server port (port 443).
6. Click **Save and Close**.
7. If you use a self-signed certificate, click **Yes** to authorize the security certificate.
The Workflow Automation Options Changed dialog box displays.
8. Click **Yes** to reload the web UI, and add the Workflow Automation features.

Related information

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

Upgrading OnCommand Unified Manager

You should consult the upgrade workflow to learn how to upgrade from a previous version of Unified Manager to Unified Manager 7.0.

About this task

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

If Unified Manager is paired with an instance of OnCommand Workflow Automation, and there are new versions of software available for both products, you should upgrade Workflow Automation prior to upgrading Unified Manager. If you have already upgraded Unified Manager prior to upgrading Workflow Automation, you must disconnect the two products, and then set up a new Workflow Automation connection.

Similarly, if Unified Manager is paired with an instance of Performance Manager, and there are new versions of software available for both products, you should upgrade Unified Manager prior to upgrading Performance Manager.

Note: There is no upgrade path from Unified Manager 5.x to Unified Manager 7.0. Both Unified Manager 5.x and Unified Manager 7.x can monitor storage systems that are running ONTAP software concurrently. However, if both Unified Manager 5.x and Unified Manager 7.x are polling the same clusters, the increased overhead might result in slower response times.

Steps

1. [Download the Unified Manager ISO image](#) on page 46
Before upgrading to Unified Manager, you must first download the software.
2. [Upgrade Unified Manager](#) on page 47
You can upgrade to Unified Manager 7.0 from 6.x.
3. [Upgrading to Unified Manager 7.0 from Unified Manager 6.3 RC1](#) on page 48
When you are upgrading from Unified Manager 6.3 RC1 to Unified Manager 7.0, you must follow special instructions.

Related tasks

[Setting up a connection between OnCommand Workflow Automation and Unified Manager](#) on page 44

[Connecting Performance Manager and Unified Manager](#) on page 39

[Removing Unified Manager](#) on page 50

[Deploying Unified Manager](#) on page 11

Downloading the Unified Manager 7.0 ISO image

Before upgrading to Unified Manager 7.0, you must download the Unified Manager 7.0 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 that are required for upgrading to Unified Manager 7.0.

Steps

1. Log in to the NetApp Support Site, and navigate to the Software Download page.
2. Download the `OnCommandUnifiedManager-7.0-virtual-update.iso` file.
3. Save the image file to a local directory or network directory that is accessible to your vSphere Client.
4. Verify the checksum to ensure that the software downloaded correctly.

Related information

[NetApp Support](#)

Upgrading to Unified Manager 7.0 on VMware

You can upgrade from Unified Manager 6.3 or 6.4 to Unified Manager 7.0.

Before you begin

You must have downloaded the `OnCommandUnifiedManager-7.0-virtual-update.iso` file from the NetApp Support Site.

You must have the following information:

- Login credentials for the NetApp Support Site
-
- Credentials for accessing the VMware vCenter Server and vSphere Client
- Credentials for the maintenance user

About this task

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

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

Steps

1. In the vSphere Client, click **Home > Inventory > VMs and Templates**, and select the virtual machine (VM) on which the virtual appliance for Unified Manager 6.3 or Unified Manager 6.4 is installed.
2. If the Unified Manager VM is running, navigate to **Summary > Commands > Shut Down Guest**.
3. Create a backup copy—such as a snapshot or clone—of the Unified Manager VM to create an application-consistent backup.
4. From the vSphere Client, 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-7.0-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, reminding you to back up the virtual machine on which the virtual appliance resides.

11. Type y to continue.

The upgrade process and the restart of Unified Manager services can take several minutes to complete.

12. Press any key to continue.

You are automatically logged out of the maintenance console.

13. Optional: Log in to the maintenance console, and verify the version of Unified Manager.

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

After you finish

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 OnCommand Unified Manager**Issue**

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

Cause

When you open a browser connection to the Unified Manager server, cookies are created. If you then upgrade to a newer version of Unified Manager, 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 web UI using the same credentials.

