Requirements for installing Unified Manager

OnCommand Unified Manager 9.5

NetApp
October 23, 2024

Table of Contents

Requirements for installing Unified Manager

Before you can install Unified Manager you must ensure that the server on which you plan to install Unified Manager meets specific software, hardware, CPU, and memory requirements.

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	VMware: • 5 GB (thin provisioned) • 152 GB (thick provisioned)
Red Hat or CentOS: 150 GB, where the capacity is allocated as follows: • 50 GB allotted to the root partition • 100 GB of free disk space allotted to the `/opt/netapp/data` directory, which is mounted on an LVM drive or on a separate local disk attached to the target system ⓘ The `/tmp` directory should have at least 10 GB of free space and the `/var/log` directory should have at least 16 GB of free space.	Windows: 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.

Mounted `/opt/netapp` or `/opt/netapp/data` requirements

You can mount `/opt/netapp` or `/opt/netapp/data` on an NAS or SAN device. Note that using remote mount points may cause scaling issues. If you do use a remote mount point, ensure that your SAN or NAS network has sufficient capacity to meet the I/O needs of Unified Manager. This capacity will vary and may increase based on the number of clusters and storage objects you are monitoring.

If you have mounted `/opt/netapp` or `/opt/netapp/data` from anywhere other that the root file system, and you have SELinux enabled in your environment, you must set the correct context for the mounted directories.

See the topic SELinux requirements for mounting /opt/netapp or /opt/netapp/data on an NFS or CIFS share for information about setting the correct SELinux context.

VMware software and installation requirements

The VMware vSphere system on which you install Unified Manager requires specific versions of the operating system and supporting software.

Operating system software

The following versions of VMware ESXi are supported:

- ESXi 5.5, 6.0, and 6.5

The following versions of vSphere are supported:

- VMware vCenter Server 5.5, 6.0, and 6.5

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

mysupport.netapp.com/matrix

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

Installation requirements

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

If you deploy an NFS datastore on a storage system that is running ONTAP software, you must use the NetApp NFS Plug-in for VMware VAAI to use thick provisioning.

If deployment fails using your High Availability-enabled environment because of insufficient resources, you may need to modify the Cluster Features Virtual Machine Options by disabling the VM Restart Priority, and leaving the Host Isolation Response powered on.

Red Hat Enterprise Linux and CentOS software and installation requirements

The Linux system on which you install Unified Manager requires specific versions of the operating system and supporting software.

Operating system software

The Linux system must have the following versions of the operating system and supporting software installed:

- Red Hat Enterprise Linux or CentOS 64-bit version 7.x

  Red Hat Enterprise Linux 6.x is not supported starting with Unified Manager 9.4.

See the Interoperability Matrix for the complete and most current list of supported Red Hat Enterprise Linux and CentOS versions.

mysupport.netapp.com/matrix

The following third-party packages are required:

- MySQL Community Edition version 5.7.23 or later versions in the 5.7 family (from the MySQL repository)
- OpenJDK version 11 (from the Red Hat Extra Enterprise Linux Server repository)

  ⓘ Oracle Java is not supported starting with Unified Manager 9.5.

- p7zip version 16.02 or later (from the Red Hat Extra Packages for Enterprise Linux repository)

ⓘ 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.

User authorization requirements

Installation of Unified Manager on a Red Hat Enterprise Linux system or CentOS system can be performed by the root user or by non-root users by using the `sudo` command.

Installation requirements

The best practices for installing Red Hat Enterprise Linux or CentOS and the associated repositories on your system are as follows:

- You must install Red Hat Enterprise Linux or CentOS according to Red Hat best practices, and you should select the following default options, which requires selecting “Server with GUI”.
- While installing Unified Manager on Red Hat Enterprise Linux or CentOS, the system must have access to the appropriate repository so that the installation program can access and install all the required software dependencies.
- For the `yum` installer to find dependent software in the Red Hat Enterprise Linux repositories, you must have registered the system during the Red Hat Enterprise Linux installation or afterwards by using a valid Red Hat subscription.

