Active IQ® Unified Manager 9.6

Installation Guide

For Microsoft® Windows®

November 2020 | 215-14505_2020-11_en-us
doccomments@netapp.com

NetApp®

Contents

Introduction to Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) enables you to monitor and manage the health and performance of your ONTAP storage systems from a single interface. You can deploy Unified Manager on a Linux server, on a Windows server, or as a virtual appliance on a VMware host.

After you have completed the installation and have added the clusters that you want to manage, Unified Manager provides a graphical interface that displays the capacity, availability, protection, and performance status of the monitored storage systems.

Related information

NetApp Interoperability Matrix Tool

What the Unified Manager server does

The Unified Manager server infrastructure consists of a data collection unit, a database, and an application server. It provides infrastructure services such as discovery, monitoring, role-based access control (RBAC), auditing, and logging.

Unified Manager collects cluster information, stores the data in the database, and analyzes the data to see if there are any cluster issues.

Active IQ Unified Manager product documentation

Active IQ Unified Manager is accompanied by a set of guides that describe how to install and use the product. Online help is also provided in the user interface.

Active IQ Unified Manager Installation Guide

Provides installation, upgrade, and setup instructions for Unified Manager on the VMware, Linux, and Windows platforms.

Active IQ Unified Manager System Configuration Guide

Provides initial setup and configuration instructions for Unified Manager. This includes adding clusters, adding users, configuring alerts, and setting up remote authentication.

Active IQ Unified Manager Workflow Guide for Managing Cluster Health

Provides information about using Unified Manager to manage and troubleshoot cluster storage health issues. This guide also describes how to use the Unified Manager maintenance console to perform special operations such as restoring a database backup and connecting to an external data provider to offload performance statistics.

Active IQ Unified Manager Workflow Guide for Managing Cluster Performance

Provides information about using Unified Manager to manage and troubleshoot cluster storage performance issues. This includes identifying workloads that are overusing cluster components so that you can take corrective action to bring performance back to normal levels of operation.

Active IQ Unified Manager Reporting Guide

Provides information about using Unified Manager to create custom reports about the capacity, health, performance, and protection status of your ONTAP storage objects. This includes scheduling the report for delivery to specified users on a regular schedule through email.

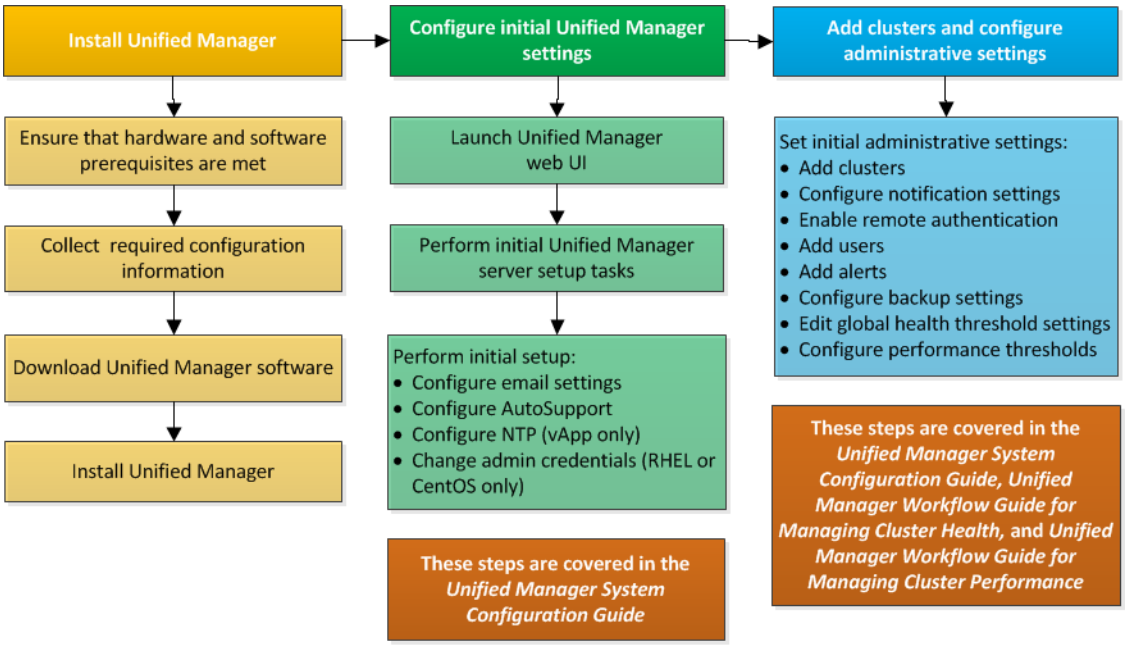
Active IQ Unified Manager Online Help

Provides information about using Unified Manager to manage and troubleshoot cluster storage health and performance issues. Additionally, it provides field level descriptions for every UI page in the product. The online help is included with the software, and is also available as a PDF document that you can review offline.

