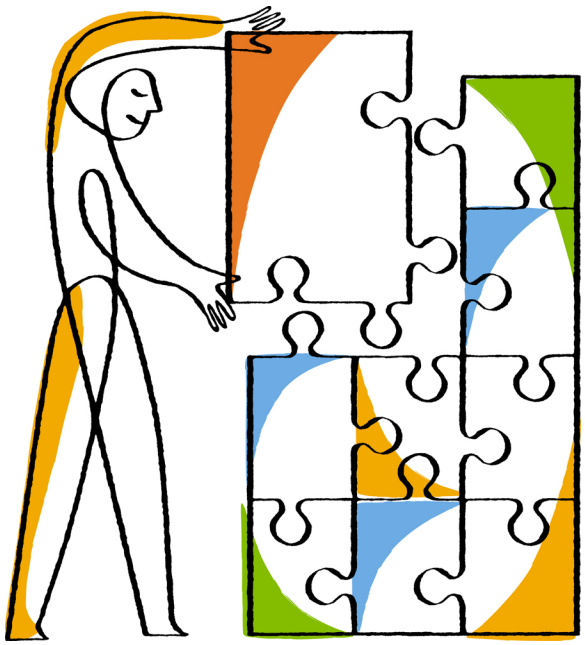
OnCommand® Unified Manager 6.3

Installation and Setup Guide

For Microsoft® Windows®



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

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

Part number: 215-10194_B0
October 2015

Contents

Unified Manager installation and setup on Windows 5
How Unified Manager works with Windows 5
System requirements for Unified Manager 6
Installing Unified Manager 8
Prerequisites for installing Unified Manager 8
Installing Unified Manager on Windows 10
Performing an unattended installation of Unified Manager 11
Setting up Unified Manager in a failover clustering environment 13
Requirements for Unified Manager in a failover clustering environment 13
Installing Unified Manager on MSCS 14
Configuring Unified Manager server with MSCS using configuration scripts 14
Configuring after installation 17
Configuring your environment after initial setup 17
Configuring Unified Manager to send alert notifications 17
Configuring notification settings 18
Enabling remote authentication 18
Disabling nested groups from remote authentication 19
Adding authentication servers 20
Testing the configuration of authentication servers 21
Editing global threshold settings 22
Configuring global aggregate threshold values 22
Configuring global volume threshold values 23
Editing unmanaged relationship lag threshold settings 23
Adding a user 24
Adding clusters 25
Adding an alert 26
Configuring database backup settings 28
Restoring a database backup on Windows 28
Changing the maintenance user password 29
Generating and sending support bundle 29
Upgrading to Unified Manager 6.3 from Unified Manager 6.3 on Windows 30
Setting up a connection between OnCommand Workflow Automation and Unified Manager 32
Creating a database user 32
Setting up a connection between OnCommand Workflow Automation and Unified Manager 33
Uninstalling Unified Manager 34
Troubleshooting Unified Manager installation on Windows 35
Command-line interface commands not working on Windows 35
Copyright information 36
Trademark information 37

How to send comments about documentation and receive update notifications 38
Index 39

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

To ensure 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

Component	Recommended
RAM	12 GB
Free disk space	120 GB
CPU	9.572 GHZ of 4 vCPU

Software requirements

Unified Manager runs only on a 64-bit Windows operating system and should be installed on a dedicated machine. You must not install any other application on the server. 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

Supported browsers

- Microsoft Internet Explorer 10 and 11
- Google Chrome 41 and 42
- Mozilla Firefox ESR 31 and 38
- Apple Safari 7 and 8

Supported browser client platforms

- Windows Vista, Windows 7, and Windows 8
- Red Hat Enterprise Linux 64-bit 6.5 and 6.6
- SUSE Linux Enterprise Server 11 SP2
- Macintosh OS X 10.8

Protocol and port requirements

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.

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.

