OnCommand® Unified Manager 7.0

Installation and Setup Guide

For Microsoft® Windows®

July 2016 | 215-11253_A0
doccomments@netapp.com

Contents

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 install Unified Manager on a Windows server.

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.

Unified Manager installation and setup on Windows

Installing Unified Manager on Windows includes performing tasks such as preparing for the installation, downloading the installer, and running the installer. After the installation is complete, you can configure Unified Manager to meet your requirements.

How Unified Manager works with Windows

You can install and run Unified Manager on Windows to monitor and manage clustered Data ONTAP.

The Windows server on which you install Unified Manager can be running either on a physical machine or on a virtual machine running on VMware ESXi Server or Microsoft Hyper-V. To install Unified Manager on Windows, you must first download the OnCommand Unified Manager Windows installer from the NetApp Support Site, and install Unified Manager.

System requirements for Unified Manager

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

Hardware requirements

The following capabilities and capacities must be reserved to support Unified Manager.

Hardware configuration	Minimum requirement
Free disk space	120 GB
Reserved RAM	12 GB **Note:** Microsoft recommends that you reserve virtual memory 1.5 to 3 times the size of the reserved RAM.
Reserved CPU cycle capacity	9572 MHz of 4 virtual CPUs

The reservation of memory and CPU resources is required for running Unified Manager. Reserving the listed values for memory and CPU resources guarantees that the required minimum amount is always available for the system.

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 system to boot. If four cores are not adequate, you must increase the number of CPU sockets or CPU cores per socket to provide the required CPU cycles that are needed to run Unified Manager.

Software requirements

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

- Microsoft Windows Server 2008 R2 Standard and Enterprise Edition
- Microsoft Windows Server 2008 SP2 Standard and Enterprise Edition
- Microsoft Windows Server 2012 Standard and Datacenter Edition
- Microsoft Windows Server 2012 R2 Standard and Datacenter Edition

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

Supported browsers

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

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

When you are using a browser or API client, 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. 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, and 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 be made only using HTTPS.
MySQL database	MySQL	3306	Used to enable OnCommand Workflow Automation and OnCommand Report 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 that are used by the Unified Manager server to connect to specific destinations.

The Unified Manager server uses the following protocols and ports to connect 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. Internet access is required to perform this function.
Authentication server	LDAP	389	Used to make authentication requests, and user and group lookup requests.
Authentication server	LDAPS	636	Used to make authentication requests, and user and group lookup requests.

Destination	Protocol	Port	Description
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.

Supported versions of ONTAP software

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

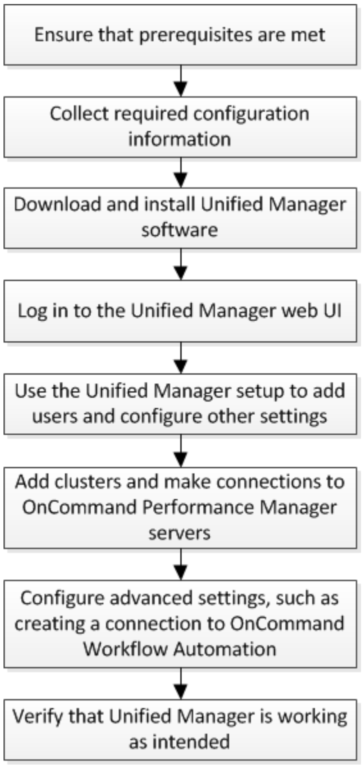
Integration with other OnCommand products

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.

Installing Unified Manager

The installation workflow describes the tasks that you must perform before you can use Unified Manager. You can install Unified Manager on Microsoft Windows to monitor and troubleshoot data storage capacity, availability, performance, and protection issues.


Ensure that prerequisites are met
Collect required configuration information
Download and install Unified Manager software
Log in to the Unified Manager web UI
Use the Unified Manager setup to add users and configure other settings
Add clusters and make connections to OnCommand Performance Manager servers
Configure advanced settings, such as creating a connection to OnCommand Workflow Automation
Verify that Unified Manager is working as intended

Prerequisites for installing Unified Manager on Windows

Before installing Unified Manager on the Windows platform, you must ensure that you have the required information, and that you have completed certain tasks.

