OnCommand® Unified Manager

Installation and Setup Guide

For Use with Core Package 5.2.1

January 2017 | 215-09127_D0
doccomments@netapp.com

NetApp®

Contents

Overview of OnCommand Unified Manager manageability software components

OnCommand Unified Manager Core Package provides backup and restore capabilities, monitoring, and provisioning for a storage environment. OnCommand Unified Manager Core Package brings together multiple products, including Operations Manager, protection capabilities, and provisioning capabilities, into a single framework that provides an integrated, policy-based data and storage management.

OnCommand Unified Manager 5.1 and later supports Data ONTAP operating in 7-Mode environments or clustered environments. However, OnCommand Unified Manager 5.1 or later does not support management of both modes from the same OnCommand Unified Manager instance. During the OnCommand Unified Manager installation process, you are prompted to select either a 7-Mode environment or a clustered environment.

Note: NetApp has announced the end of availability of OnCommand Unified Manager Host Package. However, the Online Help and other documents include references to OnCommand Unified Manager Host Package. For more information, see *bulletin*.

Core Package installation and configuration checklists

It is helpful to use checklists to verify that you have completed each task in the installation and configuration process, including reviewing system requirements; downloading and installing a variety of software.

Plan for, download, and install the software

This checklist provides an overview of the installation process for OnCommand Unified Manager Core Package.

1. *Review the system requirements* on page 10.
    - Browser requirements
    - License requirements
    - Network storage requirements
    - Core Package hardware and software requirements
2. *Download the OnCommand Core Package software* on page 21.
3. *Download the Host Agent software* on page 13.
4. *Download the Open Systems SnapVault software* on page 13.
5. Install the Core Package software: *Windows* on page 22, *Linux,* on page 24 or *by script* on page 26.
6. *Install the Host Agent software* on page 13.
7. *Install the Open Systems SnapVault software* on page 13.

OnCommand Unified Manager Core Package architecture

OnCommand Unified Manager Core Package includes interaction among front-end user interfaces (such as the OnCommand console, the NetApp Management Console, and the Operations Manager console) and back-end servers or services (such as the OnCommand Unified Manager server and storage systems).

You can use the Operations Manager console and the NetApp Management Console to manage your physical environment.

Related concepts

Contents of the OnCommand Unified Manager Core Package on page 8

Contents of the OnCommand Unified Manager Core Package

Understanding what components compose the OnCommand Unified Manager Core Package and what these components enable you to do helps you determine which components you want to enable during the installation and setup process.

Components installed with the OnCommand Unified Manager Core Package

Understanding the different components of the OnCommand Unified Manager Core Package helps you determine which components you want to enable during the installation and setup process.

The following components are installed on your system:

OnCommand Unified Manager server

Enabled by default.

OnCommand Unified Manager server services

Enabled by default.

NetApp Management Console with protection, provisioning, and Performance Advisor capabilities

Bundled with the Core Package but must be installed separately.

OnCommand Windows PowerShell cmdlets

Downloaded with the Core Package but must be installed separately. Perform local backup and restore operations of virtual objects, as well as mount and unmount operations, using the Windows PowerShell interface.

Related tasks

Downloading OnCommand Unified Manager Core Package on page 21
Installing OnCommand Unified Manager Core Package on Windows on page 22
Installing OnCommand Unified Manager Core Package on Linux on page 24

Functionality available with OnCommand Unified Manager Core Package

You can manage physical storage objects on primary and secondary storage after installing OnCommand Unified Manager Core Package software using OnCommand console, Operations Manager console, NetApp Management Console, and separate PowerShell Cmdlets for OnCommand Unified Manager, which all are installed with OnCommand Unified Manager Core Package.

The Core Package includes the OnCommand Unified Manager graphical user interface (GUI) console from which you can access storage management functionality that was previously accessible through separate NetApp software products. OnCommand Unified Manager delivers access to this functionality through three GUI consoles and a separate set of PowerShell Cmdlets for OnCommand Unified Manager:

OnCommand console

The OnCommand console enables you to perform the following tasks:

- View a set of dashboard panels that provide high-level status of physical objects and support drill-down capabilities.
- Launch other capabilities in the Core Package.
- Export, share, schedule, sort, filter, hide, and print data in the reports for physical objects.

Operations Manager console

The Operations Manager console enables you to perform the following tasks:

- Manage users and roles.
- Monitor clusters, nodes, and vFiler units.
- Monitor physical objects for performance issues and failures.
- Manage storage systems and vFiler units, and virtual servers.
- Schedule and manage scripts.
- Track storage usage and available capacity.

NetApp Management Console

The NetApp Management Console enables you to perform the following tasks:

- Provision physical resources.
- Back up and restore physical objects.
- Manage space on secondary storage.
- Provide disaster recovery for physical objects (automated failover and manual failback).
- Monitor performance.
- View dashboards for physical objects.
- Create and edit storage services.

PowerShell Cmdlets for OnCommand

The PowerShell Cmdlets for OnCommand Unified Manager enable you to manage OnCommand Unified Manager protection-related capabilities through the command-line interface.

Related tasks

Downloading OnCommand Unified Manager Core Package on page 21
Installing OnCommand Unified Manager Core Package on Windows on page 22
Installing OnCommand Unified Manager Core Package on Linux on page 24

System requirements

Before you install the software, you must ensure that your host system conforms to all supported platform requirements. Servers running OnCommand Unified Manager Core Package must meet specific software, hardware, and operating system requirements.

Browser support, requirements, and limitations

To ensure that you can install and launch the software successfully, you must follow the requirements and limitations for the Microsoft Internet Explorer and Mozilla Firefox browsers supported by the OnCommand Unified Manager management software.

Supported browsers

The OnCommand Unified Manager management software supports the following browsers, based on the operating system and the GUI console used:

Operating system	OnCommand GUI console used	Supported browser
Windows	OnCommand console	• Microsoft Internet Explorer 8, 9, 10, and 11 • Mozilla Firefox 10.0, 26.0, 30.0 and 31.0 • Google Chrome 36.0 and 37.0
Linux	OnCommand console	• Microsoft Internet Explorer 8, 9, 10, and 11 • Mozilla Firefox 26.0, 30.0 and 31.0 • Google Chrome 36.0 and 37.0

See the Interoperability Matrix Tool for possible updates to this information.

Browser requirements and limitations

Mozilla Firefox

Mozilla Firefox versions 17.0, 18.0, and 19.0 are not supported. You should disable the automatic upgrade feature in Firefox to avoid installing an unsupported version.

Microsoft Internet Explorer, version 8

- To avoid browser display issues, you must disable the Compatibility View feature before launching the OnCommand console.
  For details, see the Microsoft support site.
- To ensure that OnCommand console can be launched, you must ensure that active scripting and that binary and script behaviors are enabled.
- If enhanced security is enabled in Internet Explorer 8, you might have to add http://*`DataFabric Manager server IP address`*:8080 to the browser's list of trusted sites so that you can access the server.
  You might also have to add port 8443 to the list of trusted sites if you are using SSL.
  You can add ports and URLs in the Security tab under **Tools > Internet Options**.

Microsoft Internet Explorer, version 9

If enhanced security is enabled, you must disable it. If enhanced security is enabled in Internet Explorer 9, the OnCommand console might not load.

Related references

Required ports for the Core Package on page 17

Related information

Microsoft Support: support.microsoft.com/
NetApp Interoperability Matrix Tool: mysupport.netapp.com/NOW/products/interoperability/

Accessing the OnCommand console on a Linux-based PC

If you install and run OnCommand Unified Manager server on a Linux workstation or server, you must launch the OnCommand console GUI using the Internet Explorer 8 or Firefox browser on a separate Windows system to manage the OnCommand Unified Manager server, which is running on a Linux-based computer.

Steps

1. Install the OnCommand Unified Manager Core Package on a Linux workstation or server.
2. Install the NetApp Management Console on a Windows machine.
3. Install the Firefox or Internet Explorer browser on the same Windows machine as the NetApp Management Console.
4. Configure the NetApp Management Console and the browser to point to the Linux workstation or server where the OnCommand Unified Manager server is installed.
5. Launch the OnCommand console GUI using the Internet Explorer or Firefox browser that is running on the Windows machine where it can communicate with the OnCommand Unified Manager server that is running on the Linux workstation or server.

License requirements

Each of the OnCommand Unified Manager components has specific licensing requirements.

Core Package

OnCommand Unified Manager Core Package does not require a license.

DataFabric Manager server

The OnCommand Unified Manager server requires one core license key, which is free and is used only to establish a unique serial number for the server.

Data ONTAP requirements

Certain OnCommand Unified Manager functionality requires other types of licenses for Data ONTAP.

- NetApp has announced the end of availability for SAN licenses. OnCommand Unified Manager server customers should check with their NetApp sales representative regarding other NetApp SAN management solutions.
- OnCommand Unified Manager Core Package 5.2.1 does not support the Business Continuance Option (BCO) license because NetApp has announced its end of support. If you are using the BCO license to monitor and manage your data protection

environment, use the data protection capability of the NetApp Management Console in Core Package 5.2.1. Otherwise, use Core Package 5.1 or earlier.

See the Interoperability Matrix Tool for details.

Related information

NetApp Support Site: mysupport.netapp.com

License requirements for data protection

If you want to use the Business Continuance Option (BCO) license for data protection, you should use Core Package 5.1 or earlier. If you want to upgrade to Core Package 5.2R1, you must use the NetApp Management Console to monitor and manage your data protection environment.

In OnCommand Unified Manager Core Package 5.2R1, you cannot use the BCO license to monitor and manage your data protection environment. OnCommand Unified Manager Core Package 5.2R1 does not support the BCO license because NetApp has announced end of support for this feature.

Important: Before upgrading to OnCommand Unified Manager Core Package 5.2R1, all BCO functionality must be transferred to protection capability or removed.

Related information

Customer Product Communiqué CPC-0612-02: mysupport.netapp.com/info/communications/ECMP1110544.html

Network storage requirements for database files

To enable optimal database access and performance results, OnCommand Unified Manager server requires that the OnCommand Unified Manager server database files be installed on a server using either SAN or iSCSI to connect to the network.

Sybase and OnCommand Unified Manager server do not support accessing the OnCommand Unified Manager server Sybase database files on NAS.

You should not delete the SQL files that are installed in the `/tmp` directory. If the SQL files are deleted from the `/tmp` directory, the OnCommand Unified Manager server cannot start.

Related information

Running a SQL Anywhere database file that is stored remotely from the server machine

Starting the database server

OnCommand Unified Manager Core Package hardware and software requirements

Before installing the OnCommand Unified Manager Core Package, ensure that your system meets the hardware and software requirements.

Software required prior to installing OnCommand Unified Manager Core Package

Before installing OnCommand Unified Manager Core Package, you must install Adobe Flash Player 8.0 or later on the machine from which you launch the OnCommand console.

You can download the software from the Adobe downloads site.

Before you download Flash Player, you should ensure that file downloads are enabled in your web browser and, if you are using Microsoft Internet Explorer, verify that the security settings for ActiveX controls are enabled.

You must install Adobe Flash Player from each browser type that you intend to use with the OnCommand console, even if the browsers are on the same system. For example, if you have both Mozilla Firefox and Microsoft Internet Explorer on the same system and you think you might use both browsers to access the OnCommand console, you must install Adobe Flash Player using the Firefox browser, and then install Adobe Flash Player using the Internet Explorer browser.