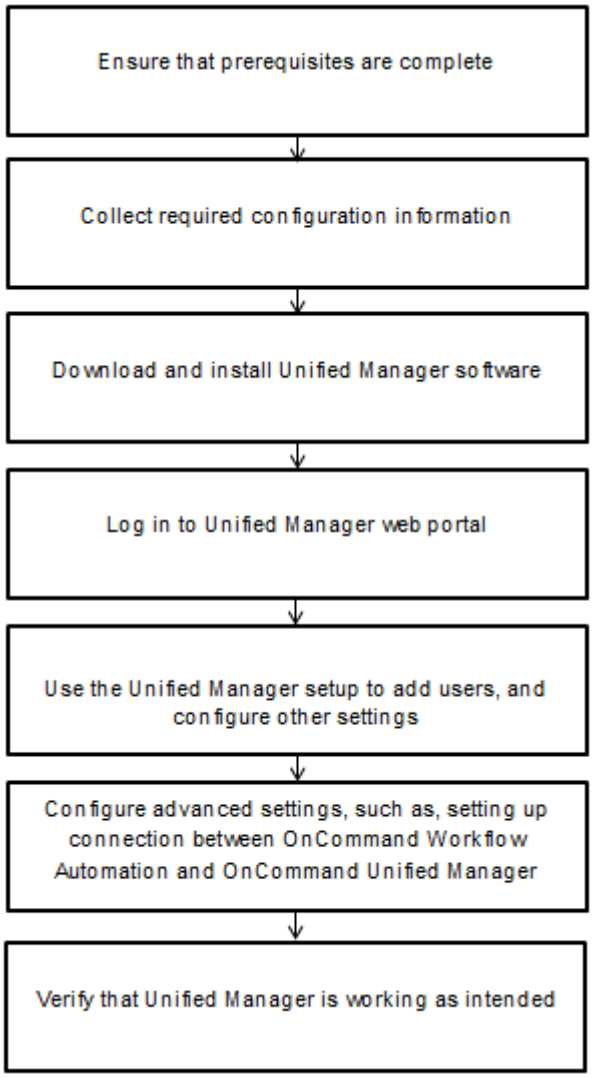
Depending on your environment, you can choose to modify the ports and protocols used by the Unified Manager server to connect to specific destinations.

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	LDAPS	636	Used to make authentication requests, and user and group lookup requests.
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.
Syslog	UDP	514	Used to listen to and access EMS messages from Data ONTAP clusters and create appropriate events based on the messages. Currently, only MetroCluster configuration events use this interface.

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.



Prerequisites for installing Unified Manager

Before installing Unified Manager, you must ensure that you have the required information and 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 for the credentials.

- You must disable Microsoft IIS worldwide web publishing service and ensure that port 80/443 is free.
- You must reserve 120 GB free hard disk space, where the capacity is allocated as follows:
  - 100 GB of disk space for the Unified Manager installation directory
  - 20 GB disk space for the MySQL data directory.
- Reserve 2 GB disk space for the `temp` directory to extract the installation files.
- 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 must be installed:
  - JRE 1.8.0.51
  - MySQL Community Edition 5.6.26
  - 7zip 9.20.1

  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 not shared with any other application.
- Microsoft Windows Server 2008 or 2012 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 on the default port.
- The 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	Perform 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.	Receive Unified Manager notifications through email.
AutoSupport server	• Mail host	Send AutoSupport messages through SMTP. If you do not have a mail host configured, you can use HTTP or HTTPS to send AutoSupport messages.

Unit or system	Details	Purpose
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.	Authenticate and authorize using AD LDAP or AD LDAPS.
SNMP management application	• IP address • Port	Receive Unified Manager notifications.
Syslog server	• IP address	Send log data.

Installing Unified Manager on Windows

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

Before you begin

- You must have reviewed the *installation prerequisites* on page 8.
- 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 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 new location for Unified Manager installation directory and MySQL data directory.