Overview of the installation sequence

The installation workflow describes the tasks that you must perform before you can use Unified Manager.

The chapters of this installation guide describe each of the items shown in the workflow below.



Requirements for installing Unified Manager

Before you begin the installation process, ensure that the server on which you want to install Unified Manager meets the specific software, hardware, CPU, and memory requirements.

NetApp does not support any modification of the Unified Manager application code. If you need to apply any security measures to the Unified Manager server, you should make those changes to the operating system on which Unified Manager is installed.

For more details about applying security measures to the Unified Manager server, see the Knowledge Base article.

Supportability for Security Measures applied to Active IQ Unified Manager for Clustered Data ONTAP

Related information

NetApp Interoperability Matrix Tool

Virtual infrastructure and hardware system requirements

Depending on whether you are installing Unified Manager on virtual infrastructure or on a physical system, it must meet minimum requirements for memory, CPU, and disk space.

The following table displays the values that are recommended for memory, CPU, and disk space resources. These values have been qualified so that Unified Manager meets acceptable performance levels.

Hardware configuration	Recommended settings
RAM	12 GB (minimum requirement 8 GB)
Processors	4 CPUs
CPU cycle capacity	9572 MHz total (minimum requirement 9572 MHz)
Free disk space	150 GB, where the capacity is allocated as follows: • 100 GB of disk space for the installation directory • 50 GB of disk space for the MySQL data directory

Unified Manager can be installed on systems with a small amount of memory, but the recommended 12 GB of RAM ensures that enough memory is available for optimal performance, and so that the system can accommodate additional clusters and storage objects as your configuration grows. You must not set any memory limits on the VM where Unified Manager is deployed, and you must not enable any features (for example, ballooning) that hinder the software from utilizing the allocated memory on the system.

Additionally, there is a limit to the number of nodes that a single instance of Unified Manager can monitor before you need to install a second instance of Unified Manager. See the *Best Practices Guide* for more details.

Technical Report 4621: Unified Manager Best Practices Guide

Memory-page swapping negatively impacts the performance of the system and the management application. Competing for CPU resources that are unavailable because of overall host utilization can degrade performance.

Dedicated use requirement

The physical or virtual system on which you install Unified Manager must be used exclusively for Unified Manager and must not be shared with other applications. Other applications might consume system resources and can drastically reduce the performance of Unified Manager.

Space requirements for backups

If you plan to use the Unified Manager backup and restore feature, you must allocate additional capacity so that the "data" directory or disk has 150 GB of space. A backup can be written to a local destination or to a remote destination. The best practice is to identify a remote location that is external to the Unified Manager host system that has a minimum of 150 GB of space.

Host connectivity requirements

The physical system or virtual system on which you install Unified Manager must be configured in such a way that you can successfully `ping` the host name from the host itself. In case of IPv6 configuration, you should verify that `ping6` to the host name is successful to ensure that the Unified Manager installation succeeds.

You can use the host name (or the host IP address) to access the product web UI. If you configured a static IP address for your network during deployment, then you designated a name for the network host. If you configured the network using DHCP, you should obtain the host name from the DNS.

If you plan to allow users to access Unified Manager by using the short name instead of using the fully qualified domain name (FQDN) or IP address, then your network configuration has to resolve this short name to a valid FQDN.

Windows software and installation requirements

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

Operating system software

Third-party software

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 2016 Standard and Datacenter Edition
- Microsoft Windows Server 2019 Standard and Datacenter Edition

Note that Windows Server 2012 is not supported as it was in earlier releases. See the Interoperability Matrix for the complete and most current list of supported Windows versions.

mysupport.netapp.com/matrix

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

The following third-party packages are required:

- Microsoft Visual C++ 2015 Redistributable package version 14.0.24212
- Microsoft Visual C++ Redistributable Packages for Visual Studio 2013 version 12.0.40660
- MySQL Community Edition version 5.7.26, or later versions in the 5.7 family
- OpenJDK version 11.0.3
- p7zip version 18.05 or later

If these third-party packages are not installed, Unified Manager installs them as part of the installation.