Related information

Adobe Downloads: www.adobe.com/downloads

Software required for Open Systems SnapVault

You must separately download and install Open Systems SnapVault software if you intend to back up and restore data residing on non-NetApp physical storage systems; otherwise, you cannot back up and restore data on those storage environments.

OnCommand Unified Manager Core Package supports the use of Open Systems SnapVault to back up and restore virtual machines in a non-NetApp storage environment, but it is not required. OnCommand Unified Manager Core Package supports Open Systems SnapVault 2.6.1, 3.0, and 3.0.1.

Related information

Documentation on the NetApp Support Site: mysupport.netapp.com

Software required for NetApp Host Agent (7-Mode environments only)

You must separately download and install NetApp Host Agent software if you want OnCommand Unified Manager to monitor SAN hosts.

The Host Agent software collects information such as operating system name and version, HBA port details, and file-system metadata, and then sends that information to the OnCommand Unified Manager server. The NetApp Host Agent software must be installed on any Windows or Linux hosts from which you want to monitor SAN host NetApp OnCommand management software.

NetApp Host Agent is also required if you want to remotely start, stop, or restart Open Systems SnapVault software by using NetApp Management Console. In this case, the Host Agent must be installed on the same machine as Open Systems SnapVault.

The minimum version supported by OnCommand Unified Manager Core Package is NetApp Host Agent version 2.7.

Related information

NetApp Host Agent Installation and Administration Guide - mysupport.netapp.com/documentation/productsatoz/index.html

Hardware requirements for Windows Server with 1 to 25 storage systems

You must meet certain software and hardware requirements when you use systems running Windows 64-bit OS on x64 hardware.

Operating system requirements

The software requirements are as follows:

- Microsoft Windows Server 2008, Enterprise or Standard edition
- Microsoft Windows 2008 R2, Enterprise or Standard edition

- Microsoft Windows Server 2012, Datacenter or Standard edition
- Microsoft Windows Server 2008 or 2008 R2 running on VMware ESX 4.0, ESX 4.1, ESXi 4.0, ESXi 4.1, ESXi 5.0, ESXi 5.1, or ESXi 5.5
- Microsoft Windows Server 2012 Standard edition or 2012 R2 running on VMware ESX 4.0, ESX 4.1, ESXi 4.0, ESXi 4.1, ESXi 5.0, ESXi 5.1, or ESXi 5.5

See the Interoperability Matrix Tool for more details about this information.

Hardware requirements

The hardware requirements are as follows:

Hardware	Requirements
Processor	• Intel or AMD x64 processor • 2 GHz or faster CPU
Memory	• 4 GB RAM (minimum)
Disk space	• 10 GB (minimum) • 40 GB (recommended)
Temporary disk space for installation	• 4 GB

Related information

NetApp Interoperability Matrix Tool: mysupport.netapp.com/NOW/products/interoperability/

Requirements for Windows Server with 25 or more storage systems

You must follow certain hardware and software requirements when you use systems running Windows 64-bit OS on x64 hardware.

Operating system requirements

The software requirements are as follows:

- Microsoft Windows Server 2008, Enterprise or Standard edition
- Microsoft Windows 2008 R2, Enterprise or Standard edition
- Microsoft Windows Server 2012, Datacenter or Standard edition
- Microsoft Windows Server 2008 or 2008 R2 running on VMware ESX 4.0, ESX 4.1, ESXi 4.0, ESXi 4.1, ESXi 5.0, ESXi 5.1, or ESXi 5.5
- Microsoft Windows Server 2012 Standard edition or 2012 R2 running on VMware ESX 4.0, ESX 4.1, ESXi 4.0, ESXi 4.1, ESXi 5.0, ESXi 5.1, or ESXi 5.5

See the Interoperability Matrix Tool for more details about this information.

Hardware requirements

The hardware requirements are as follows:

Hardware	Requirements
Processor	• Intel or AMD x64 processor • 2 GHz or faster CPU
Memory	• 6 GB RAM (minimum) • 12 GB RAM (recommended)
Disk space	• 12 GB (minimum) • 60 GB (recommended)
Temporary disk space for installation	• 4 GB

Related information

NetApp Interoperability Matrix Tool: mysupport.netapp.com/NOW/products/interoperability/

Requirements for Linux workstation or server with 1 to 25 storage systems

To ensure that your installation succeeds, you must follow certain software and hardware requirements when you use systems running Linux workstation or server.

Operating system requirements

The software requirements for 64-bit Linux workstation or server are as follows:

- Oracle Enterprise Linux 5.6, 6.0, 6.1, 6.4(Unbreakable Enterprise kernel), or 6.5(Unbreakable Enterprise kernel)
- Red Hat Enterprise Linux Server 5.6, 5.7, 5.8, 5.9, 6, 6.1, 6.2, 6.3, 6.4, or 6.5
- SUSE Linux Enterprise Server 10 SP3, 10 SP4, 11, 11 SP1, 11 SP2, or 11SP3

The software requirements for 64-bit Linux server on VMware ESX 4.0, ESX 4.1, ESXi 4.0, ESXi 4.1, ESXi 5.0, ESXi 5.1, or ESXi 5.5 are as follows:

- Red Hat Enterprise Linux Server 5.6, 5.7, 5.8, 5.9, 6, 6.1, 6.2, 6.3, 6.4, or 6.5
- SUSE Linux Enterprise Server 10 SP3, 10 SP4, 11, 11 SP1, 11 SP2, or 11SP3

See the Interoperability Matrix Tool for more details about this information.

Hardware requirements

The hardware requirements for 64-bit Linux workstation or server and 64-bit Linux server on VMware ESX or ESXi are as follows:

Hardware	Requirements
Processor	• Intel or AMD x64 processor • 2 GHz or faster CPU
Memory	• 4 GB RAM (minimum)

Hardware	Requirements
Disk space	• 4 GB of free disk space (minimum) • 8 GB (recommended)
Temporary disk space for installation	• 4 GB

Related information

NetApp Interoperability Matrix Tool: mysupport.netapp.com/NOW/products/interoperability/

Requirements for Linux workstation or server with 25 or more storage systems

To ensure that your installation succeeds, you must meet certain software and hardware requirements when you use systems running Linux workstation or server.

Operating system requirements

The software requirements for 64-bit Linux workstation or server are as follows:

- Oracle Enterprise Linux 5.6, 6.0, 6.1, 6.4(Unbreakable Enterprise kernel), or 6.5(Unbreakable Enterprise kernel)
- Red Hat Enterprise Linux Server 5.6, 5.7, 5.8, 5.9, 6, 6.1, 6.2, 6.3, 6.4, or 6.5
- SUSE Linux Enterprise Server 10 SP3, 10 SP4, 11, 11 SP1, 11 SP2, or 11 SP3

The software requirements for 64-bit Linux server on VMware ESX 4.0, ESX 4.1, ESXi 4.0, ESXi 4.1, ESXi 5.0, ESXi 5.1, or ESXi 5.5 are as follows:

- Red Hat Enterprise Linux Server 5.6, 5.7, 5.8, 5.9, 6, 6.1, 6.2, 6.3, 6.4, or 6.5
- SUSE Linux Enterprise Server 10 SP3, 10 SP4, 11, 11 SP1, 11 SP2, or 11 SP3

See the Interoperability Matrix Tool for more details about this information.

Hardware requirements

The hardware requirements for Linux workstation or server are as follows:

Hardware	Requirements
Processor	• Intel or AMD x64 processor • 2 GHz or faster CPU
Memory	• 6 GB RAM (minimum) • 12 GB RAM (recommended)
Disk space	• 4 GB of free disk space (minimum) • 8 GB (recommended)
Temporary disk space for installation	• 4 GB

Related information

NetApp Interoperability Matrix Tool: mysupport.netapp.com/NOW/products/interoperability/

Required ports for the Core Package

You might have to configure your firewall on OnCommand Unified Manager Core Package to open default ports that enable communication between OnCommand Unified Manager server and various components, such as managed storage systems and agents. If a port is not open, communication fails between OnCommand Unified Manager server and the storage system or other component.

The following default ports must be open on your firewall:

Default port number	Description
22	The port used for initiating, on storage systems, a secure cluster console, secure storage system takeover and giveback, and secure remote command execution The port is also used for vFiler unit monitoring and management.
23	The port used to initiate a Telnet session to managed storage systems
25	The SMTP port used by OnCommand Unified Manager server to send email for alarms and AutoSupport notification when the `autosupportProtocol` option is set to **`SMTP`**
80	The port used for storage system management
161	The port used to communicate with storage systems
162	The port used by managed storage systems to send SNMP traps to OnCommand Unified Manager server to speed up monitoring of important events This port is configurable.
443	The port used for SecureAdmin-based storage system management
514	The port used for initiating, on storage systems, a cluster console, storage system takeover and giveback, and remote command execution, as well as for vFiler unit monitoring and management
4092	The port used to connect to the NetApp Host Agent
4093	The port used for a secure connection to the NetApp Host Agent
8080	The port used for Operations Manager console access
8088	The port used for NetApp Management Console access
8443	The port used for secure Operations Manager console access
8488	The port used for secure NetApp Management Console access
10000	The port used by Protection Manager to monitor and manage storage system SnapVault and SnapMirror relationships, and SnapVault relationships from Open Systems SnapVault agents

Dedicated system for OnCommand Unified Manager standard edition

OnCommand Unified Manager standard edition has certain installation requirements that you need to be aware of.

- Both OnCommand Unified Manager and its OnCommand Unified Manager server must be installed on a dedicated system.
- To install OnCommand Unified Manager and its OnCommand Unified Manager server on a virtual machine, you must reserve CPU and memory prior to the installation.

Installation requirements specific to 7-Mode environments

Some OnCommand Unified Manager installation and setup features are specific to 7-Mode environments and are noted as 7-Mode only in the documentation. All other installation information, requirements, and instructions apply to both 7-Mode and clustered environments.

When you begin installing OnCommand Unified Manager in a 7-Mode environment, you must select 7-Mode when prompted.

If you change your environment from clustered to 7-Mode, you must delete the clustered objects from the OnCommand Unified Manager server.

Related concepts

Software required for NetApp Host Agent (7-Mode environments only) on page 13

Installation requirements specific to clustered environments

OnCommand Unified Manager supports both clustered and 7-Mode environments, however; there are some minor distinctions in the installation process in the clustered environment of which you should be aware.

When you begin installing OnCommand Unified Manager in a clustered environment, you must select clustered environment when prompted. OnCommand Unified Manager can monitor up to 250 controllers in the clustered environment.

If you are installing or upgrading OnCommand Unified Manager in a clustered environment, you can install only the Standard edition of the software.

When you upgrade your 7-Mode environment to a clustered environment, you must delete the 7-Mode objects from the OnCommand Unified Manager server.

Upgrading from the Express edition of OnCommand Unified Manager to a clustered environment is not allowed. If you currently have the Express edition of OnCommand Unified Manager installed, you must first upgrade to the Standard edition of OnCommand Unified Manager 5.0.

Host services and NetApp Host Agent are not supported in a clustered environment. If you are managing host services when upgrading to a clustered environment, you are notified that the host services will be removed. Information related to host services and NetApp Host Agent features are noted as 7-Mode only in the documentation. All other installation information, requirements, and instructions apply to both 7-Mode and clustered environments.