   If you do not change the installation directory. Unified Manager is installed in the default install 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`

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

- Install directory – This is the root directory for Unified Manager, which you would have selected during installation. Example: `C:\Program Files\NetApp\`
- MySQL data directory – This is the directory where MySQL databases are stored, you would have selected this during installation. Example: `C:\ProgramData\MySQL\`
- Unified Manager application data directory (appDataDir) – This is the directory where all the application generated data like, logs, support bundle, backup, and all other additional data are stored. Example: `C:\ProgramData\NetApp\OnCommandAppData\` where c:\ refers to root of the Unified Manager installation directory.

Performing an unattended installation of Unified Manager

You can install Unified Manager on Windows without user intervention 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 using the default local administrator account.
2. Navigate to the location where you want to install Unified Manager.

Option	Description
If third-party packages are pre-installed	**OnCommandUnifiedManager-6.3.EXE /V"MYSQL_PASSWORD=*mysql_password* INSTALLDIR=\"*Installation directory*\" MYSQL_DATA_DIR=\"*MySQL data directory*\" MAINTENANCE_PASSWORD=*maintenance_password* MAINTENANCE_USERNAME=*maintenance_username* *CompletePathForLogFile*"** Example **OnCommandUnifiedManager-6.3.N150623.0351.exe /s /v"MYSQL_PASSWORD=netapp1! 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-6.3.EXE /V"MYSQL_PASSWORD=*mysql_password* INSTALLDIR=\"*Installation directory*\" MYSQL_DATA_DIR=\"*MySQL data directory*\" MAINTENANCE_PASSWORD=*maintenance_password* MAINTENANCE_USERNAME=*maintenance_username* *CompletePathForLogFile*"** Example **OnCommandUnifiedManager-6.3.N150623.0351.exe /s /v"MYSQL_PASSWORD=netapp1! 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 means quiet mode with 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 have to 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 means 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 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 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:

Option	Steps
If you have an existing Unified Manager installation and want to configure high availability	You can bring another server to be paired with existing and follow the steps: **a.** Upgrade existing Unified Manager to Unified Manager 6.3. **b.** Create a backup of the existing Unified Manager installation and store the backup to a mounted LUN. **c.** Install Unified Manager on both the nodes. *Installing Unified Manager on Windows* on page 10 **d.** Restore the backup of the existing Unified Manager installation on the second node in high availability.
If you are setting up high availability on a new installation	Install Unified Manager on both the nodes. *Installing Unified Manager on Windows* on page 10

Configuring Unified Manager server with MSCS using configuration scripts

After installing Unified Manager on both the 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:

Platform	Create a service group or role
Windows 2008	**a.** Launch Failover Cluster Manager. **b.** Right-click **Service group > More Actions > Create Empty Service**. **c.** Add the global IP address to the service by right-clicking **Role > Add Resources > More Resources > IP address**. **Note:** Both the nodes must be able to ping this IP address because Unified Manager will be launched using this IP address after high availability is configured. **d.** Add the data disk to the role by right-clicking **Role > Add Storage**.
Windows 2012	**a.** Launch Failover cluster manager. **b.** Click **Roles > Create Empty Role**. **c.** Add the global IP address to the role by right-clicking**Role > Add Resources > More Resources > IP address**. **Note:** Both the nodes must be able to ping this IP address because Unified Manager will be 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_name_cluster_name -f shared_location_path -k data_disk`

   Example

   ```
   C:\Program Files\NetApp\ocum\bin>perl .\ha_setup.pl --first -t mscs -g
   umrole -i "IP Address" -n scspr0038457002.gdl.englab.netapp.com -k
   "Cluster Disk 2" -f E:\
   ```

   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 the 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 the Unified Manager server services (MySQL, ocie, ocieau) using `services.msc`.
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 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 the nodes in the high-availability setup must be able to access the shared location.

Configuring after installation

After installation of the software is complete, you can log in to the web UI as the default user umadmin, 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 you want to monitor.

Because the default user umadmin is assigned the OnCommand Administrator user role, that user has authorization 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 18

   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 18

   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 20

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

4. *Edit global threshold settings* on page 22

   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 24

   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 26

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

Configuring notification settings

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

Before you begin

The following information must be available:

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

You must have the OnCommand Administrator or Storage Administrator role.