Upgrading to Unified Manager 7.0 from Unified Manager 6.3 RC1

When you are upgrading from Unified Manager 6.3 RC1 to Unified Manager 7.0, you must follow special instructions.

Before you begin

- You must have downloaded the `OnCommandUnifiedManager-7.0-virtual-update.iso` file from the NetApp Support Site.
- You must have the following information:
 - Credentials for accessing the VMware vCenter Server and vSphere Client
 - Credentials for the maintenance user

About this task

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

Steps

1. Log in to the vSphere Client, and navigate to **Home > Inventory > VMs and Templates** .
2. Select the virtual machine (VM) on which Unified Manager 6.3 RC1 is installed.
3. If the Unified Manager VM is running, navigate to **Summary > Commands > Shut Down Guest**.
4. Create a backup copy—such as a snapshot or clone—of the Unified Manager VM to create an application-consistent backup.
5. From the vSphere Client, power on the Unified Manager VM.
6. Click the **CD/DVD Drive** icon, and select **Connect to ISO image on local disk**.
7. Select the `OnCommandUnifiedManager-7.0-virtual-update.iso` file, and click **Open**.
8. From the **Console** tab, log in as a maintenance user.
9. In the **Main Menu**, type **4** to select Support/Diagnostics.
10. To access the diagnostic console, type **erds** at the command prompt .
 You are prompted with the following message: Remote diagnostic access is disabled. Would you like to enable remote diagnostic access? (y/N).
11. Type **y** to enable remote diagnostic access.
12. When prompted, enter a new UNIX password for the diagnostic user.
13. Type **x** to exit the maintenance console.
14. Log in to the maintenance console with **diag** as the user name and the new UNIX password that you set.
15. In the diagnostic command shell, run the `sudo ln -sf /cdrom /media/cdrom` command.
 This command creates a symbolic link from `/cdrom` to `/media/cdrom`.
16. After the command is successfully executed, log out from the console.
17. Log in to the vSphere Client console as a maintenance user.
18. In the **Main Menu**, type **1** to select Upgrade.

After the upgrade, you must wait for the discovery process to finish before you perform any task in the Unified ManagerUI. You can log in to the web UI to use the upgraded version of Unified Manager.

Removing Unified Manager

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

Before you begin

- You must have credentials for accessing VMware vCenter Server and vSphere Client.
- The Unified Manager server must not have an active connection to any Performance Manager servers.
If there is an active connection, you must delete the connection by using the Performance Manager maintenance console.
- The Unified Manager server must not have an active connection to a Workflow Automation server.
If there is an active connection, you must delete the connection by using the Administration menu.
- All clusters (data sources) must be removed from the Unified Manager server before you delete the virtual machine (VM).

Steps

1. In the vSphere Client, click **Home > Inventory > VMs and Templates**.
2. Select the VM that you want to destroy, and click the **Summary** tab.
3. If the VM is running, click **Commands > Shut Down Guest**.
4. 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 © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S.

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

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

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

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

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

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

Trademark information

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

<http://www.netapp.com/us/legal/netapptmlist.aspx>

How to send comments about documentation and receive update notifications

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

If you have suggestions for improving this document, send us your comments by email.