Downloading OnCommand Unified Manager Core Package

Before installing OnCommand Unified Manager Core Package, you must download the software package from the NetApp Support Site.

Before you begin

- You must have an account on the NetApp Support Site.

About this task

You can choose from the executable files based on your operating system.

You must not change the default location of the local TempFolder directory, or the installation fails.

You can install OnCommand Unified Manager Core Package 5.2.1 on 64-bit systems only.

> **Note:** You must install Core Package 5.1 or earlier to use a 32-bit Windows system or Linux system.

Steps

1. Using your browser, locate and select OnCommand Unified Manager Core Package on the software download page of the NetApp Support Site.
2. From the drop-down list, select the operating system platform on which you are installing and click **Go!**
3. Click **View & Download** for the software version that you want to install.
4. On the **Description** page, click **Continue**.
5. Review and accept the license agreement.
6. On the **Download** page, click the link for the installation file:
   - For Windows systems, click **occore-setup-*version_number*-win-x64.exe**.
   - For Linux systems, click **occore-setup-*version_number*-linux-x64.sh**.
7. Click **Save File** to download the software to the default installation directory.

   The installer automatically extracts the installation files to the %TEMP% location.

Related information

NetApp Support Site: mysupport.netapp.com

Installing OnCommand Unified Manager Core Package on Windows

After you have met the guidelines, requirements, and restrictions for installing OnCommand Unified Manager Core Package, you can follow the prompts in the installation wizard to install the software.

Before you begin

- You must have administrator privileges for the Windows computer on which you are installing the Core Package.
- You must have downloaded the setup file.
- You must have the following items:
  - The OnCommand Unified Manager server license key
  - Credentials for network access
  - The IP address of the server on which you are installing the software
  - The path of the directory on which you want to install, if different from the default location
- In addition, your antivirus software must include the following changes:
  - Either the antivirus software is disabled or an exclusion is added for the OnCommand Unified Manager server.
    If this condition is not met, the installation fails.
  - The Sybase ASA files are excluded to avoid both OnCommand Unified Manager server performance issues and the possibility of database corruption.

About this task

If you have to manage both 7-Mode and clustered Data ONTAP server environments, you must install two separate Core Packages on two Windows servers.

For optimal performance, you must install the Core Package software on a dedicated system, especially if you are managing more than 30 storage systems with the OnCommand Unified Manager server.

If you are installing the Core Package on a virtual machine, the virtual machine must have reserved CPU and memory resources.

Steps

1. Start the Core Package installation wizard by running the appropriate setup file.
2. Choose the environment: 7-Mode or Cluster-Mode.

   Attention: After the Core Package installation is complete, you cannot change the environment.

3. Select the installation location, if different from the default.

   Note: Do not change the default location of the local `TempFolder` directory, or the installation fails. The installer automatically extracts the installation files to the `%TEMP%` location.

4. Review the summary screen and consider whether you want to make changes before completing the installation, and then click **Install**.

5. When the Installation Complete screen is displayed, click **Next** to continue.
6. If you want to start the OnCommand console, clear your browser cache, and then select Launch OnCommand console.
7. Click **Finish**.

After you finish

During the installation process, the installer creates some temporary folders that are automatically deleted the next time you reboot the system. You can delete these folders without adversely affecting the installation of the Core Package.

Related concepts

OnCommand Unified Manager Core Package hardware and software requirements on page 12

Related tasks

Downloading OnCommand Unified Manager Core Package on page 21
Determining whether a storage system belongs to a workgroup or a domain on page 34

Related references

Software required prior to installing OnCommand Unified Manager Core Package on page 12

Installing OnCommand Unified Manager Core Package on Linux

After you have met the guidelines, requirements, and restrictions for installing OnCommand Unified Manager Core Package, you can follow the prompts in the installation wizard to install the software.

Before you begin

- You must have downloaded the setup file.
- You must have the following items:
  - The OnCommand Unified Manager server license key
  - Credentials for network access
  - The IP address of the server on which you are installing the software
  - The path of the directory on which you want to install, if different from the default location
- In addition, your antivirus software must include the following changes:
  - Either the antivirus software is disabled or an exclusion is added for the OnCommand Unified Manager server.
    If this condition is not met, the installation fails.
  - Sybase ASA files are excluded to avoid both OnCommand Unified Manager server performance issues and the possibility of database corruption.
- If you are installing the Core Package on Red Hat Enterprise Linux Advanced Platform 5.x, the SELinux status must be disabled.

About this task

If you have to manage both 7-Mode and clustered environments for Data ONTAP, you must install two separate Core Packages on two Linux servers.

For optimal performance, you must install the Core Package software on a dedicated system, especially if you are managing more than 30 storage systems with the OnCommand Unified Manager server.

If you are installing the Core Package on a virtual machine, the virtual machine must have reserved CPU and memory resources.

Steps

1. Start the Core Package installation wizard by running the appropriate setup file.
2. Follow the prompts and then select the environment: 7-Mode or Cluster-Mode.

   Attention: After the Core Package installation is complete, you cannot change the environment.

   When the URL for opening the OnCommand console is displayed, the installation is complete.
3. Copy and paste the URL to a browser to open the OnCommand console.

Related concepts

OnCommand Unified Manager Core Package hardware and software requirements on page 12

Related tasks

Downloading OnCommand Unified Manager Core Package on page 21

Related references

Software required prior to installing OnCommand Unified Manager Core Package on page 12

Installing OnCommand Unified Manager Core Package with a script

You can quickly deploy OnCommand Unified Manager Core Package using a scripted, unattended installation. The installation script contains the installation settings for the Core Package.

Before you begin

- You must have administrator privileges for the Windows computer on which you are installing the Core Package.
- The script must contain the following required information:
    - OnCommand Unified Manager server license key
    - Credentials for network access
    - IP address of the server on which you are installing
    - Directory path where you want to install if different from the default location

About this task

The installation script can reside in one of the following locations:

- Default installation script
- FTP
- HTTP/HTTPS
- NFS
- Local disk
- USB flash drive

Steps

1. Create a script using the supported commands.
2. Edit the installation script as required to change the options that are unique for each installation.
3. Save the script to the location from which you want to run it.
4. Run the scripted installation or set a schedule for when the script is to run.

Related references

Required ports for the Core Package on page 17

Options you can use for the Windows installation script

You can use options to configure the settings in the installation script when installing the Core Package on Windows.

You can use the following options in the script:

Script	Description
`/S`	Performs the installation silently, without any installation screens appearing.

`/OPMOD=`**`7-Mode`**
`/OPMOD=`**`Cluster-Mode`**
	Specifies whether the environment is 7-Mode or clustered.
	If the option is set to **`7-Mode`**, the Core Package for a 7-Mode environment is installed.
	If the option is set to **`Cluster-Mode`**, the Core Package for a clustered environment is installed.

`/LICENSEKEY=`*`license_key`*	Specifies the license key.
`/UPGRADE`	Specifies that an upgrade is required.

No options are available for the following situations:

- Accepting or rejecting the AutoSupport agreement from the CLI.
  When a silent installation is performed, the installation assumes that you accept the AutoSupport agreement.
- Specifying whether you want to perform a backup during the upgrade.
  In a silent upgrade, a backup is performed by default.
- Specifying the installation directory or database backup location directory; otherwise, the default OnCommand Unified Manager server paths are used.

Options you can use for the Linux installation script

You can use options to configure the settings in the installation script when installing the Core Package on Linux.

You can use the following options in the script:

Option	Description
`-a`	Specifies that the AutoSupport notice agreement is accepted. If the option is not specified, the AutoSupport notice is displayed, which prompts you to accept or decline.
`-d` *`installation_directory`*	Specifies the path of the installation directory. If the option is not specified, the Core Package is installed in the default directory: for example, `/opt/NTAPdfm/`
`-l` *`licenses_key`*	Specifies the license key. If the option is not specified, a message is displayed during the installation that prompts you to enter the license key.

`-b` **`yes`**
`-b` **`no`**
	Specifies whether to perform a database backup during the upgrade.

`-B`*`backup_file_name`*	Specifies the backup file name. If the option is not specified, the default backup file name is stored in the `data` directory of the installation directory.

Option	Description
`-n`	Removes NetCache support if you upgrade your OnCommand Unified Manager server. **Note:** You should use this option only for upgrades from OnCommand Unified Manager server versions earlier than 3.8. If the option is not specified and you are upgrading from a version earlier than 3.8, a message is displayed about the removal of NetCache support for OnCommand Unified Manager server.

`-m` **`7-Mode`**
`-m` **`Cluster-Mode`**
	Specifies whether the environment is 7-Mode or clustered.
	If the option is set to **`7-Mode`**, the Core Package for a 7-Mode environment is installed.
	If the option is set to **`Cluster-Mode`**, the Core Package for a clustered environment is installed.

`-w` *`wrapper_directory`*	Specifies the path for installing the OnCommand Unified Manager server CLI wrappers.

Setting up Web security after restoring a database on a new OnCommand Unified Manager Core Package installation

You can restore a database backup from another OnCommand Unified Manager server instance to the new OnCommand Unified Manager server installation, for instance, when you want to upgrade your hardware; however, database backups do not include the key and certificate file, so these must be generated or imported, and HTTPS must be enabled if it was set on the old system.

About this task

Perform these steps from a console session on the new OnCommand Unified Manager server after you install the OnCommand Unified Manager Core Package.

Steps

1. Perform one of the following actions:
    - Enter the `dfm ssl service setup` command to create new client certificates.
    - Enter `dfm ssl server import` to import an existing certificate.
2. If the HTTPS service was enabled on the system from which the database backup was made, you must also enable the HTTPS service on the new system by entering `dfm option set httpsEnabled=Yes`.

Enabling FIPS on OnCommand Unified Manager server

You can enable the Federal Information Processing Standard (FIPS) 140-2 mode on the OnCommand Unified Manager server by using the DataFabric Manager global options. By default, FIPS 140-2 is disabled on OnCommand Unified Manager Core Package.

Before you begin

Your storage systems must be running clustered Data ONTAP.

About this task

You must perform this task from a console session on the OnCommand Unified Manager server after you install OnCommand Unified Manager Core Package.

Steps

1. Enable FIPS by running the following command from a console session:

   ```
   dfm option set sslFipsEnabled=Yes
   ```

2. When prompted, restart all the all the OnCommand Unified Manager server services by running the following commands:

   ```
   dfm service stop
   ```

   ```
   dfm service start
   ```

3. Verify that the OnCommand Unified Manager server is operating in FIPS mode by choosing one of the following options:

   - Check log files such as “dfmmonitor.log”, “dfmserver.log”,“dfmeventd”, and “error.log”.
   - Use the DataFabric Manager global option **`sslFipsEnabled`**.

FIPS mode limitations

You must be aware of the limitations associated with the FIPS mode before you enable it on the OnCommand Unified Manager server.

- FIPS mode is not supported for OnCommand Unified Manager server on systems running Data ONTAP operating in 7-Mode.
- MD5 as an authentication algorithm is not supported in SNMPv3 communication.
- The use of privacy password is not supported in SNMPv3 communication.
- The certificate key length for HTTPS communication with the OnCommand Unified Manager server HTTPD service of less than 1024 bits is not supported.
  If you have a certificate that is not supported in the FIPS mode, then you can regenerate the certificate key by using the `dfm ssl server setup` command and selecting the key size of 1024 bits or more. However, the recommended key size is 2048 bits.