Steps

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

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

   Tip: If the host name of the SMTP server cannot be resolved, you can specify the IP address (IPv4 or IPv6) of the SMTP server instead of the host name.

Enabling remote authentication

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

Before you begin

You must have the OnCommand Administrator role.

About this task

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

Remote authentication is supported over LDAP and LDAPS (Secure LDAP).

Steps

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

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

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

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

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

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

   If you select the **Use Secure Connection** option for an authentication server, then Unified Manager communicates with the authentication server using the Secure Socket Layer protocol.

   Note: Unified Manager uses 389 as default port for non-secure communication and 636 as default port for secure communication.

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

Disabling nested groups from remote authentication

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

Before you begin

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

About this task

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

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Management Server > Authentication**.
3. 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 pair (using the same database), you can also add the partner authentication server. This enables the management server to communicate with the partner when one of the authentication servers is unreachable.

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Management Server > Authentication**.
3. Enable or disable the Use secure connection authentication by choosing one of the following options:

If you want to...	Then do this...
Enable the Use secure connection option	**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 click **Close**. **f.** In the Authorize Host dialog box, click **Yes**. **Note:** When you enable the **Use Secure Connection** 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 the Use secure connection option	**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**.

Result

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

After you finish

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

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 by searching for a remote user or group from your authentication servers and authenticate them using the configured settings.

Before you begin

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

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 **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Management Server > Authentication**.
3. In the **Authentication Setup Options** dialog box, click **Test Authentication**.
4. In the **Test User** dialog box, specify the user name and password of the remote user or 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 22

  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 23

  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 23

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

Configuring global aggregate threshold values

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

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

Before you begin

You must have the OnCommand Administrator or Storage Administrator role.

About this task

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

Steps

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

Configuring global volume threshold values

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

Before you begin

You must have the OnCommand Administrator or Storage Administrator role.

About this task

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

Steps

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

Editing unmanaged relationship lag threshold settings

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

Before you begin

You must have the OnCommand Administrator or Storage Administrator role.

About this task

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

Steps

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

Adding a user

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

Before you begin

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

About this task

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

Steps

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

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

Adding clusters

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

Before you begin

- The following information must be available:
  - Host name or cluster-management IP address
    The host name is the FQDN or short name that Unified Manager uses to connect to the cluster. This host name must resolve to the cluster-management IP address.
    The cluster-management IP address must be the cluster-management LIF of the administrative Storage Virtual Machine (SVM). If you use a node-management LIF, the operation fails.
  - Data ONTAP administrator user name and password
  - Type of protocol (HTTP or HTTPS) that can be configured on the cluster and the port number of the cluster
- You must have the OnCommand Administrator or Storage Administrator role.
- The Data ONTAP administrator must have the ONTAPI and SSH administrator roles.
- The Unified Manager FQDN must be able to ping Data ONTAP.
  You can verify this by using the 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 **Storage** > **Clusters**.
2. From the **Clusters** page, click **Add**.
3. In the **Add Cluster** dialog box, specify the values required, 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 finishes.
4. Click **Add**.
5. If HTTPS is selected, perform the following steps:
   a. In the **Authorize Host** dialog box, click **View Certificate** to view the certificate information about the cluster.
   b. Click **Yes**.

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

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

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

Result

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

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 your script to the alert.

Before you begin

- You must have configured notification settings such as the email address, SMTP server, and SNMP trap host so that the Unified Manager server can use these settings to send notifications to users when an event is generated.
- You must know the resources and events for which you want to trigger the alert, and user names or email addresses of users you want to notify.
- You must have added scripts to Unified Manager 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 **Administration > Manage Alerts**.
2. In the **Manage Alerts** page, click **Add**.
3. In the **Add Alert** dialog box, perform the following steps:
   a. Click **Name** and enter a name and description for the alert.
   b. Click **Resources** and select the resources to be included or excluded from the alert.

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

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

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

d. Click **Actions** and select the users that you want to notify, 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 have modified the email address of the selected user from the Manage Users page, the modified email address is not updated for the selected user.