[*doccomments@netapp.com*](mailto: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 [12](#)
 - downloading [12](#)
- 7.0 release of Unified Manager
 - introduction to [5](#)
- A**
- accessing
 - Unified Manager web UI [16](#)
- Active Directory
 - using to enable remote authentication [28](#)
- adding
 - alerts [34](#)
 - authentication servers [30](#)
 - clusters [22](#)
 - clusters to Performance Manager [23](#)
 - clusters, volumes, aggregates to Favorites list [25](#)
 - favorites [24](#)
- aggregates
 - adding to Favorites list [25](#)
 - configuring global threshold values for [32](#)
- alerts
 - adding [34](#)
 - configuring your environment for [27](#)
 - creating [34](#)
- alternate configuration
 - monitoring capacities [14](#)
- authentication
 - testing for remote users and groups [31](#)
- authentication servers
 - adding [30](#)
- authentication, remote
 - disabling nested groups [29](#)
 - enabling [28](#)
- AutoSupport
 - what it does [5](#)
- B**
- backups
 - configuring database settings [36](#)
 - creating automatic backups [36](#)
 - restoring database on a virtual machine [37](#)
- browsers
 - supported [8](#)
- C**
- cannot log in to the web UI after upgrade
 - troubleshooting [48](#)
- certificates
 - viewing HTTPS security [21](#)
- certificates, HTTPS security
 - generating [20](#)
- Chrome
 - browser requirements [8](#)
- client software
 - supported versions [8](#)
- clustered Data ONTAP systems
 - See* clusters
- clusters
 - adding [22](#)
 - adding to Favorites list [25](#)
 - adding to Performance Manager [23](#)
 - moving to a different Performance Manager [25](#)
 - viewing discovery status [22](#)
- comments
 - how to send feedback about documentation [54](#)
- configurations
 - modifying virtual appliance default [15](#)
 - monitoring capacities [14](#)
- configuring
 - aggregate global threshold values [32](#)
 - database backup settings [36](#)
 - notification settings [27](#)
 - thresholds [32](#)
 - Unified Manager [18](#)
 - volume global threshold values [33](#)
 - your environment after deploying Unified Manager [19](#)
- connection setup
 - between Unified Manager and Workflow Automation [44](#)
- connections
 - between Performance Manager and Unified Manager, purpose of [39](#)
 - introduction to setting up between Performance Manager and Unified Manager [39](#)
- CPU requirements
 - table of [6](#)
- creating
 - alerts [34](#)
- customizing
 - Unified Manager host name [19](#)
- D**
- database user roles
 - Integration Schema, Report Schema [44](#)
- database users
 - creating [34, 44](#)
- databases
 - configuring backup settings [36](#)
 - restoring backup on a virtual machine [37](#)
- default configuration
 - monitoring capacity [14](#)
- default configurations
 - modifying virtual appliance [15](#)
- deleting
 - connection between Performance Manager and Unified Manager [43](#)
- deploying
 - Unified Manager [11](#)
 - Unified Manager virtual appliance [12](#)

- deployment
 - Unified Manager [10](#)
- deployment issues
 - maintenance user not created [51](#)
- discovery
 - viewing the status of clusters [22](#)
- documentation
 - how to receive automatic notification of changes to [54](#)
 - how to send feedback about [54](#)
- downloading
 - ISO image for upgrading Unified Manager [46](#)
 - software for deployment of Unified Manager as a virtual appliance [12](#)
 - the .ova file for deployment of Unified Manager [12](#)

E

- editing
 - lag threshold settings for unmanaged protection relationships [33](#)
- environment
 - setup [19](#)
- ESXi requirements
 - virtual appliance [7](#)

F

- Favorites list
 - managing storage objects from [24](#)
- feedback
 - how to send comments about documentation [54](#)
- Firefox
 - browser requirements [8](#)
- full integration connections
 - configuring [40](#)

G

- generating
 - HTTPS security certificates [20](#)
- groups
 - testing remote authentication [31](#)
- groups, nested
 - disabling remote authentication of [29](#)

H

- hardware
 - requirements [6](#)
- host names
 - changing [19](#)
- HTTPS
 - viewing the security certificate [21](#)
- HTTPS security certificates
 - generating [20](#)

I

- information

- how to send feedback about improving documentation [54](#)
- infrastructure requirements
 - table of [6](#)
- installation
 - configuring initial setup [16](#)
 - deploying Unified Manager virtual appliance [12](#)
 - Unified Manager [10](#)
- installation of Unified Manager
 - downloading the software [12](#)
- installing
 - accessing the GUI [16](#)
 - Unified Manager [11](#)
- integrated connections
 - configuring full [40](#)
 - configuring partial [42](#)
- Internet Explorer
 - browser requirements [8](#)
- ISO image
 - downloading before upgrading Unified Manager [46](#)
- issue resolution
 - what AutoSupport does [5](#)