For more information about the minimum certificate key length, see the “Critical Security Parameters and Public Keys” section of the *OpenSSL FIPS 140-2 Security Policy* document.

For more information about the recommended certificate key length, see the “Key Agreement and Key Transport Using RSA ” section of the *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths* document.

Related tasks

Enabling FIPS on OnCommand Unified Manager server on page 30

Installing NetApp Management Console

You can download and install NetApp Management Console through the OnCommand console. NetApp Management Console is required to perform many of your physical storage tasks. You must install NetApp Management Console 3.3, which contains bug fixes found in the 3.2 version.

Before you begin

You must be authorized to perform all the steps of this task; your RBAC administrator can confirm your authorization in advance.

About this task

During this task, the OnCommand console launches the Operations Manager console. Depending on your browser configuration, you can return to the OnCommand console by using the Alt-Tab key combination or clicking the OnCommand console browser tab. After the completion of this task, you can leave the Operations Manager console open, or you can close it to conserve bandwidth.

Steps

1. Log in to the OnCommand console if necessary.
2. Click the **File** menu, and then click **Download Management Console**.

   A separate browser tab or window opens to the Management Console Software page in the Operations Manager console.
3. Click the download link for the Linux or Windows installation.
4. In the download dialog box, click **Save File**.

   The executable file is downloaded to your local system, from the system on which the OnCommand Unified Manager Core Package was installed.
5. From the download directory, run the `nmconsole-setup-xxx.xxx` executable file.

   The NetApp Management Console installation wizard opens.
6. Follow the prompts to install NetApp Management Console.

Result

After installation, you can access NetApp Management Console from the following locations:

- On Windows systems, the default installation path is `C:\Program Files\NetApp \Management Console`.
  You can launch the console from the NetApp directory on the Start menu.
- On Linux systems, the default installation path is `/usr/lib/NetApp/management_console/`.
  You can launch the console from `/usr/bin`.

Installing or upgrading OnCommand Unified Manager Windows PowerShell cmdlets

To use Windows PowerShell cmdlets with the OnCommand console, you must manually install them. You also must manually upgrade the cmdlets if you upgrade your version of the console.

Before you begin

You must have installed the appropriate version of OnCommand Unified Manager Core Package.

Steps

1. Navigate to the appropriate folder:

If you have installed the OnCommand Unified Manager Core Package on...	Then do this...
A Windows server	Navigate to the `*DFM_Install_dir*\DFM\web\clients` folder.
A Linux server	Navigate to the `/opt/NTAPdfm/web/clients` folder.

This folder contains the Windows PowerShell installation package.

2. Execute the installation file:

If you are installing the cmdlets on...	Then do this...
The same Windows server	Double-click the executable file and follow the installation wizard prompts.
A different Windows server	Copy the installation file to the server or workstation to which you want to install the cmdlets and then execute the installation.
A Linux server	Copy the installation file to a Windows server on which you want to install the cmdlets and then execute the installation. Windows PowerShell Cmdlets are not supported on Linux.

After you finish

You can execute the Windows PowerShell cmdlets for OnCommand console.

Determining whether a storage system belongs to a workgroup or a domain

The storage system that you use for the OnCommand Unified Manager Core Package installation must belong to a domain rather than a workgroup. Prior to installing the Core Package, you must determine if the system belongs to a workgroup or a domain.

Step

1. Right-click **My Computer** and click **Properties** and the **Computer Name** tab.

   For details, see the documentation for your Windows operating system.

   The Computer Name tab displays either a Workgroup label or a Domain label.

Certificate-based authentication

Connecting OnCommand Unified Manager server to a virtual or cloud infrastructure network using certificate-based authentication means that authentication occurs using an SSL certificate. Using the certificate makes the requirement for user names or passwords unnecessary.

Certificate-based authentication occurs when a client, such as the host service or cloud orchestration tool, connects to the OnCommand Unified Manager server with a Web service or ZAPI request. The client presents a self-signed certificate to OnCommand Unified Manager server. In turn, OnCommand Unified Manager server accepts the certificate, validates the certificate, and processes the request if it authenticates the client.

Certificate information

An SSL certificate is a digital document whose legitimacy is signed off by its creator. The certificate is used to verify that a key belongs to an individual or organization.

When you install OnCommand Unified Manager server or the host service, the truststore contains no certificates to trust. You must add client certificates to the truststore before OnCommand Unified Manager server will trust those client connections.

By default, the OnCommand Unified Manager server installs the OnCommand Unified Manager server key and certificate pair, and any trusted certificates in a repository called the OnCommand Unified Manager server truststore

When OnCommand Unified Manager server is installed, it is configured to not trust any public certificate authorities (CAs). If you want OnCommand Unified Manager server to trust clients with certificates signed by a public CA, you must add the root CA certificate to the truststore.

Certificates are identified in the Windows Trusted Root Certification Authorities store with the following titles in the Issued To and Issued By columns:

- DataFabric Manager - VIM
- DFM Host Services for VIM
- DFM Plugin for VIM

Managing certificates for cloud service clients

You can manage certificates on your OnCommand Unified Manager server for clients in a cloud infrastructure network, including generating a key and a self-signed certificate, adding certificates to a truststore, listing all certificates in a truststore, displaying details of certificates in a truststore, removing a certificate from a truststore, and disabling certificate-based authentication.

Generating a key and self-signed certificate

You can generate a key and certificate pair by using the `dfm ssl service setup` command.

Steps

1. On OnCommand Unified Manager server, open a console session.
2. Enter the following command:

   `dfm ssl service setup -f`

The `-f` option causes the command to overwrite existing key and certificate pairs.

3. To force OnCommand Unified Manager server to immediately use the newly generated key, enter the following command:

   ```
   dfm ssl service reload
   ```

Adding a certificate in the truststore

You can add a certificate in the OnCommand Unified Manager server truststore for clients in a cloud infrastructure network by using the `dfm ssl service truststore add` command.

Before you begin

The certificate must be in privacy-enhanced mail (PEM) format.

Step

1. On the OnCommand Unified Manager server console, enter the following command:

   ```
   dfm ssl service truststore add -f cacert.pem
   ```

   The `-f` option adds the certificate without prompting you for permission.

Removing a certificate from the truststore

You can remove a cloud service client certificate from the OnCommand Unified Manager server truststore by using the `dfm ssl service truststore remove` command.

Step

1. On the OnCommand Unified Manager server console, enter the following command:

   ```
   dfm ssl service truststore remove certificate_number
   ```

Displaying the list of certificates in a truststore

You can use the OnCommand Unified Manager server command-line interface to display a list of all the certificates in a truststore. You might want to do this to determine how long a certificate is valid, to find information about the certificate's issuer, or to find the certificate number assigned to a specific certificate.

Step

1. On the OnCommand Unified Manager server console, enter the following command:

   ```
   dfm ssl service truststore list
   ```

Displaying details about certificates in a truststore

You can display the details about one or more certificates in a truststore, including details about the certificate serial number, signature algorithm, issuer, valid from and valid to dates, and public key algorithm.

Steps

1. On the OnCommand Unified Manager server, open a console session.
2. Enter the following command:

   ```
   dfm ssl service truststore detail certificate number
   ```

   `certificate number` displays details about a specific certificate in the truststore.

You can use the `dfm ssl service truststore list` command to find the certificate numbers.

Displaying the contents of the OnCommand Unified Manager server key and certificate file

You can display the contents of a key and certificate file, including the expiry date of the certificate, and verify whether the certificate is generated correctly by using the OnCommand Unified Manager server command-line interface. The key and certificate file contents are displayed in hexadecimal format.

Step

1. On the OnCommand Unified Manager server console, enter the following command:

   ```
   dfm ssl service show -c -k -f -o output
   ```

   `-c` selects the certificate for printing.

   `-k` selects the key for printing.

   `-o` saves the information to a file.

   `-f` overwrites the file without prompting.

Displaying DataFabric Manager server certificate details

You can display the OnCommand Unified Manager server certificate details, including the certificate serial number, valid to and valid from dates, and signature algorithm.

Before you begin

The system date and time must be correct on the system where OnCommand Unified Manager server is installed; otherwise, the Not Before and Not After dates might be displayed incorrectly in the command output.

Steps

1. On the OnCommand Unified Manager server, open a console session.
2. Enter the following command:

   ```
   dfm ssl service detail -f -o outputfile
   ```

   `-f` overwrites the file without prompting.

   `-o` saves the information to a file.

Disabling certificate-based authentication

The OnCommand Unified Manager server uses certificate-based authentication by default to authenticate clients in a cloud infrastructure network. You can disable this feature so that clients cannot use a root certificate to connect to the OnCommand Unified Manager server. You might want to disable certificate-based authentication when a certificate is expiring or you are replacing a certificate.

Steps

1. On the OnCommand Unified Manager server console, open the command-line interface.
2. Enter the following command:

   ```
   dfm option set serverCertAuthEnabled=No
   ```

Managing certificates for host services clients

You can manage certificates for host services clients on your OnCommand Unified Manager server, including registering certificates, authorizing certificates, unregistering certificates, and displaying certificate information for a specific host service.

Authorizing a host service certificate

When you register a new host service with OnCommand Unified Manager server, you must manually authorize the authentication certificate so that requests from the host service to OnCommand Unified Manager server are successful.

Steps

1. Enter the following command from a OnCommand Unified Manager server console session:

   ```
   dfm hs list
   ```

   The host requesting authorization is listed with the status "Authorization Pending".

2. Record the ID number of the host requiring authorization.

   The host ID is located in the first column of the list output.

3. Using the ID number you recorded in Step 2, enter the following command:

   ```
   dfm hs authorize ID number
   ```

   You are asked whether you authorize the host service to use this OnCommand Unified Manager server.

4. Enter `y` to authorize the host service certificate.

Migrating certificates, keys, and truststores manually

During OnCommand Unified Manager server database backups, the directories containing certificates, keys, and truststores for both cloud service clients and host service clients are not backed up. If you want to restore database backups to a different OnCommand Unified Manager server, you must manually migrate the certificates, keys, and truststore directories or the restore fails.

About this task

This procedure is not required when you back up and restore the database to the same OnCommand Unified Manager server.

Steps

1. On the OnCommand Unified Manager server you want to migrate, back up the database.

2. On the OnCommand Unified Manager server you just backed up, copy the following three folders from the `\`*`DataFabric Manager install directory`*`\conf\keys\` directory:

   - `certs`
   - `private_keys`
   - `truststore`

3. Restore the database to the new OnCommand Unified Manager server.

4. Copy the three folders from the original OnCommand Unified Manager server to the same directory on the destination OnCommand Unified Manager server.

5. Perform one of the following actions, depending on which type of clients you are migrating:

   - If you migrate clients in a cloud infrastructure, after the migration, generate a new OnCommand Unified Manager server certificate on the destination OnCommand Unified Manager server by entering `dfm ssl service setup`, and then load the new certificate by entering `dfm ssl service reload`

     Note: If you do not generate a new certificate, the new OnCommand Unified Manager server will load the certificate that was migrated from the original OnCommand Unified Manager server causing OnCommand Unified Manager server hostname validation to fail on cloud service clients.

   - If you are migrating host service clients, after the migration, unregister the host service and then register the new host service from the Host Services tab in the OnCommand console.