You can also choose to notify users through SNMP traps.

4. Click **Save**.

Example of adding an alert

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

- Alert name: Test
- Resources: includes all volumes whose name contains “abc” and excludes all the volumes whose name contains “xyz”
- Events: includes all critical events
- 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 set the frequency to notify the user every 15 minutes. You can configure an alert to repeatedly send notification to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.

7. 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 database backup schedules. You can also 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.
- Ensure that JBoss user has write permissions to the backup directory.

Steps

1. Click **Administration > Database Backup**.
2. In the **Backup and Restore** page, click **Actions > Database Backup Settings**.
3. 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.
4. Select **Schedule Frequency**.
5. In the Backup Schedule section, specify a daily or weekly schedule.

   Daily

   If you select this option, you should 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 should 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.
6. Click **Save and Close**.

Restoring a database backup on Windows

In case of dataloss 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 using the restore commands available in Unified Manager.

Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- You must have installed and configured Unified Manager
- A backup of Unified Manager must already exist in the system, in which you are performing the restore operation.
- The backup file must of `7z` type.

Steps

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

um cli login-u*maint_username*

.

2. In 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_6.3.N150418.2300_backup_windows_04-20-2015-02-51.7z

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

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

Changing the maintenance user password

In case, if you want to change the maintenance user password in Unified Manager, you can do so using the following procedure.

Before you begin

- You must have installed Unified Manager on Windows.
- You must log in to Windows with administrator privileges.

Steps

1. Log in as an administrator to the target Windows system on which Unified Manager is running.
2. Click Forgot Password

   An email with a link to reset your password is sent to your email address
3. Click reset password link in the email
4. Enter the new password and login to Unified Manager web UI.

   If Unified Manager is installed in a VCS environment, then you must change the maintenance user password on both nodes of the VCS setup. The maintenance user password for both nodes must be same.

Generating and sending support bundle

For the purpose of generating a package of data that can be used for storage domain troubleshooting, Unified Manager enables you to generate a zipped support bundle. If you install Unified Manager on Windows, you can generate this bundle through a command line.

Before you begin

You must log in to Windows operating system with administrator privileges.

About this task

You usually perform this task at the request of technical support.

Steps

1. Log in with administrator privilege to Windows operating system on which you have installed Unified Manager.
2. At the command line navigate to the *`Application_install_directory`*`\ocum\bin\` folder and run :

   `supportbundle.bat`

   The support bundle compiles support files and bundles those files into a zipped package. When the process is finished, a message is displayed similar to the following:

   ```
   Support bundle saved to C:\ProgramData\NetApp\OnCommandAppData
   \ocum\support\support_bundle_20150722_095835_324.7z
   ```

Upgrading to Unified Manager 6.3 from Unified Manager 6.3 on Windows

You can upgrade from Unified Manager 6.3 RC1 to Unified Manager 6.3 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 for 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.

Steps

1. Log in to the the NetApp Support Site at *mysupport.netapp.com* and navigate to the Software Download page.
2. Download the Unified Manager 6.3 Windows installation file to a target directory in the Windows system.
3. If Unified Manager is configured for high-availability, then using the Microsoft Cluster Server, stop all Unified Manager services on the first node.
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. Enter Y in the MySQL console pop-up window to continue the MySQL upgrade.

   When you upgrade MySQL, you must enter Y in the MySQL console pop-up, this is applicable for both unattended and interactive install.

8. Stop all Unified Manager services on the second node using Microsoft Cluster Server.
9. Switch the service group to the second node in the high-availability setup.
10. Upgrade Unified Manager on the second node.
11. Start all the Unified Manager services using Microsoft Cluster Server on both the nodes.
12. In the command prompt, enter **Y** to continue, or enter any other character to abort.

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

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

Setting up a connection between OnCommand Workflow Automation and Unified Manager

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

Before you begin

You must have installed Unified Manager.

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

You must have the OnCommand Administrator or Storage Administrator role.