L

- lag threshold settings
 - editing for unmanaged protection relationships [33](#)
- license requirements
 - VMware vSphere [6](#)
- Linux
 - supported versions [8](#)
- local users
 - changing password for [38](#)
 - creating [34](#)

M

- machines, virtual
 - restarting from the maintenance console [21](#)
- Macintosh
 - supported versions [8](#)
- maintenance console
 - console, maintenance
 - restarting the Unified Manager virtual machine from [21](#)
 - restarting the Unified Manager virtual machine from [21](#)
 - role of maintenance user [5](#)
- maintenance user
 - not created during deployment [51](#)
 - purpose [5](#)
- memory requirements
 - table of [6](#)
- messages, AutoSupport
 - how used for troubleshooting [5](#)
- modifying
 - lag threshold settings for unmanaged protection relationships [33](#)
- monitoring
 - cluster performance [22](#)
- moving
 - clusters to a Performance Manager server [25](#)

N

- nested groups
 - disabling remote authentication of [29](#)
- network settings
 - customizing the host name [19](#)
- notifications
 - adding alerts [34](#)
 - configuring settings for [27](#)

O

- OnCommand Workflow Automation
 - configuring connection with Unified Manager [45](#)
 - setting up a connection with Unified Manager [44](#)
- ONTAP
 - supported versions [8](#)
- Open LDAP
 - using to enable remote authentication [28](#)

P

- partial integration connections
 - configuring [42](#)
- passwords
 - changing local user [38](#)
- performance
 - monitoring for clusters [22](#)
- Performance Manager
 - adding clusters to [23](#)
 - configuring full integration connection to a Unified Manager server [40](#)
 - configuring partial integration connection to a Unified Manager server [42](#)
 - deleting a connection to a Unified Manager server [43](#)
 - introduction to setting up a connection to Unified Manager [39](#)
 - moving a clusters to [25](#)
 - purpose of connection with Unified Manager [39](#)
- performance monitoring
 - configuring full integration connection between Performance Manager and Unified Manager [40](#)
 - configuring partial integration connection between Performance Manager and Unified Manager [42](#)
 - deleting connections between Performance Manager and Unified Manager [43](#)
 - disabling [43](#)
 - enabling [40, 42](#)
- physical storage
 - adding clusters [22](#)
- platforms
 - supported [8](#)
- ports
 - requirements [8](#)
- privileges
 - creating a user with the Event Publisher role [40](#)
- protection relationships, unmanaged
 - editing lag threshold settings for [33](#)
- protocols
 - required ports [8](#)

R

- relationships, unmanaged protection
 - editing lag threshold settings for [33](#)
 - releases of Unified Manager
 - introduction to 7.0 [5](#)
 - remote authentication
 - disabling nested groups [29](#)
 - enabling [28](#)
 - remote groups
 - adding [34](#)
 - testing authentication [31](#)
 - remote users
 - adding [34](#)
 - testing authentication [31](#)
 - removing
 - favorites [24](#)
 - Unified Manager [50](#)
 - reports
 - creating a database user with the Report Schema role [44](#)
 - requirements
 - hardware [6](#)
 - ONTAP, supported versions [8](#)
 - port [8](#)
 - software [8](#)
 - virtual appliance [7](#)
 - virtual infrastructure [6](#)
 - VMware vSphere license [6](#)
 - restoring
 - database backup on a virtual machine [37](#)
 - role, Event Publisher
 - creating a user having [40](#)
 - roles
 - assigning to users [34](#)
- S**
- security certificates
 - viewing HTTPS [21](#)
 - security certificates, HTTPS
 - generating [20](#)
 - servers
 - required ports [8](#)
 - servers, authentication
 - adding [30](#)
 - setting up
 - aggregate global threshold values [32](#)
 - notification settings [27](#)
 - thresholds [32](#)
 - volume global threshold values [33](#)
 - setting up connections
 - between Performance Manager and Unified Manager, introduction to [39](#)
 - settings, lag threshold
 - editing for unmanaged protection relationships [33](#)
 - setup
 - post-deployment [19](#)
 - software requirements
 - compliance with [8](#)
 - storage objects
 - adding to favorites [25](#)
 - suggestions