Enabling secure communication between the OnCommand Unified Manager server and Data ONTAP

You should configure the storage system running Data ONTAP and the OnCommand Unified Manager server to enable secure communication.

Before you begin

- You must have enabled secure communication on the storage system running Data ONTAP by using OnCommand System Manager or the Data ONTAP command-line interface.
- You must have enabled SNMPv3 on the storage system running Data ONTAP and on the OnCommand Unified Manager server.

  For more information about enabling SNMP, see the *Data ONTAP Network Management Guide* and the *OnCommand Unified Manager Operations Manager Administration Guide*.

Steps

1. Initialize the OnCommand Unified Manager server private key and generate a self-signed certificate by running the following command and following the prompt:

   `dfm ssl server setup -f`

2. Restart the HTTP service by running the following commands:

   `dfm service stop http`

   `dfm service start http`

3. Enable HTTPS by running the following command:

   `dfm option set httpsEnabled=Yes`

4. Request for a signed certificate from a well-known CA by running the following command:

   `dfm ssl server req -f -o server.csr`

   The `server.csr` file should be signed by a CA.

5. Import the signed certificate to the OnCommand Unified Manager server by running the following command:

   `dfm ssl server import server.crt`

6. Restart the HTTP service by running the following commands:

   `dfm service stop http`

   `dfm service start http`

7. Enter the certificate information for a CA setup by running the following command and following the prompt:

   `dfm ssl self setup -f`

   The CA is ready to sign requests.

8. If the OnCommand Unified Manager server is running a private CA, perform the following steps:

   a. Run the following command to allow certificate signing requests:

      `dfm ssl self sign -f -o server.crt server.csr`

  b. Import the signed certificate to the OnCommand Unified Manager server by running the following command:

     `dfm ssl server import server.crt`

9. Change the communication options by running the following commands:

```
dfm service stop http
dfm option set httpsEnabled=yes
dfm option set httpEnabled=no
dfm option set httpsPort=8443
dfm option set hostLoginProtocol=ssh
dfm option set hostAdminTransport=https
dfm option set perfAdvisorTransport=httpsOk
dfm service start http
```

10. Verify that secure communication is enabled with the host by running the command:

    `dfm host diag` ***`hostID_or_hostIP`***

    You should be able to connect to the OnCommand console by using the following URL: https://*`DataFabric_Manager_server_IP_or_hostname`*:*`httpsPort`*/

Related information

Documentation on the NetApp Support Site: mysupport.netapp.com

Upgrading to OnCommand Unified Manager Core Package

You can upgrade to OnCommand Unified Manager Core Package to use the monitoring tools and dashboards of the OnCommand console.

If you are upgrading on a Windows 64-bit server, from OnCommand Unified Manager server 4.x to OnCommand Unified Manager Core Package 5.0 or later, you must back up the OnCommand Unified Manager server 4.x database before the upgrade. When you restore the database after the upgrade, the installation directory `C:\Program Files\NetApp\DataFabric Manager\DFM\` is chosen based on the 64-bit Core Package.

> **Note:** If you do not back up before upgrading, the installer chooses the `Program Files (x86)` directory, which is the location for 32-bit applications.

Related references

License requirements for data protection on page 12

Changes that affect upgrade to OnCommand Unified Manager Core Package

While planning your upgrade to OnCommand Unified Manager Core Package 5.2.1, you must consider the changes in the product that affect the upgrade, such as changes to the database. Also, OnCommand Unified Manager Core Package 5.1 or later requires two separate OnCommand Unified Manager servers to monitor and manage 7-Mode and cluster objects.

Upgrade changes in OnCommand Unified Manager Core Package 5.2.1

Upgrade to OnCommand Unified Manager Core Package 5.2.1 might take a long time to complete because the following processes are included during the upgrade:

- Validating the OnCommand Unified Manager server database
- Removing the storage objects that are marked-deleted in the database and the associated entries in the history tables
  Some storage objects might be manually or automatically deleted from a controller monitored by the OnCommand Unified Manager server. Such objects are marked-deleted on the OnCommand Unified Manager server database, but are not removed from the database.
- Removing events older than 180 days from the day of installation, or as specified in the eventsPurgeInterval option

> **Attention:** If the upgrade fails during the database validation, you must try to restore the previous version's database backup to a new installation of OnCommand Unified Manager Core Package 5.2.1. Contact technical support if the database restore fails or if the upgrade fails during any other part of the process.

You can run the DFM Deleted Object Purge Tool before upgrading to determine an approximate time required for the upgrade. This tool can determine the additional upgrade time required due to the cleaning of marked deleted objects. You must install the tool by downloading it from the NetApp Support Site.

> **Note:** You should check the `monitor.db` file size and allocate approximately 15 minutes for each gigabyte of data.

Upgrade from OnCommand Unified Manager Core Package 5.1 to OnCommand Unified Manager Core Package 5.2.1

Upgrade from OnCommand Unified Manager Core Package 5.1 to OnCommand Unified Manager Core Package 5.2.1 takes a long time to complete because of the following change in the upgrade process:

- Cleaning and validation of the OnCommand Unified Manager server database in Core Package 5.2.1

Upgrading from DataFabric Manager 3.x to OnCommand Unified Manager Core Package 5.2.1

Upgrade from DataFabric Manager 3.x to OnCommand Unified Manager Core Package 5.2.1 takes time to complete due to the following changes in the product:

- Cleaning and validation of the OnCommand Unified Manager server database in Core Package 5.2.1
- Deleting of unwanted storage objects in Core Package 5.1, if you are monitoring and managing controllers running Data ONTAP operating in 7-Mode and clustered Data ONTAP

  In OnCommand Unified Manager Core Package 5.1 or later, you must have two separate OnCommand Unified Manager servers to monitor and manage controllers running Data ONTAP operating in 7-Mode and clustered Data ONTAP. An upgrade to the clustered environment deletes all the 7-Mode controllers. Similarly, an upgrade to the 7-Mode environment deletes all the cluster controllers.

  Note: This is applicable during an upgrade or restore to Core Package 5.1.
- Changes in the Performance Advisor file format in OnCommand Unified Manager server 4.0

  This is applicable if you use Performance Advisor. The delay in upgrade occurs because the Performance Advisor data is read and rewritten in the new file format.

Related concepts

Upgrade issues with DataFabric Manager 3.8 or earlier on page 48

Related information

NetApp Support Site: mysupport.netapp.com

Upgrading OnCommand Unified Manager Core Package on Windows

You can upgrade to the latest version by installing OnCommand Unified Manager Core Package.

Before you begin

- You must have administrator privileges for the Windows computer on which you are installing the Core Package.
- If you are upgrading from the Express edition of OnCommand Unified Manager Core Package to clustered Data ONTAP, you must have first upgraded to OnCommand Unified Manager Core Package 5.0 and installed the Standard edition.
- You must have downloaded the setup file.
- You must have the following items:

- ◦ Credentials for network access
- ◦ The IP address of the server on which you are installing the software
- ◦ Directory path for the installation

  If you are upgrading to OnCommand Unified Manager Core Package while migrating to a new system, you should use the original OnCommand Unified Manager server installation path. You must not change this installation path because it might disrupt some functionality.

  For example, if the original installation path is `C:\Program Files (x86)\NetApp\DataFabric Manager`, you should use this path. Do not change this path to `D:\Application\NetApp\DataFabric Manager`.

About this task

The installation software automatically detects and stops any OnCommand Unified Manager server services that are running on the system.

You can view the `sybase.log` file, which is located at *`install_directory`*`/log/`, to monitor the progress of the database delete operation for the mode that is being removed. You should perform a backup of the database. If you do not perform a backup, your data is not archived.

When you upgrade a OnCommand Unified Manager server that was earlier managing both 7-Mode and clustered Data ONTAP objects to a 7-Mode environment, a message is displayed after you select the mode: `Purging objects of undesired mode from the database.` During a restore operation, you are prompted to delete the objects.

Steps

1. Start the Core Package installation wizard by running the appropriate setup file.
2. Review and accept the license and AutoSupport agreements.

   You cannot install the Core Package unless you accept the license agreement.
3. Select the Data ONTAP environment: 7-Mode or Cluster-Mode.

   Note: If you are upgrading using the Express edition, this prompt is not displayed.
4. When prompted, confirm if you want to back up the database.

   Backing up the database can take several minutes to many hours, depending on the size of your database.
5. Review the summary screen and consider whether you want to make changes before completing the installation, and then click **Install**.
6. When the **Installation Complete** screen is displayed, click **Next**.
7. Click **Finish** to close the wizard.

After you finish

- You should clear the browser cache before you first start the OnCommand console and when you upgrade to a new version of the software.

Related tasks

Downloading OnCommand Unified Manager Core Package on page 21
Installing OnCommand Unified Manager Core Package on Windows on page 22
Determining whether a storage system belongs to a workgroup or a domain on page 34

Upgrading OnCommand Unified Manager Core Package on Linux

You can upgrade to the latest version of the Standard edition by installing OnCommand Unified Manager Core Package.

Before you begin

- If you have a large database, you must have backed up the database before starting the setup wizard.
- You must have root user privileges for the Linux system on which you are installing OnCommand Unified Manager Core Package.
- If you are upgrading from the Express edition of OnCommand Unified Manager to clustered Data ONTAP, you must have upgraded to OnCommand Unified Manager Core Package 5.0 and installed the Standard edition.
- You must have downloaded the setup file.
- You must have the following items:
  - Credentials for network access
  - The IP address of the server on which you are installing the software
  - Directory path where you want to install, if different from the default location

About this task

The installation software automatically detects and stops any OnCommand Unified Manager server services that are running on the system.

You should perform a backup of the database. If you do not perform a backup, your data is not archived.

Steps

1. Start the Core Package installation wizard by running the appropriate setup file.
2. Follow the prompts and select the Data ONTAP environment: 7-Mode or Cluster-Mode.

   Note: If you are upgrading the Express edition, this prompt is not displayed.
3. Continue responding to the prompts.

   When the URL for opening the OnCommand console is displayed, the upgrade is complete.
4. Copy and paste the URL to a browser to open the OnCommand console.

Related tasks

Downloading OnCommand Unified Manager Core Package on page 21
Installing OnCommand Unified Manager Core Package on Linux on page 24

Upgrading from Core Package 32-bit to Core Package 64-bit

OnCommand Unified Manager Core Package 5.2 does not support installation on a 32-bit server. Before you upgrade to Core Package 5.2 in your Windows or Linux server, you must back up and restore your 32-bit OnCommand Unified Manager server database.

Before you begin

- The installation directory must have twice the space of the backup data.

  The restore operation creates a temporary copy of the backup data and therefore the installation directory should have enough space.
- The new OnCommand Unified Manager server must be on the same subnet as the old OnCommand Unified Manager server.

Steps

1. Create a backup of the 32-bit OnCommand Unified Manager server database by running the following command:

   `dfm backup create` ***`backup_filename`***

2. Install the OnCommand Unified Manager Core Package 5.2 on your 64-bit server.
3. Copy the 32-bit database backup to the 64-bit server.
4. Restore the 32-bit database backup on the 64-bit server by running the following command:

   `dfm backup restore` ***`backup_filename`***

5. Run the following command to the view the old paths for the setup options:

   `dfm options list` ***`setup_option_name`***

   You should check the path for the following setup options: `databaseBackupDir`, `dataExportDir`, `dfmencKeysDir`, `perfArchiveDir`, `perfExportDir`, `pluginsDir`, `reportDesignPath`, `reportsArchiveDir`, and `scriptDir`.