Steps

1. Create a database user on page 32
   You can create a database user to begin pairing Workflow Automation with Unified Manager.
2. Set up Workflow Automation in Unified Manager on page 33
   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

If you are...	Choose this role
Accessing report-specific database views	Report Schema

6. Click **Add**.

Setting up a connection between OnCommand Workflow Automation and Unified Manager

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

Before you begin

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

Steps

1. Click **Administration > Setup Options**.
2. In the **Setup Options** dialog box, click **Add-ons > Workflow Automation**.
3. In the **Unified Manager Database User** area of the **Set Up OnCommand Workflow Automation** dialog box, select the name and enter the password for the database user that you created to support Unified Manager and OnCommand Workflow Automation connections.
4. In the **Workflow Automation Credentials** area of **Set Up OnCommand Workflow Automation** dialog box, type the host name or IP address (IPv4 or IPv6) and user name and password for the OnCommand Workflow Automation setup.

   You must use Unified Manager server port 443.
5. Click **Save and Close**.
6. If you use a self-signed certificate, click **Yes** to authorize the security certificate.

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

Uninstalling Unified Manager

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.

You must have downloaded and installed Unified Manager on your system.

Steps

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

Option	Steps
If you want to uninstall Unified Manager from the programs and features wizard	**a.** Navigate to **Control Panel** > **Program and Features**. **b.** Select OnCommand Unified Manager, and click **Uninstall**.
If you want to uninstall Unified Manager from the 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.

After you uninstall Unified Manager, application generated data and MySQL databases created by Unified Manager will not be deleted. For more information, see *Installing Unified Manager on Windows* on page 10

3. Uninstall the following third-party packages and data because they are not removed during the 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

Command-line interface commands not working on Windows

In some of the Windows servers, after you install Unified Manager, you cannot run commands from any path from the command line without specifying the full path of the Unified Manager `bin` directory.

Steps

1. Log in to the Windows command-line interface as an administrator.
2. Navigate to the `bin` directory of Unified Manager and perform one the following steps:
   - If you select the default install directory, example `C:\Program Files \NetApp\` run the cli command from `C:\Program Files \NetApp\ocum\bin`
   - If you select the custom install directory, example: `C:\SW_UM\` run the cli commands from `C:\SW_UM\NetApp\ocum\bin\`
3. Perform a new installation of Unified Manager.
4. Log off and log in to Unified Manager and run the CLI commands from any path.

Copyright information

Trademark information

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 to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

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

You can also contact us in the following ways:

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

Index

A

Active Directory
  using to enable remote authentication *18*
adding
  alerts *26*
  authentication servers *20*
  clusters *25*
aggregates
  configuring global threshold values for *22*
alerts
  adding *26*
  configuring your environment for *17*
  creating *26*
authentication
  adding servers *20*
  testing for remote users and groups *21*
authentication, remote
  disabling nested groups *19*
  enabling *18*

B

backups
  configuring database settings *28*
  restoring database on Windows *28*
browsers
  requirements for installation *6*

C

changing
  maintenance user password *29*
clustered Data ONTAP systems
  See clusters
clusters
  adding *25*
  viewing discovery status *25*
commands
  cli commands not working from any path *35*
comments
  how to send feedback about documentation *38*
configuration options
  after initial software setup *17*
  after installing Unified Manager *17*
configuring
  aggregate global threshold values *22*
  database backup settings *28*
  notification settings *18*
  thresholds *22*
  Unified Manager using scripts *14*
  volume global threshold values *23*
connection setup
  between Unified Manager and Workflow Automation *32*
creating
  alerts *26*

D

database user roles
  Integration Schema, Report Schema *32*
database users
  creating *24*, *32*
databases
  configuring backup settings *28*
  restoring backup on Windows *28*
disabling
  Use secure connection *20*
discovery
  viewing the status of clusters *25*
documentation
  how to receive automatic notification of changes to *38*
  how to send feedback about *38*

E

editing
  unmanaged relationship lag threshold settings *23*
enabling
  Use secure connection *20*