- You must download the Unified Manager installation file from the NetApp Support Site, and copy the file to the server on which you want to install Unified Manager.

  You must have valid credentials to log in to the NetApp Support Site. If you do not have valid credentials, you can register on the site to obtain the credentials.

- You must disable Microsoft IIS worldwide web publishing service and ensure that ports 80 and 443 are free.

- You must reserve 120 GB of free hard disk space, where the capacity is allocated as follows:
  - 100 GB of disk space for the Unified Manager installation directory
  - 20 GB of disk space for the MySQL data directory

- You must reserve 2 GB of disk space for the `temp` directory to extract the installation files.

- You must reserve 2 GB of disk space in the Windows drive for caching the Unified Manager MSI files.

- Microsoft .NET 4.0 must be installed.

- The following third-party packages are required:
  - JRE 1.8.0.92, or later
  - MySQL Community Edition 5.6.28, or later in the 5.6 family
  - 7zip 9.20.1, or later

  If these third-party packages are not installed, Unified Manager installs them as part of the installation.
- The server on which you want to install Unified Manager must be dedicated exclusively to running Unified Manager, and must not be shared with any other application.
- The Microsoft Windows Server on which you want to install Unified Manager must be configured with a fully qualified domain name (FQDN) such that `ping` responses to the host name and FQDN are successful.
- If MySQL is pre-installed, you must ensure that it is using the default port, and you must ensure that you have not installed the sample databases.
- UDP port 514 must be free, and must not used by any other service.

Required configuration information

Unit or system	Details	Purpose
Arrays	• IP address • User name and password	Performs operations on storage systems. **Note:** The root or administrator account credentials are required for storage (arrays).
Mail server	• IP address • User name and password **Note:** User name and password are required if your mail server requires authentication.	Receives Unified Manager notifications through email.
AutoSupport server	Mail host	Sends AutoSupport messages through SMTP. If you do not have a mail host configured, you can use HTTP or HTTPS to send AutoSupport messages.
Microsoft Active Directory (AD) LDAP Server	• IP address • User name and password • Group name You should use an LDAP bind account with read-only privilege.	Authenticates and authorizes using AD LDAP or AD LDAPS.
SNMP management application	• IP address • Port	Receives Unified Manager notifications.

Unit or system	Details	Purpose
Syslog server	IP address	Sends log data.

Installing Unified Manager on Windows

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

Before you begin

- You must have reviewed the installation prerequisites.
  Installation prerequisites on page 9
- You must have Windows administrator privileges.

Steps

1. Log in to Windows using the default local administrator account.
2. Navigate to the directory where the installation file is located.
3. Right-click and run the Unified Manager installer executable (`.exe`) file as an administrator.

   Unified Manager detects missing or pre-installed third-party packages and lists them. If the required third-party packages are not installed in the system, Unified Manager installs them as part of the installation.
4. Click **Next**.
5. Enter the user name and password to create the maintenance user.
6. In the **Database Connection** wizard, enter the MySQL root password.
7. Click **Change** to specify a new location for the Unified Manager installation directory and MySQL data directory.

   If you do not change the installation directory, Unified Manager is installed in the default installation directory.
8. Click **Next**.
9. In the **Ready to Install Shield**wizard, click **Install**.
10. After the installation is complete, click **Finish**.
11. Log in to the Unified Manager web user interface using the following URL: `https://`*`IP address`*

Result

As part of the installation, Unified Manager creates three directories:

- Installation directory
  This is the root directory for Unified Manager, which you specified during installation. Example: `C:\Program Files\NetApp\`
- MySQL data directory
  This is the directory where the MySQL databases are stored, which you specified during installation. Example: `C:\ProgramData\MySQL\`

- Unified Manager application data directory (appDataDir)

  This is the directory where all the application-generated data is stored. This includes logs, support bundles, backup, and all other additional data. Example: `C:\ProgramData\NetApp\OnCommandAppData\`, where C:\ refers to the root of the Unified Manager installation directory.