   #### Example

   - Run the following command:

     `dfm options list dataExportDir`

     Result: The command displays the path in which the dataExportDir data is located: *`installation_directory`*`/data/` in Windows and `/opt/NTAPdfm/data/` in Linux.

6. Copy the data for each option to the new 64-bit install directory.

   #### Example

   Copy the data from the *`installation_directory`*`/data/` location to the new installation directory in Windows.

   Alternatively, copy the data from the `/opt/NTAPdfm/data/` location to the new installation directory in Linux.

7. Restart the OnCommand Unified Manager server services by running the command:

   `dfm service stop`

   `dfm service start`

Related tasks

Installing OnCommand Unified Manager Core Package on Windows on page 22
Installing OnCommand Unified Manager Core Package on Linux on page 24

Upgrading Core Package to manage 7-Mode and clustered Data ONTAP environments

You can install two separate instances of OnCommand Unified Manager Core Package and migrate data from earlier versions of OnCommand Unified Manager server to enable management of both 7-Mode and clustered Data ONTAP environments. OnCommand Unified Manager does not support management of both 7-Mode and clustered environments from the same server.

Before you begin

You must have two OnCommand Unified Manager server license keys, one for each server instance.

You must back up your existing database before you upgrade.

Steps

1. Download and install OnCommand Unified Manager Core Package.
2. When you are prompted, choose 7-Mode as your environment, and complete the installation.
3. On a second server, perform a new installation of OnCommand Unified Manager Core Package, choosing the clustered environment.
4. On the second server, restore the database that you backed up before the upgrade.

   A warning message is displayed that all 7-Mode data will be deleted.
5. Disable the license key on the second server by entering the following command at the CLI:

   ```
   dfm license disable all
   ```

   After the restore, the two OnCommand Unified Manager server installations share the same license key; therefore, you must disable one license to avoid conflicts.
6. Add a new license key to the second server by entering the following command:

   ```
   dfm license install NewLicenseKey
   ```
7. Verify that the new license key is installed by entering the following command:

   ```
   dfm license list
   ```

   The second server installation is complete.

Related tasks

Downloading OnCommand Unified Manager Core Package on page 21
Installing OnCommand Unified Manager Core Package on Windows on page 22
Installing OnCommand Unified Manager Core Package on Linux on page 24

Upgrade issues with DataFabric Manager 3.8 or earlier

You can upgrade to OnCommand management software from previous versions of the OnCommand Unified Manager server. However, due to changes in system behavior between releases, you might have to resolve issues before upgrading.

The following issues are associated with upgrading to OnCommand Unified Manager Core Package 5.1 from DataFabric Manager 3.8 and earlier. Issues associated with upgrading from OnCommand Unified Manager server 4.0 or later to OnCommand Unified Manager Core Package are covered in the requirements and installation instructions throughout this guide and in the *OnCommand Unified Manager Core Package Release Notes*.

Supported methods to upgrade from Solaris to Windows or Linux

DataFabric Manager 3.8 and later does not support Solaris. Therefore, you must migrate the OnCommand Unified Manager server database on Solaris to a server running Windows or Linux before you upgrade to DataFabric Manager 3.8 or later.

You can migrate the database by creating an archive copy of the backup by using the `dfm backup create <backup_filename>` command, then restore the database by using the `dfm backup restore <backup_filename>` command.

Upgrade path from DataFabric Manager 3.5 to OnCommand Unified Manager Core Package 5.x

You can upgrade to OnCommand Unified Manager Core Package 5.x from OnCommand Unified Manager server 4.0 or later. If you want to upgrade from OnCommand Unified Manager server 3.5 to OnCommand Unified Manager Core Package 5.x, you must first upgrade to OnCommand Unified Manager server 4.0.

Upgrading from DataFabric Manager 3.7.1

If you have created custom reports with GUILink and SecureGUILink as fields in DataFabric Manager 3.7.1 or earlier, upgrading to DataFabric Manager 3.8 or later causes the `dfm report view` command to fail. You must open the custom report in Operations Manager console and save the report to view it.

Upgrading from DataFabric Manager 3.7 on Linux

If you are upgrading from DataFabric Manager 3.7 to DataFabric Manager 3.8 or later on Linux, the upgrade might fail with the following notification:

```
rpm: /opt/NTAPdfm/lib/libgcc_s.so.1: version `GCC_4.2.0' not found
(required by /usr/lib/libstdc++.so.6)
```

You can resolve this issue by deleting the entry `/opt/NTAPdfm/lib` from the environment variable LD_LIBRARY_PATH.

Upgrading from DataFabric Manager 3.7 or earlier

If you are upgrading from DataFabric Manager 3.7 or earlier to DataFabric Manager 3.8 or later, you must delete the existing Data Source Name (DSN) entry for the Adaptive Server Anywhere 9.0 driver and create a new DSN entry for SQL Anywhere 10.

Upgrading from DataFabric Manager 3.5 or earlier

If you are upgrading from DataFabric Manager 3.5 or earlier to DataFabric Manager 3.6 or later, it takes a long time to upgrade the performance data files (data of 20 GB or more). The length of time depends on the platform used. The space used by the performance data files increases by about 65% during the upgrade.

Upgrading from DataFabric Manager 3.2 or earlier

Because of database schema changes, you might experience a delay of several minutes to a few hours when upgrading from DataFabric Manager 3.2 or earlier.

The time required to perform the upgrade depends on the size of the database, the amount of history in the database, the CPU speed, and the I/O throughput of the system. The following processes might require a lot of time:

- Merging rotating history tables
- Populating history tables
- Populating volume history tables
- Populating aggregate history tables
- Reloading the database into the latest file format (at the end of upgrade)

Upgrading from DataFabric Manager 2.1 or earlier, on Windows

Because of a database upgrade that is no longer supported on a Windows platform, you must first upgrade to DataFabric Manager 2.2 or later (up to DataFabric Manager 3.2) before you upgrade to DataFabric Manager 4.0.

Windows installation path when upgrading to DataFabric Manager 3.6 or later

Following are the default installation paths for various software versions:

- DataFabric Manager 3.8 through 4.0.1 on Windows
  32-bit platform: `C:\Program Files\NetApp\DataFabric Manager`
  64-bit platform: `C:\Program Files (x86)\NetApp\DataFabric Manager`
- DataFabric Manager 3.6 or later (up to 3.7.1):
  `C:\Program Files\NetApp\DataFabric`
- Versions earlier than DataFabric Manager 3.6:
  `C:\Program Files\Network Appliance\DataFabric`

Installing OnCommand Unified Manager Core Package in a custom Linux directory

If you used the `-d <new directory>` command to install DataFabric Manager 3.2 or earlier in a custom directory, the software was installed in an NTAPdfm directory that was automatically created within the new directory you specified.

If you use the `-d <new directory>` command to install DataFabric Manager 3.3 or later in a custom directory, the software is installed in the new directory you specify; no additional NTAPdfm directory is created.

Viewing dynamic data

To use Disaster Recovery, the browser that you use to view Operations Manager console must support Java applets.

Conversion of group names from DataFabric Manager 3.1 or earlier

The naming convention for hierarchical groups uses the forward slash character (/) as a separator between levels in the hierarchy. If you upgrade from DataFabric Manager 3.1 or earlier, any group that uses the forward slash character in its name is renamed so that the group is not mistaken for a subgroup in a hierarchy.

Each forward slash character is replaced by a hyphen character (-). If the new name is already in use by another group, OnCommand Unified Manager adds an increasing numeric suffix to the name until an unused name is derived. For example, OnCommand Unified Manager would try to rename group apple/orange to appleorange, then to apple-orange1, then to apple-orange2, and so on, until an unused group name is found.

Upgrade considerations for configuration groups

After upgrading from DataFabric Manager 3.1 or earlier, some administrators of configuration resource groups might gain additional privileges through inheritance. Before upgrading, review the privileges for group hierarchies that include configuration resource groups and make adjustments as necessary.

Upgrading from the Express edition to the Standard edition

The Express edition of OnCommand Unified Manager server has a limit on the number of storage objects it can support. By upgrading to the Standard edition, you can manage more number of storage objects and use additional monitoring functionality suitable for large-scale environments.

Before you begin

- You must be using a dedicated server for the OnCommand Unified Manager server.
- The hardware requirements for the Standard edition must be met.

About this task

You cannot download and install the Express edition as it is no longer supported. Once you upgrade to the Standard edition, you cannot revert back to the Express edition.

While performing the upgrade from your existing Express edition, you are asked if you want to upgrade to the Standard edition. If you enter “no”, the upgrade is aborted.

You must perform the task from a console session on the OnCommand Unified Manager server.

Steps

1. Run the following command for upgrading to the Standard edition:

   ```
   dfm database upgrade standard
   ```

2. When prompted, perform a backup.

   You can skip this step if you have performed a recent backup.

3. Restart all the OnCommand Unified Manager server services by running the following commands:

   ```
   dfm service stop
   ```

   ```
   dfm service start
   ```

4. Verify that the Standard edition is installed successfully by running the following command:

   ```
   dfm about
   ```

Uninstalling OnCommand Unified Manager Core Package

If you are no longer using the package or need additional space, it might be necessary to uninstall and remove packages. When you uninstall the Core Package from your system, the installer automatically removes all components.

Uninstalling OnCommand Unified Manager Core Package from Windows

You can uninstall OnCommand Unified Manager Core Package, for instance, when a Core Package installation is unsuccessful, or when you want to reconfigure your system with a fresh installation. You uninstall the Core Package using the Control Panel application for your operating system.

Before you begin

You must have ensured that there are no other dependencies on the Core Package, because the wizard uninstalls all associated components.

Steps

1. On the Windows server where you installed the Core Package, navigate to the Windows Control Panel and **Control Panel > Programs and Features**.

   For details, see the documentation for your Windows operating system.

2. Scroll through the list of installed programs to find the program that you want to remove.

3. Click the program that you want to uninstall, and then click **Uninstall/Change** or **Change/Remove**, depending on your operating system.

   The NetApp install wizard opens.

4. Select **Remove**, and then click **Next**.

5. Click **Uninstall**.

6. If requested, reboot the system.

   A system reboot is required when, during the uninstallation process, the `\DataFabric Manager\DFM` program directory is not moved to a new directory. The new directory is created with a name that indicates the date and time that you performed the uninstall process: for example, `\DataFabricManager\DFM-20110622140520\`, which specifies that OnCommand Unified Manager Core Package was uninstalled on June 22, 2011, at 2:05:20 PM. When this uninstallation directory is not created, you must reboot to complete the uninstallation process and newly install OnCommand Unified Manager Core Package.

Related tasks

Installing OnCommand Unified Manager Core Package on Windows on page 22

Uninstalling the OnCommand Unified Manager Core Package from Linux

You can use the command `rpm -e` to uninstall the OnCommand Unified Manager Core Package from Linux, for instance, when a Core Package installation is unsuccessful, or when you want to reconfigure your system with a fresh installation.

Before you begin

You must have ensured that there are no other dependencies on the Core Package, because the wizard uninstalls all associated components.