Note: Starting with Unified Manager 9.5, OpenJDK is provided in the Unified Manager installation package and installed automatically. Oracle Java is not supported starting with Unified Manager 9.5.

If MySQL is pre-installed, you must ensure that:

- It is using the default port.
- The sample databases are not installed.
- The service name is "MYSQL".

Note: If you plan to upgrade any of the third-party software after Unified Manager has been running, you must shut down Unified Manager first. After the third-party software installation is complete you can restart Unified Manager.

Installation requirements

- Microsoft .NET 4.5.2, or greater, must be installed.
- 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.
- 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.
- You must disable Microsoft IIS worldwide web publishing service and ensure that ports 80 and 443 are free.
- You must make sure that the Remote Desktop Session Host setting for "Windows Installer RDS Compatibility" is disabled during the installation.
- UDP port 514 must be free, and must not be used by any other service.

Note: The Unified Manager installation program configures the following exclusions in Windows Defender:

- Unified Manager data directory
- Unified Manager installation directory
- MySQL data directory

If your server has a different antivirus scanner installed you must configure these exclusions manually.

Supported browsers

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

Unified Manager has been tested with the following browsers; other browsers might work but have not been qualified. See the Interoperability Matrix for the complete list of supported browser versions.

mysupport.netapp.com/matrix

- Mozilla Firefox ESR 60
- Google Chrome version 72 and 73

Note: Microsoft Internet Explorer is no longer supported.

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

If you are planning to configure Unified Manager for SAML authentication so that an identity provider (IdP) authenticates users, check the list of browsers supported by the IdP as well.

Protocol and port requirements

Using a browser, API client, or SSH, the required ports must be accessible to the Unified Manager UI and APIs. The required ports and protocols enable communication between the Unified Manager server and the managed storage systems, servers, and other components.

Connections to the Unified Manager server

In typical installations you do not have to specify port numbers when connecting to the Unified Manager web UI, because default ports are always used. For example, because Unified Manager always attempts to run on its default port, you can enter `https://<host>` instead of `https://<host>:443`.

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

Interface	Protocol	Port	Description
Unified Manager web UI	HTTP	80	Used to access the Unified Manager web UI; automatically redirects to the secure port 443.
Unified Manager web UI and programs using APIs	HTTPS	443	Used to securely access the Unified Manager web UI or to make API calls; API calls can only be made using HTTPS.
Maintenance console	SSH/SFTP	22	Used to access the maintenance console and retrieve support bundles.
Linux command line	SSH/SFTP	22	Used to access the Red Hat Enterprise Linux or CentOS command line and retrieve support bundles.
MySQL database	MySQL	3306	Used to enable OnCommand Workflow Automation and OnCommand API Services access to Unified Manager.
Syslog	UDP	514	Used to access subscription-based EMS messages from ONTAP systems and to create events based on the messages.
REST	HTTPS	9443	Used to access realtime REST API-based EMS events from authenticated ONTAP systems.

Note: The ports used for HTTP and HTTPS communication (ports 80 and 443) can be changed using the Unified Manager maintenance console. See the *Active IQ Unified Manager System Configuration Guide* for more information.

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/TCP	Used to monitor and manage storage systems.
Storage system	NDMP	10000/TCP	Used for certain Snapshot restore operations.
AutoSupport server	HTTPS	443	Used to send AutoSupport information. Requires Internet access to perform this function.

Destination	Protocol	Port	Description
Authentication server	LDAP	389	Used to make authentication requests, and user and group lookup requests.
	LDAPS	636	Used for secure LDAP communication.
Mail server	SMTP	25	Used to send alert notification emails.
SNMP trap sender	SNMPv1 or SNMPv3	162/UDP	Used to send alert notification SNMP traps.
External data provider server	TCP	2003	Used to send performance data to an external data provider, such as Graphite.
NTP server	NTP	123/UDP	Used to synchronize the time on the Unified Manager server with an external NTP time server. (VMware systems only)

Completing the worksheet

Before you install and configure Unified Manager, you should have specific information about your environment readily available. You can record the information in the worksheet.

Unified Manager installation information

The details required to install Unified Manager.

System on which software is deployed	Your value
Host fully qualified domain name	
Host IP address	
Network mask	
Gateway IP address	
Primary DNS address	
Secondary DNS address	
Search domains	
Maintenance user name	
Maintenance user password	

Unified Manager configuration information

The details to configure Unified Manager after installation. Some values are optional depending on your configuration.