- how to send feedback about documentation [54](#)
- supported
 - browser and platform [8](#)
 - browsers [8](#)
 - platforms [8](#)
- system requirements
 - for deploying the Unified Manager virtual appliance [6](#)

T

- testing
 - authentication for remote users and groups [31](#)
- threshold settings, lag
 - editing for unmanaged protection relationships [33](#)
- thresholds
 - configuring [32](#)
 - configuring global values for aggregates [32](#)
 - configuring global values for volumes [33](#)
- troubleshooting
 - maintenance user is not created [51](#)
 - virtual appliance installation issues [51](#)
 - web UI login issue after upgrade [48](#)
 - what AutoSupport does [5](#)
- Twitter
 - how to receive automatic notification of documentation changes [54](#)

U

- UI
 - accessing [16](#)
- Unified Manager
 - accessing the web UI [16](#)
 - configuring [18](#)
 - configuring connection with Workflow Automation [45](#)
 - configuring the virtual appliance [16](#)
 - deploying [10, 11](#)
 - downloading the ISO image before upgrading Unified Manager [46](#)
 - downloading the software [12](#)
 - installing [10, 11](#)
 - introduction to 7.0 release [5](#)
 - supported ONTAP versions [8](#)
 - uninstalling [50](#)
 - upgrading to 7.0 [46](#)
 - upgrading to 7.0 from 6.3 RC1 [48](#)
 - upgrading to 7.0 from 6.x [47](#)
- Unified Manager upgrade
 - downloading the ISO image before [46](#)
- Unified Manager virtual appliance
 - system requirements for deploying [6](#)
- uninstalling
 - Unified Manager [50](#)
- unmanaged protection relationships
 - editing lag threshold settings for [33](#)
- upgrade issues

- cannot log in to web UI after, troubleshooting [48](#)
- upgrade process
 - from Unified Manager 6.x to Unified Manager 7.0 [47](#)
 - to Unified Manager 7.0 [46](#)
- upgrading
 - to Unified Manager 7.0 on VMware [47](#)
 - Unified Manager 6.3 RC1 to Unified Manager 7.0 [48](#)
- user roles
 - assigning [34](#)
- users
 - adding [34](#)
 - changing password for local [38](#)
 - creating [34](#)
 - creating having the Event Publisher role [40](#)
 - maintenance [5](#)
 - testing remote authentication [31](#)
- users, database
 - creating [44](#)

V

- vApp
 - See* virtual appliance
- viewing
 - discovery status of clusters [22](#)
 - Favorites list [24](#)
- virtual appliance
 - configuring initial setup [16](#)
 - deploying Unified Manager [12](#)
 - requirements [7](#)
 - system requirements for deploying, Unified Manager [6](#)
 - what it does [5](#)
- virtual appliance (vApp)
 - destroying [50](#)
- virtual appliance default configurations
 - modifying [15](#)
- virtual infrastructure
 - requirements [6](#)
- virtual machines
 - restarting from the maintenance console [21](#)
 - restoring database backup [37](#)
- volumes
 - adding to Favorites list [25](#)
 - configuring global threshold values for [33](#)
- vSphere requirements
 - virtual appliance [7](#)

W

- Windows
 - supported versions [8](#)
- Workflow Automation
 - configuring connection with Unified Manager [45](#)
 - creating a database user with the Integration Schema role [44](#)
 - setting up a connection with Unified Manager [44](#)