Step

1. At the command prompt, type the command to uninstall the OnCommand Unified Manager Core Package: for example, `rpm -e NTAPdfm`.

   The software automatically uninstalls.

Related tasks

Installing OnCommand Unified Manager Core Package on Linux on page 24

Troubleshooting OnCommand Unified Manager installation and setup

If you encounter unexpected behavior during the installation or when using OnCommand Unified Manager, you can use specific troubleshooting procedures to identify and resolve the cause of such issues.

Address already in use

Description

This message occurs when the Windows computer has run out of outbound ports. A Transmission Control Protocol (TCP) connection has closed, causing the socket pair associated with the connection to go into a TIME-WAIT state. This prevents other connections from using the TCP protocol, source Internet Protocol (IP) address, destination IP address, source port, and destination port for an unknown period of time.

Corrective action

Reduce the length of the TCP TIME-WAIT delay.

See the *Microsoft MSDN library* for more information.

There is a problem with this Windows Installer package

Description

This message occurs when you uninstall an application by using the Add or Remove Programs tool in Windows server. The Windows Installer service manages the installation and removal of programs. If there is a problem with the registration of the Microsoft installation engine, you might not be able to remove programs that you have installed by using the Windows installer.

Corrective action

Unregister and reregister the Windows Installer service. See KB891985 on the *Microsoft support site* for more information.

Cursor displays in multiple locations in the same dashboard panel

Cause

This problem occurs when you use the Firefox browser to open the OnCommand console.

Corrective action

Disable a browser setting in Firefox, as follows:

1. Open the Firefox browser and click the **Tools** menu, then click **Options**.
2. Click the **Advanced** tab.
3. Clear the Always use the cursor keys to navigate within pages option.
4. Restart the Firefox browser.

No related objects are displayed for a virtual object

Issue

No physical servers corresponding to a virtual object are displayed in the Related Objects list in the Server tab of the OnCommand console.

Cause

This problem occurs when you add or register a new host service but the mapping between the physical servers and virtual objects does not occur.

Corrective action

1. Refresh the monitor by opening a console session and type the following command:

   ```
   dfm host discover -m share <storage system>
   ```

2. To view the results, type the following command:

   ```
   dfm details <storage system>
   ```

3. Search for the `shareTimestamp` value to ensure that discovery for the storage system is complete.
4. Click **Rediscover** in the Host Services tab of the OnCommand console to rediscover the host service.
5. Verify that the physical servers are displayed in the Related Objects list in the Server tab.

Could not find any storage mapping for virtual object

Description

This message occurs in the following circumstances:

- When you create a new dataset in the OnCommand console that contains a datastore or a virtual machine from an NFS-based qtree

Corrective action

1. Refresh the monitor by opening a console session and type the following command:

   ```
   dfm host discover -m share <storage system>
   ```

2. To view the results, type the following command:

   ```
   dfm details <storage system>
   ```

   If you created a dataset from an NFS-based qtree, then you must set the export permission for the qtree in the storage system.
3. Search for the `shareTimestamp` value to ensure that discovery for the storage system is complete.
4. Click **Rediscover** in the Host Services tab of the OnCommand console to rediscover the host service.
5. Verify that the physical servers are displayed in the Related Objects list in the Server tab.

Storage mapping fails for virtual machine and datastore created on VMFS datastore using FC LUN

Issue

Host service does not display any storage mapping in the OnCommand console for virtual machine and datastore created on VMFS datastore using FC LUN.

Cause

This problem occurs when you do not correctly unmap an FC LUN from the ESX host and there are non-accessible LUNs in the datastore that you created, the SCSI target might not get updated in the vCenter Server inventory.

Corrective action

Remove the non-accessible LUN and rescan the storage adapter.

Operation timed out

Description

This message occurs when an ESX or vCenter Server is busy creating snapshots or running local backups. In this instance, a copy operation for a restore might timeout from the vCenter server and the restore operation fails.

Corrective action

You can retry the restore operation when the ESX or vCenter Server is not as busy or you can use a different ESX or vCenter Server that is also connected to the same datastores.

Primary key for table is not unique

Description

This message occurs if you move the virtual machine when adding the entire virtual machine folder to the vCenter Server inventory. This causes the new virtual machine to have the same universal unique identifier (UUID) as the virtual machine from which the virtual machine folder was copied, and a UUID conflict occurs causing the host service discovery to fail.

Corrective action

Delete the folder that was moved and then copy the virtual machine folder to the vCenter Server inventory.

Error 1067 while starting the DFM WebUI service

Description

This message occurs during the installation of the Core Package, when the server has Java installation (older, newer, or same version) that sets Java-specific environment variables. This results in the DFM WebUI service failing to start when the installation is complete.

Corrective action

You can uninstall the tool or application that sets the Java-specific environment variables or you can delete these variables when the DFM WebUI service fails to start after you install the Core Package. You can start the service manually by typing the `dfm service start webui/http` command.

Verifying host service to OnCommand Unified Manager server communication

Issue

You can use the `dfm hs diag` command to verify that communication is enabled between the host service and the OnCommand Unified Manager server, and to verify that the host service can communicate with the VMware plug-in. You can use this command to troubleshoot connectivity issues or to verify that communication is enabled before starting a host service backup.

Corrective action

1. On the OnCommand Unified Manager server console, type the following command:

   ```
   dfm hs diag <host service>
   ```

Administrators usergroup does not exist on <vFiler name>

Description

This message occurs when you have a vFiler and you did not run the RBAC monitor for that vFiler, causing the vFiler configuration job for adding the vFiler credentials to the host service to fail.

Corrective action

1. Run the RBAC monitor for the vFiler using the command `dfm host discover -m rbac <Vfiler Name>`.
2. Run the configuration job for the vFiler.

Installing and configuring the Core Package in an MSCS environment

Microsoft Cluster Server (MSCS) provides high-availability protection for your Windows environment.

As part of the OnCommand Unified Manager Core Package installation process, the OnCommand Unified Manager server and its associated services are installed on your system. The cluster resources, including the services for the OnCommand Unified Manager server, the network name, the network address, and the shared data disks, are always online and available on one of the nodes. You must configure the network name and address, and the shared data disks, during the OnCommand Unified Manager Core Package installation process.

When any failure occurs, whether a node failure or a failure of one of the resources, all the resources are automatically moved, or failed over, to the partner node by MSCS.

This failover process is assisted by using a quorum resource on the cluster. The quorum resource is a physical storage device that can be accessed by both nodes in the cluster, although only one node has access to the quorum resource at any given time. The node that has access to the quorum resource is the node that has control of the cluster resource.

Preparing to install the OnCommand Unified Manager Core Package in an MSCS environment

To ensure high availability of the OnCommand Unified Manager server, you must configure the services to be accessible through a network name and a network address. The OnCommand Unified Manager server can also use this network name or network address; therefore, you do not have to add new network resources for the services.

An MSCS cluster that is configured with the OnCommand Unified Manager server consists of two nodes, each node running the same version of the OnCommand Unified Manager server.

All of the OnCommand Unified Manager server data (database files, Performance Advisor files, and so on) is configured to be accessed from a shared data disk.

Prerequisites for installing the OnCommand Unified Manager Core Package in MSCS

Before installing the Core Package in MSCS, you must set up two Windows servers running on identical hardware platforms. You must ensure that all the requirements and guidelines for configuring cluster servers are met, according to the MSCS documentation.

During the MSCS setup, you must ensure that you have completed the following actions:

- Creating a shared data disk to be used as a quorum resource.
- Creating a network name resource and a network address resource.
- Adding cluster resources to a resource group.

Related information

Introducing Microsoft Cluster Service (MSCS)

Configuration requirements for the OnCommand Unified Manager Core Package in MSCS

You must meet specific configuration requirements when you set up your MSCS environment to use OnCommand Unified Manager Core Package.

To ensure OnCommand Unified Manager Core Package installs and functions properly in an MSCS environment, the following MSCS configuration conditions must exist:

- Microsoft Windows servers running Windows 2008 Enterprise Edition, or Data Center Edition have the same patch versions on identical hardware.

  Note: MSCS is not supported on Windows Server 2008 and Windows Server 2008 R2. However, you can configure DataFabric Manager 3.8 or later for high availability on these platforms by using Failover Clustering. For more details, see the technical report on *High-Availability Support for DataFabric Manager server*.

- The OnCommand Unified Manager server is connected to the storage system using either iSCSI or Fibre Channel (FC), and it is in a SAN environment.
- FC switched fabric or iSCSI-based storage is used for shared data disks with a NetApp storage system as the storage back end.
- Members of the cluster are member servers, and not domain controllers.
- The same version of OnCommand Unified Manager Core Package is installed using the same path on both of the cluster nodes: for example, `C:\Program Files\NetApp\DataFabric Manager\DFM`.
- All OnCommand Unified Manager server administrators are domain users, rather than local system users, so that the user login is successful even when the OnCommand Unified Manager server services fail over to the partner node.
- 64-bit Perl in Windows 64-bit 2008 server is installed, to run OnCommand Unified Manager server configuration scripts.

Related information

Technical report on High-Availability Support for OnCommand Unified Manager server: media.netapp.com/documents/tr-3767.pdf

Configuration limitations for the OnCommand Unified Manager Core Package in MSCS

OnCommand Unified Manager Core Package in MSCS is not supported on certain environmental conditions of the MSCS environment.

The following are configuration limitations of installing OnCommand Unified Manager Core Package in an MSCS environment:

- IPv6 virtual IP address on failover clustering is supported on Windows 2008 only.
- Quorum type “node and disk majority” in Failover Cluster is supported on Windows 2008 server only.
- OnCommand Unified Manager Core Package in MSCS is not supported on Windows running in a virtual machine.
- OnCommand Unified Manager server does not support a host service created as a generic service from failover cluster manager in Microsoft Windows.

Installing the OnCommand Unified Manager Core Package in an MSCS environment

Before installing the OnCommand Unified Manager Core Package, you must configure MSCS with a shared disk for a quorum resource, assign a network name and a network address, place the cluster resources in a cluster resource group.

After the installation is complete, you have to add OnCommand Unified Manager server services to MSCS. You must install OnCommand Unified Manager Core Package on the first node, and repeat on the second node.

Configuring MSCS for the OnCommand Unified Manager Core Package installation

Before you install OnCommand Unified Manager Core Package in MSCS, you must configure your MSCS environment.

About this task

You must complete this task by using Cluster Administrator in the MSCS interface. See the MSCS documentation for more details.

You must configure MSCS to create the following:

- A shared quorum disk, which is used for storing the cluster configuration information
- A network name and a network address, which are used for managing the cluster server and the OnCommand Unified Manager server
- A resource group to store the resources so that all these resources are available to both the cluster nodes

Steps

1. Select a domain user and add the domain user to the **Administrators Group** on both the cluster nodes.

   Example

   Enter the following command in **Administrators Group**:

   `domain\dfmuser`

2. Create a shared data disk:

   a. Make the disk accessible to both the cluster nodes.

   b. Map the disk to a drive letter (such as drive `S:`).

      Note: The data disk should be mapped to the same drive letter on both the cluster nodes.

   c. Add the shared data disk, as a physical disk resource, to the cluster server.

   This disk is a resource for storing data specific to OnCommand Unified Manager Core Package.

3. Verify that the new resource group can successfully fail over to the partner node.

Result

Cluster Administrator displays the resources, nodes, and groups. In addition to the content displayed after the initial setup, Cluster Administrator displays a physical disk resource named Disk `S:`.