Setting	Your value
Maintenance user email address	
SMTP server host name or IP address	
SMTP user name	
SMTP password	
SMTP port	25 (Default value)
Email from which alert notifications are sent	

Setting	Your value
Authentication server host name or IP address	
Active Directory administrator name or LDAP bind distinguished name	
Active Directory password or LDAP bind password	
Authentication server base distinguished name	
Identity provider (IdP) URL	
Identity provider (IdP) metadata	
SNMP trap destination host IP addresses	
SNMP port	

Cluster information

The details for the storage systems that you will manage using Unified Manager.

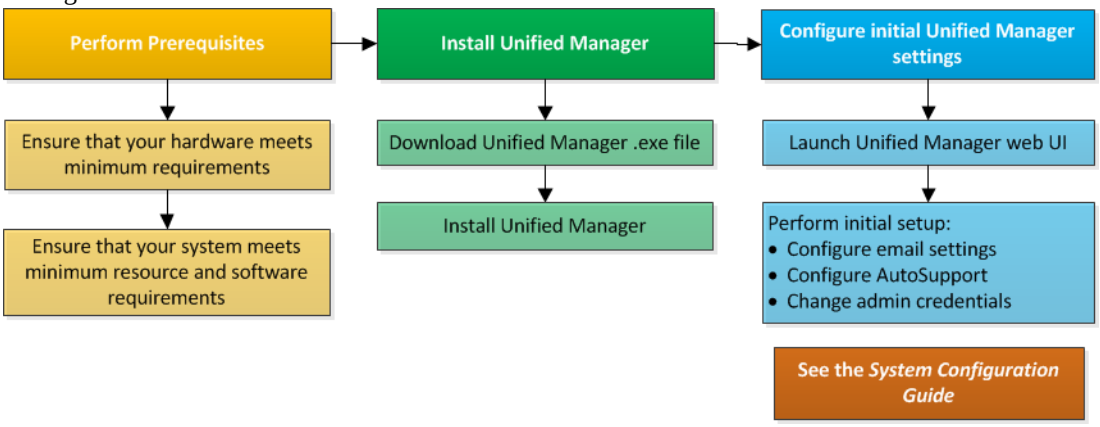
Cluster 1 of N	Your value
Host name or cluster-management IP address	
ONTAP administrator user name **Note:** The administrator must have been assigned the "admin" role.	
ONTAP administrator password	
Protocol (HTTP or HTTPS)	

Installing, upgrading, and removing Unified Manager software

You can install Unified Manager software, upgrade to a newer version of software, or remove the Unified Manager application.

Overview of the installation process

The installation workflow describes the tasks that you must perform before you can use Unified Manager.



Installing Unified Manager on Windows

It is important that you understand the sequence of steps to download and install Unified Manager on Windows. Before you install Unified Manager on Windows, you can decide if you want to configure Unified Manager for high availability.

Installing Unified Manager

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

Before you begin

- The system on which you plan to install Unified Manager must meet the system and software requirements.
  Hardware system requirements
  Windows software and installation requirements

  Note: Starting with Unified Manager 9.5, OpenJDK is provided in the installation package and installed automatically. Oracle Java is not supported starting with Unified Manager 9.5.
- You must have Windows administrator privileges.
- You must have a supported web browser.
- The Unified Manager maintenance user password must be between 8 and 20 characters, must contain upper-case letters or lower-case letters, numerals, and special characters.
- The following special characters are not allowed in the password string for the maintenance user or for the MySQL root user: " ' ` % , = & < > | ^ \ / ( ) [ ] ;
  The following special characters are allowed: ~ ! @ # $ * - ? . : + { }

Steps

1. Log in to Windows using the default local administrator account.
2. Log in to the NetApp Support Site, and locate the Download page for installing Unified Manager on the Windows platform.
3. Download the Unified Manager Windows installation file from the NetApp Support Site to a target directory in the Windows system.
4. Navigate to the directory where the installation file is located.
5. 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.
6. Click **Next**.
7. Enter the user name and password to create the maintenance user.
8. In the **Database Connection** wizard, enter the MySQL root password.
9. 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.
10. Click **Next**.
11. In the **Ready to Install Shield** wizard, click **Install**.
12. After the installation is complete, click **Finish**.