Performing an unattended installation of Unified Manager

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

Steps

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

Option	Instructions

If third-party packages are pre-installed	`OnCommandUnifiedManager-7.0.exe /`
	`V"MYSQL_PASSWORD=mysql_password INSTALLDIR=`
	`\"Installation directory\" MYSQL_DATA_DIR=\"MySQL`
	`data directory\"`
	`MAINTENANCE_PASSWORD=maintenance_password`
	`MAINTENANCE_USERNAME=maintenance_username`
	`/qn /l*v CompletePathForLogFile"`
	Example:
	`OnCommandUnifiedManager.exe /s /`
	`v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:`
	`\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:`
	`\ProgramData\MYSQL\" MAINTENANCE_PASSWORD=*******`
	`MAINTENANCE_USERNAME=admin /qn /l*v C:`
	`\install.log"`

If third-party packages are not installed	`OnCommandUnifiedManager-7.0.exe /`
	`V"MYSQL_PASSWORD=mysql_password INSTALLDIR=`
	`\"Installation directory\" MYSQL_DATA_DIR=\"MySQL`
	`data directory\"`
	`MAINTENANCE_PASSWORD=maintenance_password`
	`MAINTENANCE_USERNAME=maintenance_username`
	`/qr /l*v CompletePathForLogFile"`
	Example:
	`OnCommandUnifiedManager.exe /s /`
	`v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:`
	`\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:`
	`\ProgramData\MYSQL\" MAINTENANCE_PASSWORD=*******`
	`MAINTENANCE_USERNAME=admin /qr /l*v C:`
	`\install.log"`

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

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

3. Log in to the Unified Manager web user interface by using the following URL:

   `https://IP address`

Setting up Unified Manager in a failover clustering environment

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

In this setup, only one node owns all the cluster resources. When one node goes down or any of the configured services fail to come online, the failover cluster service recognizes this event and immediately transfers control to the other node. The second node in the setup becomes active and starts providing services. The failover process is automatic and you do not have to perform any actions.

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

Requirements for Unified Manager in a failover clustering environment

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

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

- Both the cluster nodes must be running Microsoft Windows Servers 2008 or 2012 Enterprise edition or Data Center edition.
- The same version of Unified Manager must be installed using the same path on both the cluster nodes.
- Failover clustering must be installed and enabled on both the nodes.
  See Microsoft documentation for instructions.
- You must have used Fibre Channel switched fabric or iSCSI-based storage for creating shared data disk as the storage back-end.
- Optional: Using SnapDrive for Windows, a shared location must be created that is accessible to both the nodes in the high-availability setup.
  See the *SnapDrive for Windows Installation Guide* for information about installing and creating a shared location.
  You can also manage LUNs using the storage system command-line interface. See the SnapDrive for Windows compatibility matrix for more information.
- You must have the Perl installed with `XML::LibXML` and `File::chdir` modules for scripts to work.
- There must be only two nodes in the cluster setup.
- The “node and disk majority” quorum type must be used for failover clustering.
- You must have configured a shared IP address with a corresponding FQDN to be used as the cluster global IP address to access Unified Manager.
- The password for Unified Manager maintenance user on both the nodes must be same.
- You must have used only IPv4 IP address.

Installing Unified Manager on MSCS

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

Steps

1. Log in as the domain user on both the nodes of the cluster.
2. Set up high availability by choosing one of the following options:

If you want to...	Then do this...
Configure high availability on an existing Unified Manager installation	Add another server to be paired with the existing server: **a.** Upgrade the existing Unified Manager server to the latest software version. **b.** Create a backup of the existing Unified Manager installation, and store the backup to a mounted LUN. **c.** Install Unified Manager on the second node. *Installing Unified Manager on Windows* on page 11 **d.** Restore the backup of the existing Unified Manager installation onto the second node.
Configure high availability on a new Unified Manager installation	Install Unified Manager on both the nodes. *Installing Unified Manager on Windows* on page 11

Configuring Unified Manager server with MSCS using configuration scripts

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

Before you begin

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

Steps

1. Log in to the first node of the cluster.
2. Create a service group in Windows 2008 or a role in Windows 2012 using Failover Cluster Manager:
   a. Launch Failover Cluster Manager.
   b. Create the empty service group or role:
      - Service group: Right-click **Service group** > **More Actions** > **Create Empty Service**.
      - Role: Click **Roles** > **Create Empty Role**.
   c. Add the global IP address to the service or role by right-clicking **Role** > **Add Resources** > **More Resources** > **IP address**.