F

Failover Cluster
  configuration requirements *13*
Failover Cluster Manager
  setting up Unified Manager using scripts *14*
failover clustering
  requirements for configuring Unified Manager *13*
feedback
  how to send comments about documentation *38*

G

groups
  testing remote authentication *21*
groups, nested
  disabling remote authentication of *19*

H

high availability
  installing Unified Manager in MSCS *14*
  MSCS, in Unified Manager *13*
  setting up Unified Manager in Failover Cluster Manager *14*

I

information
  how to send feedback about improving documentation *38*
installation

Unified Manager on Windows, troubleshooting issues *35*
installing
Unified Manager *8*
Unified Manager in MSCS *14*
Unified Manager on Windows *10*
Unified Manager, prerequisites *8*
Unified Manager, unattended installation *11*

L

lag threshold settings
editing for unmanaged relationships *23*
local users
creating *24*

M

minimum requirements
hardware *6*
software *6*
modifying
unmanaged relationship lag threshold settings *23*
MSCS
configuring for Unified Manager *13*
installing Unified Manager in *14*

N

nested groups
disabling remote authentication of *19*
notification
adding alerts *26*
configuring settings *18*

O

OnCommand Administrator user role
enabling configuration *17*
OnCommand Workflow Automation
setting up a connection with Unified Manager *32*
setting up connection with Unified Manager *33*
Open LDAP
using to enable remote authentication *18*
options, configuration
after initial software setup *17*

P

physical storage
adding clusters *25*
platforms
requirements for installation *6*
prerequisites
for installing Unified Manager *8*

R

relationships, unmanaged
editing lag thresholds settings for *23*
remote authentication
disabling nested groups *19*
enabling *18*
remote groups
adding *24*
testing authentication *21*
remote users
adding *24*
testing authentication *21*
reports
creating a database user with the Report Schema role *32*
requirements
for configuring Unified Manager in Failover Cluster *13*
for installing Unified Manager *8*
minimum hardware and software *6*
restoring
database backup on Windows *28*
roles
assigning to users *24*

S

scripts
using to set up Unified Manager in Failover Cluster Manager *14*
setting up
aggregate global threshold values *22*
notification settings *18*
SMTP server *18*
SNMP *18*
thresholds *22*
volume global threshold values *23*
settings, lag threshold
editing for unmanaged relationships *23*
silent installation
See unattended installation
suggestions
how to send feedback about documentation *38*
support bundles
generating in Windows *29*
supported
browsers and platforms *6*
protocol and ports *6*

T

testing
authentication for remote users and groups *21*
threshold settings, lag
editing for unmanaged relationships *23*
thresholds
configuring *22*
global values for aggregates *22*
global values for volumes *23*
troubleshooting
Unified Manager installation issues *35*
Troubleshooting
command line interface *35*
twitter
how to receive automatic notification of documentation changes *38*

U

unattended installation
Unified Manager *11*
unattended uninstallation
uninstalling Unified Manager using command line *34*
Unified Manager
configuring for high availability *13*
configuring using scripts in Failover Cluster Manager *14*
failover clustering configuration requirements *13*
installation and setup tasks *5*
installing *8*
installing in MSCS *14*
installing on Windows *10*
performing an unattended installation *11*
prerequisites for installing *8*
uninstalling from Windows *34*
upgrading from 6.3 to 6.3 *30*
uninstalling
Unified Manager from Windows *34*
unmanaged relationships
editing lag thresholds settings for *23*
upgrading
to Unified Manager 6.3 *30*
Use secure connection
enabling or disabling *20*
user roles
assigning *24*
users
adding *24*
creating *24*
testing remote authentication *21*
users, database
creating *32*

V

viewing
discovery status of clusters *25*
volumes
configuring global threshold values for *23*

W

Windows
how Unified Manager works on *5*
installing Unified Manager *10*
restoring database backup *28*
troubleshooting Unified Manager installation issues *35*
upgrading to Unified Manager 6.3 from 6.3 *30*
Workflow Automation
creating a database user with the Integration Schema role *32*
setting up a connection with Unified Manager *32*
setting up connection with Unified Manager *33*