Result

The installation creates multiple 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\MySQLServerData\`
- Java directory

  This is the directory where OpenJDK will be installed. Example: `C:\Program Files\NetApp\JDK\`
- 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\`

After you finish

You can access the web UI to perform the initial setup of Unified Manager, as described in the *Active IQ Unified Manager System Configuration Guide*.

Performing an unattended installation of Unified Manager

You can install Unified Manager 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	**`ActiveIQUnifiedManager-x.y.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:** **`ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:\ProgramData\MYSQL\MySQLServer\" MAINTENANCE_PASSWORD=******* MAINTENANCE_USERNAME=admin /qn /l*v C:\install.log"`**
If third-party packages are not installed	**`ActiveIQUnifiedManager-x.y.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:** **`ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:\ProgramData\MYSQL\MySQLServer\" 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 mode with no user interface. 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 the same version of Microsoft Windows Server.
- 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 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 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 role in Windows 2016 or Windows 2019 using Failover Cluster Manager:
   a. Launch Failover Cluster Manager.
   b. Create the empty role by clicking **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 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`

   `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, 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 command `perl ha_setup.pl --join -t mscs -f shared_location_path` on the second node of the cluster to point to the Unified Manager server data to the LUN.

   `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.

    a. In the toolbar, click  , and then click **HTTPS Certificate** from the **Setup** menu.
    b. Click **Regenerate HTTPS Certificate**.

    The regenerated certificate provides the cluster IP address, not the fully qualified domain name (FQDN). You must use the global IP address to set up Unified Manager for high-availability.
12. Access the Unified Manager UI using the following link:

    `https://<FQDN of Global IP>`

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.

Changing the JBoss password

You can create a new, custom JBoss password to overwrite the default password that is set during installation. This task is optional, but some sites might require this security capability to override the Unified Manager installation default setting. This operation also changes the password JBoss uses to access MySQL.

Before you begin

- You must have Windows admin privileges for the system on which Unified Manager is installed.
- You must have the password for the MySQL root user.
- You must be able to access the NetApp-provided `password.bat` script in the directory `\Program Files\NetApp\essentials\bin`.

Steps

1. Log in as the admin user on the Unified Manager host machine.
2. Use the Windows Services console to stop the following Unified Manager services:
   - NetApp Active IQ Acquisition Service (Ocie-au)
   - NetApp Active IQ Management Server Service (Oncommandsvc)
3. Launch the `password.bat` script to begin the password change process:

   `C:\Program Files\NetApp\essentials\bin> password.bat resetJBossPassword`
4. When prompted, enter the MySQL root user password.
5. When prompted, enter the current JBoss user password.

   The default password is `D11h1aMu@79%`.
6. When prompted, enter the new JBoss user password, and then enter it again for confirmation.

Confirmation messages appear as the changes are made, and then you are prompted one last time for the new JBoss user password.

7. Enter the new JBoss user password one more time.
8. When the script completes, start the Unified Manager services by using the Windows Services console:
   - NetApp Active IQ Management Server Service (Oncommandsvc)
   - NetApp Active IQ Acquisition Service (Ocie-au)
9. After all of the services are started, you can log in to the Unified Manager UI.

Upgrading Unified Manager

You can upgrade Unified Manager 9.4 or 9.5 to 9.6 by downloading and running the installation file on the Windows platform.

Before you begin

- The system on which you are upgrading Unified Manager must meet the system and software requirements.
  Hardware system requirements
  Windows software and installation requirements

  Note: Starting with Unified Manager 9.5, OpenJDK is provided in the installation package and installed automatically. Oracle Java is not supported starting with Unified Manager 9.5.

  Note: Starting with Unified Manager 9.4, Microsoft .NET 4.5.2 or greater is required. Make sure you have the correct version of .NET installed before starting the upgrade.
- You must have Windows administrator privileges.
- You must have valid credentials to log in to the NetApp Support Site.
- To avoid data loss, you must have created a backup of the Unified Manager machine in case there is an issue during the upgrade.
- You must have adequate disk space available to perform the upgrade.
  The available space on the installation drive must be 2.5 GB larger than the size of the data directory. The upgrade will stop and display an error message indicating the amount of space to be added if there is not enough free space.

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 must disconnect the two products and then set up a new Workflow Automation connection after performing the upgrades. If you are performing an upgrade to only one of the products, then you should log into Workflow Automation after the upgrade and verify that it is still acquiring data from Unified Manager.