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

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

3. Run the `ha_setup.pl` script on the first node:

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

   Example

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

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

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

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

   Example

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

8. Bring all the Unified Manager services online using Failover Cluster Manager.
9. Manually switch to the other node of the Microsoft Cluster Server.
10. Verify that the Unified Manager server services are starting properly on the other node of the cluster.
11. Regenerate the Unified Manager certificate after running configuration scripts to obtain the global IP address required for setting up a connection to OnCommand Performance Manager.

    a. Click **Administration** > **Setup Options**.

    b. In the **Setup Options** dialog box, click **Management Server**.

    c. In the HTTPS section, click **Regenerate HTTPS Certificate**.

    The regenerated certificate provides the cluster IP address but not the FQDN name. Therefore, you must use the global IP address to set up a connection between OnCommand Performance Manager and Unified Manager.

12. Access the Unified Manager UI using the following URL:

    `https://`***`FQDN of the Global IP address`***

After you finish

You must create a shared backup location after high availability is configured. The shared location is required for containing the backups before and after failover. Both nodes in the high-availability setup must be able to access the shared location.

Configuring after installation

After you install Unified Manager software, you can log in to the web UI as the default user umadmin, and complete an initial setup to configure a minimum software configuration. You can then configure additional options, such as adding email alerts, adding users, changing the passwords, and adding clusters that you want to monitor.

Because the default user umadmin is assigned the OnCommand Administrator user role, that user is authorized to perform any configuration task that is possible through the web UI.

Configuring your environment after initial setup

After you perform initial setup of the software, there are several configuration tasks that you might want to perform before you start monitoring your clusters, such as adding users, enabling user authentication, and adding alerts.

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 19

   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 19

   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 21

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

4. *Edit global threshold settings* on page 23

   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 25

   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 27

   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	• Authentication server administrator name in one of following formats: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (using the appropriate LDAP notation) • Administrator password • Base distinguished name (using the appropriate LDAP notation)
Open LDAP	• 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	**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**. **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.
Disable it	**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 24

  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 24

  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 25

  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 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 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**.

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.

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 Windows

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 to a local Windows system or a remote Windows system by using the restore command.

Before you begin

- You must have Windows administrator privileges.
- You must have installed and configured Unified Manager.
- The Unified Manager backup file that you want to restore must exist in the system on which you want to perform the restore operation.
- The backup file must be of `.7z` type.

About this task

The restore feature is platform-specific and version-specific. You can restore a Unified Manager backup only on the same version of Unified Manager, and only a Windows backup file can be restored on a Windows platform.

Steps

1. Log in to the Unified Manager console as an administrator:

   ```
   um cli login -u maint_username
   ```

2. At the command prompt, restore the backup:

   ```
   um backup restore -f \ProgramData\NetApp\OnCommandAppData\ocum\backup
   \backup_file_name
   ```

   Example

   ```
   um backup restore -f \ProgramData\NetApp\OnCommandAppData\ocum\backup
   \UM_6.4.N151118.2300_backup_windows_11-20-2015-02-51.7z
   ```

   If the folder names contain space, you must include the absolute path or relative path of the backup file in double quotation marks.

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

Upgrading to Unified Manager 7.0 on Windows

You can upgrade Unified Manager 6.3 or 6.4 to Unified Manager 7.0 by downloading and running the installation file on the Windows platform.

Before you begin

- You must have Windows administrator privileges.
- You must have valid credentials to log in to the NetApp Support Site.
  If you do not have valid credentials, you can register on the site to obtain the credentials.
- To avoid data loss, you must have created a backup of the Unified Manager machine in case there is an issue during the upgrade.

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:** If you upgrade from Unified Manager 6.3 to Unified Manager 7.0, the app_registry files will not contain details about the cluster IDs. You must restart the RP and ocie services to resolve this issue.