  See the Red Hat documentation for information about the Red Hat Subscription Manager.

- You must enable the Extra Packages for Enterprise Linux (EPEL) repository to successfully install the required third-party utilities on your system.

  If the EPEL repository is not configured on your system, you must manually download and configure the repository.

  Manually configuring the EPEL repository

- If the correct version of MySQL is not installed, you must enable the MySQL repository to successfully install MySQL software on your system.

  If the MySQL repository is not configured on your system, you must manually download and configure the repository.

  Manually configuring the MySQL repository

If your system does not have internet access, and the repositories are not mirrored from an internet-connected system to the unconnected system, you should follow the installation instructions to determine the external software dependencies of your system. Then you can download the required software to the internet-connected system, and copy the `.rpm` files to the system on which you plan to install Unified Manager. To download the artifacts and packages, you must use the `yum install` command. You must ensure that the two systems are running the same operating system version and that the subscription license is for the appropriate Red Hat Enterprise Linux or CentOS version.

> You must not install the required third-party software from repositories other than the repositories that are listed here. Software installed from the Red Hat repositories is designed explicitly for Red Hat Enterprise Linux, and conforms to Red Hat best practices (directory layouts, permissions, and so on). Software from other locations might not follow these guidelines, which might cause the Unified Manager installation to fail, or might cause issues with future upgrades.

Port 443 requirement

Generic images from Red Hat and CentOS block external access to port 443. If your browser is unable to connect to your OnCommand product, this may be the issue. The following command enables access to port 443 for all external users and applications: `# firewall-cmd -zone=public -add-port=443/tcp -permanent; firewall-cmd -reload`

Consult with your IT department prior to executing this command to see if your security policies require a different procedure.

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

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 2012 Standard and Datacenter Edition
- Microsoft Windows Server 2012 R2 Standard and Datacenter Edition
- Microsoft Windows Server 2016 Standard and Datacenter Edition

> On Windows Server 2012 R2, Windows update KB2919355 must be installed on the target system or the installation will fail.

Note that Windows Server 2008 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 5.7.23, or later versions in the 5.7 family
- OpenJDK version 11
- p7zip version 18.01 or later

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

> 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”.

> 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.

> The Unified Manager installation program configures the following exclusions in Windows Defender:
>
> - Unified Manager data directory (Windows Server 2016 only)
> - 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 68 and 69
- Microsoft Internet Explorer 11

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

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

> ⓘ Firefox and Chrome are the preferred browsers as there have been some cases where complex UI pages load more slowly when using Internet Explorer.

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

You do not have to specify port numbers when connecting to the Unified Manager web UI, because default ports are always used. For example, because Unified Manager always runs on its default port, you can enter `https://<host>` instead of `https://<host>:443`. The default port numbers cannot be changed.

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

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

Interface	Protocol	Port	Description
Unified Manager web UI and programs using APIs	HTTPS	443	Used to securely access the Unified Manager web UI or to make API calls; API calls can only be made using HTTPS.
Maintenance console	SSH/SFTP	22	Used to access the maintenance console and retrieve support bundles.
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.

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.
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

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
ESXi server IP address (VMware only)	
Host fully qualified domain name	

System on which software is deployed	Your value
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	
NTP server (VMware only)	
SMTP server host name or IP address	
SMTP user name	
SMTP password	
SMTP port	25 (Default value)
Email from which alert notifications are sent	
Authentication server host name or IP address	
Active Directory administrator name or LDAP bind distinguished name	
Active Directory password or LDAP bind password	

Setting	Your value
Authentication server base distinguished name	
Identity provider (IdP) URL	
Identity provider (IdP) metadata	
SNMP trap destination host IP address	
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 ⓘ The administrator must have been assigned the “admin” role.	
ONTAP administrator password	
Protocol (HTTP or HTTPS)	