Steps

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

   ```
   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 (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.

    ```
    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:

```
ActiveIQUnifiedManager-9.6.exe /s /v"MYSQL_PASSWORD=netapp21! /qn /l*v C:\install.log
```

Upgrading third-party products

You can upgrade third-party products, such as JRE and MySQL, on Unified Manager when installed on Windows systems.

The companies that develop these third-party products report security vulnerabilities on a regular basis. You can upgrade to newer versions of this software at your own schedule.

Upgrading JRE

You can upgrade to a newer version of Java Runtime Environment (JRE) on the Windows server on which Unified Manager is installed to obtain fixes for security vulnerabilities.

Before you begin

You must have Windows admin privileges for the system on which Unified Manager is installed.

Steps

1. Log in as the admin user on the Unified Manager host machine.
2. Download the appropriate version of Java (64-bit) from the JDK site to the target system.

For example, download `openjdk-11_windows-x64_bin.zip` from `http://jdk.java.net/11/`.

3. Use the Windows Services console to stop the following Unified Manager services:
   - NetApp Active IQ Acquisition Service (Ocie-au)
   - NetApp Active IQ Management Server Service (Oncommandsvc)
4. Expand the `zip` file.
5. Copy the directories and files from the resulting `jdk` directory (for example, `jdk-11.0.2` to the location where Java is installed. Example: `C:\Program Files\NetApp\JDK\`
6. Start the Unified Manager services by using the Windows Services console:
   - NetApp Active IQ Management Server Service (Oncommandsvc)
   - NetApp Active IQ Acquisition Service (Ocie-au)

Upgrading MySQL

You can upgrade to a newer version of MySQL on the Windows server on which Unified Manager is installed to obtain fixes for security vulnerabilities.

Before you begin

- You must have Windows admin privileges for the system on which Unified Manager is installed.
- You must have the password for the MySQL root user.

Steps

1. Log in as the admin user on the Unified Manager host machine.
2. Download the appropriate version of MySQL to the target system.
3. Use the Windows Services console to stop the following Unified Manager services:
   - NetApp Active IQ Acquisition Service (Ocie-au)
   - NetApp Active IQ Management Server Service (Oncommandsvc)
   - MYSQL
4. Click the `.msi` package to invoke the upgrade of MySQL and follow the instructions on the screen to complete the upgrade.
5. Start the Unified Manager services by using the Windows Services console:
   - MYSQL
   - NetApp Active IQ Management Server Service (Oncommandsvc)
   - NetApp Active IQ Acquisition Service (Ocie-au)

Restarting Unified Manager

You might have to restart Unified Manager after making configuration changes.

Before you begin

You must have Windows administrator privileges.

Steps

1. Log in to Windows using the default local administrator account.
2. Stop the Unified Manager services:

From the...	Stop the services in following order...
Command line	**a.** `sc stop ocie-au` **b.** `sc stop Oncommandsvc`
Microsoft Service Manager	**a.** NetApp Active IQ Acquisition Service (Ocie-au) **b.** NetApp Active IQ Management Server Service (Oncommandsvc)

When installed in a high-availability setup, stop the Unified Manager service by using either Microsoft Service Manager or the command line.

3. Start the Unified Manager services:

From the...	Start the services in following order...
Command line	**a.** `sc start Oncommandsvc` **b.** `sc start ocie-au`
Microsoft Service Manager	**a.** NetApp Active IQ Management Server Service (Oncommandsvc) **b.** NetApp Active IQ Acquisition Service (Ocie-au)

When installed in a high-availability setup, start Unified Manager service by using either Microsoft Service Manager or the command line.

Uninstalling Unified Manager

You can uninstall Unified Manager 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. When installed in a high-availability setup, remove the HA service group resources and delete the HA service group before uninstalling Unified Manager from both nodes.
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 Active IQ Unified Manager, and click **Uninstall**.
Command line	**a.** Log in to the Windows command line using administrator privileges. **b.** Navigate to the Active IQ Unified Manager directory, and run the following command: `msiexec /x {A78760DB-7EC0-4305-97DB-E4A89CDFF4E1} /qn /l*v %systemdrive%\UmUnInstall.log`

If User Account Control (UAC) is enabled on the server, and you are logged in as a domain user, you must use the command-line uninstallation method.

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, Microsoft Visual C++ 2015 Redistributable, and 7zip
   - MySQL application data generated by Unified Manager
   - Application logs and contents of application data directory

Copyright and trademark

Copyright

Trademark