Steps

1. Log in to the NetApp Support Site, and locate the Download page for installing Unified Manager on the Windows platform.

   mysupport.netapp.com

2. Download the Unified Manager 7.0 Windows installation file to a target directory in the Windows system.

3. If Unified Manager is configured for high availability, stop all the Unified Manager services on the first node by using Microsoft Cluster Server, and then start the MySQL service from `services.msc`.

4. Right-click and run the Unified Manager installer executable `(.exe)` file as an administrator.

   Unified Manager prompts you with the following message:

   ```
   This setup will perform an upgrade of ‘OnCommand Unified Manager’. Do
   you want to continue?
   ```

5. Click **Yes**, and then click **Next**.

6. Enter the MySQL root password that was set during installation, and click **Next**.

7. After the upgrade is successful, if the system is configured for high availability, start all the Unified Manager services from the Failover Cluster Manager.

8. From the command prompt, run the `ha_setup.pl` script to configure the new services in the failover cluster and the files that are present in the shared location.

   Example

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

9. Stop all the Unified Manager services (RP, ocie, ocieau, and MySQL) in the first node by using Microsoft Cluster Server.

10. Start the MySQL service on the second node from `services.msc`.

11. Switch the service group to the second node in the high-availability setup.

12. Upgrade Unified Manager on the second node.

13. At the command prompt, enter **`Y`** to continue, or enter any other character to abort.

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

14. Start all the Unified Manager services on both the nodes using Microsoft Cluster Server.

15. From the command prompt, run the `ha_setup.pl` script with the **`--upgrade`** option.

    Example

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

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

After you finish

Note: To perform a silent upgrade of Unified Manager, run the following command:

```
OnCommandUnifiedManager-7.0.exe /s /v"MYSQL_PASSWORD=netapp21! /qn /l*v
C:\install.log
```

Related tasks

Setting up a connection between OnCommand Workflow Automation and Unified Manager on page 39

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.

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 35
   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 35
   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 37
   You can connect a Performance Manager server with the Unified Manager server to send performance events to Unified Manager.

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.

   - When installed on Red Hat Enterprise Linux, log in as umadmin to the Red Hat Enterprise Linux host machine. When 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 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. Restart the Performance Manager server if it does not restart 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 on Red Hat Enterprise Linux, log in as umadmin to the Red Hat Enterprise Linux machine that hosts Performance Manager. 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

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. In the maintenance console, type the number of the menu option that is labeled **Unified Manager Integration**.

2. If prompted, enter the maintenance user password again.

3. Select **Partial Integration** > **Delete Unified Manager Server Connection**.

4. 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 39
   You can create a database user to begin pairing Workflow Automation with Unified Manager.
2. Set up Workflow Automation in Unified Manager on page 40
   You can pair Workflow Automation with Unified Manager to define workflows for your storage classes.

Related tasks

Upgrading to Unified Manager 7.0 on Windows on page 31

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 theUnified 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.

Uninstalling Unified Manager from Windows

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

Before you begin

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

Steps

1. Navigate to the location from which you want to uninstall Unified Manager.
2. Uninstall Unified Manager by choosing one of the following options:

To uninstall Unified Manager from the...	Then...
Programs and Features wizard	**a.** Navigate to **Control Panel > Program and Features**. **b.** Select OnCommand Unified Manager, and click **Uninstall**.
Command line	**a.** Log in to the Windows command line using administrator privileges. **b.** Navigate to the OnCommand Unified Manager directory, and run the following command: `msiexec /x {A78760DB-7EC0-4305-97DB-E4A89CDFF4E1} /qn /l*v %systemdrive%\UmUnInstall.log`

   Unified Manager is uninstalled from your system.

3. Uninstall the following third-party packages and data that are not removed during the Unified Manager uninstallation:
   - Third-party packages: JRE, MySQL, and 7zip
   - MySQL application data generated by Unified Manager
   - Application logs and contents of application data directory

Troubleshooting Unified Manager installation on Windows

During or shortly after installation of Unified Manager on a Windows system, you might encounter some issues that require further attention. Unified Manager stores the installation log files in `AppData directory\ocum\UMInstall-timestamp`. Please refer this log

Copyright information

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

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