Related information

Introducing Microsoft Cluster Service (MSCS): http://msdn.microsoft.com

Installing the OnCommand Unified Manager Core Package in MSCS

You can install the OnCommand Unified Manager Core Package in MSCS to ensure high availability in a Windows environment. You must install the OnCommand Unified Manager Core Package on the first node, and repeat the installation procedure on the second node.

Before you begin

The following conditions must be met:

- Microsoft Cluster Server is installed and configured on both the nodes of the cluster.
- The preinstallation tasks are completed.
- You must have the Core license key.
- The workstation meets the hardware requirements.
- You have Local Administrator login permission for the OnCommand Unified Manager server.
- If you are upgrading from a previous version of the OnCommand Unified Manager server, you should back up your database before the installation or during the installation process.
- The OnCommand Unified Manager Core Package installer from the NetApp Support Site is downloaded.

About this task

The two OnCommand Unified Manager server nodes are configured to use the same database and to monitor the same set of nodes. Therefore, you can install the same license on both the nodes.

If you are upgrading from an earlier licensed version of OnCommand Unified Manager server, you do not require a license key. Both the installation and upgrade processes automatically install the AutoSupport feature with AutoSupport enabled and display a message about how to disable the feature.

Steps

1. Log in to the first node of the cluster pair as a domain user, with administrator privileges on the local system.
2. Open the **Cluster Administrator** interface and select **Owner** of the Resources folder, to ensure that the node owns the cluster resources.
3. Run the executable file.
4. Follow the setup prompts to complete the installation and note the installation directory path for later reference.
5. Stop the OnCommand Unified Manager server services after the installation is complete by entering the following command:

   ```
   dfm service stop
   ```

Attention: You should perform all cluster operations by using either Cluster Administrator or `cluster.exe`. Except where specifically indicated in installation and configuration procedures, you must not use the `dfm service start` and `dfm service stop` commands. These commands interfere with cluster operations.

6. Move the cluster resources to the second node by using the **Move Group** option in MSCS.
7. Log in to the second node of the cluster pair as a domain user, with administrator privileges on the local system.

   Note: You must log in with the same user name you used on the first node.
8. Install the Core Package on the second node at the same directory path that you used on the first node.
9. Stop the OnCommand Unified Manager server services on the second node by entering the following command:

   ```
   dfm service stop
   ```
10. Disable the automatic start-up of the OnCommand Unified Manager server by entering the following command on both the nodes:

    ```
    dfm service enable -m
    ```

After you finish

You can start configuring both the cluster nodes by using the configuration scripts that are provided with the installation, or you can perform the configuration manually.

Related concepts

Preparing to install the OnCommand Unified Manager Core Package in an MSCS environment on page 57

OnCommand Unified Manager Core Package hardware and software requirements on page 12

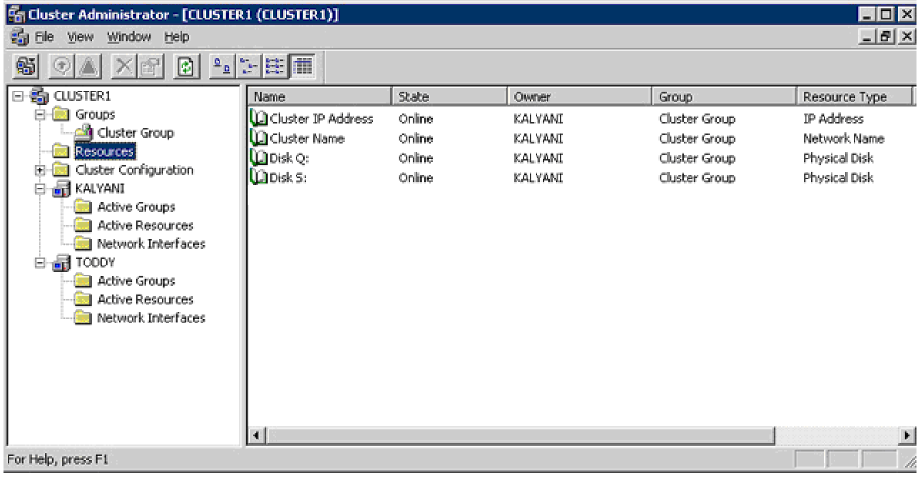
Related information

The NetApp Support Site - mysupport.netapp.com

Example of the MSCS initial setup

You should understand how the cluster, the nodes, the physical disk, the network name, and the network IP address are displayed in the Cluster Administrator interface.

The following image is an example of the Cluster Administrator interface after the initial setup of MSCS:



Name	State	Owner	Group	Resource Type
Cluster IP Address	Online	KALYANI	Cluster Group	IP Address
Cluster Name	Online	KALYANI	Cluster Group	Network Name
Disk Q:	Online	KALYANI	Cluster Group	Physical Disk
Disk S:	Online	KALYANI	Cluster Group	Physical Disk

The configuration displayed in this example is as follows:

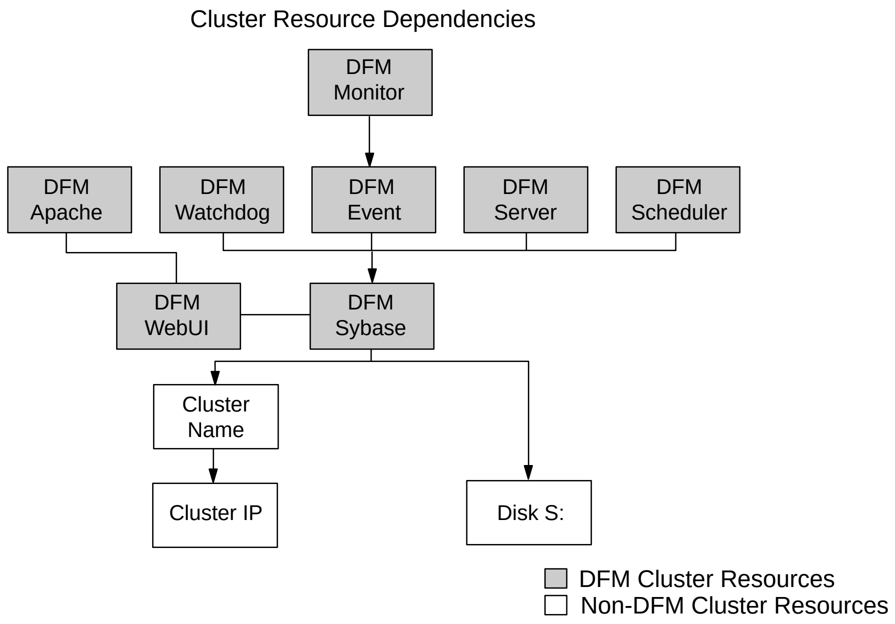
- The cluster name is Cluster 1.
- The first node name is Kalyani.
- The second node name is Toddy.
- The physical disk, the shared disk quorum resource, is created with the name Disk Q: and is mapped to drive letter Q:.
- The network name resource is called Cluster Name.
- The network IP Address resource is called Cluster IP Address.

OnCommand Unified Manager server service resources added to MSCS

You must add the OnCommand Unified Manager server cluster service resources to MSCS. The services include DFM Monitor, DFM Apache, DFM Watchdog, DFM Event, DFM Server, DFM Scheduler, DFM WebUI, and DFM Sybase.

These services are used for various purposes, such as monitoring storage systems, scheduling jobs, serving HTTP requests and executing servlets, processing events and database queries, and monitoring all the other services.

The following illustration shows the services and the dependencies among the various resources:



Configuring the OnCommand Unified Manager Core Package in an MSCS environment

When you install the OnCommand Unified Manager Core Package, the OnCommand Unified Manager server services are installed with it. To achieve high availability, you must add the OnCommand Unified Manager server cluster services to MSCS. You can configure the services either by using scripts or by adding the services manually.

The following service resources are added to MSCS:

- DFM Monitor
- DFM Apache
- DFM Watchdog
- DFM Event
- DFM Server
- DFM Scheduler
- DFM WebUI
- DFM Sybase

Adding the cluster services using a script

You can configure OnCommand Unified Manager server in your cluster environment by running a configuration script.

Steps

1. Log in to the node that owns cluster resources.
2. Move the OnCommand Unified Manager server data to the shared data disk by entering the following command:

   `dfm datastore setup` ***`new_clusterdisk_directory`***

3. Stop the OnCommand Unified Manager server services by entering the following command:

   `dfm service stop`

   This ensures that the OnCommand Unified Manager server does not try to access the data disk to be moved to the secondary node.

4. Ensure that the OnCommand Unified Manager server services do not start automatically by entering the following command:

   `dfm service enable -m`

   The `-m`option ensures that the OnCommand Unified Manager server services do not start automatically.

5. Manually move the cluster group to the second node.

6. Verify that the secondary node owns the cluster resources.

7. Enter the following commands on the secondary node:

   `dfm service enable -m`

   `dfm datastore setup -n` ***`drive_name`***

   > **Note:** You must ensure that you use the same drive letter for the secondary node as the first node. The `-n` option ensures that the data is not copied again to the shared data disk.

8. Access the directory at `C:\Program Files\NetApp\DataFabric Manager\DFM\examples` or `/opt/NTAPdfm/examples`, and `C:\Program Files(x64)\NetApp\DataFabric Manager\DFM\examples for x64-bit platform`.

9. Configure the OnCommand Unified Manager server services in your cluster environment by running the following script:

   `dfmcluster_add_resources.pl -t` ***`cluster_type`*** **`-g`** ***`cluster_group`*** **`-i`** ***`cluster_ip_resource`*** **`-n`** ***`cluster_nameresource`***

Script options for configuring services in MSCS

You can use a configuration script to add the OnCommand Unified Manager server generic service resources to MSCS.

The command to add services to the OnCommand Unified Manager server is as follows:

`perl dfmcluster_add_resources.pl` ***`option name`*** **`...`**

The `perl dfmcluster_add_resources.pl` command includes the following options:

`-t` ***`cluster_type`***

Cluster solution used for high availability. The values are **`mscs`** (default) and **`vcs`**.

`-g` ***`cluster_group`***

Name of the cluster group to which the resources are added. This group already includes the other resources.

`-i` ***`cluster_ip_resource`***

Name of the cluster IP resource that is displayed under the Name column in the Cluster Administrator.

`-n` ***`cluster_nameresource`***

Name of the cluster name resource.

`-k` ***`data_disk_resource`***

Name of the data disk resource.

Example

```
perl dfmcluster_add_resources.pl -g ClusterGroup1 -i 172.24.1.20 -n
Cluster1 -k Disk S:
```

Bringing OnCommand Unified Manager server cluster services online in MSCS

After you add the OnCommand Unified Manager server services to MSCS, you must bring the services online.

Steps

1. In the MSCS interface, select **Cluster Group** under the Groups folder.
2. Click **File**, and then click **Bring Online**.

Configuring OnCommand Unified Manager server to use the cluster name in MSCS

When OnCommand Unified Manager server sends e-mail alert messages to administrators, the OnCommand Unified Manager server uses the local system name in the URL, by default. These local system names are not accessible to users in the cluster. Therefore, you must configure OnCommand Unified Manager server to use the cluster name instead.

Step

1. Configure the OnCommand Unified Manager server to use the cluster name by entering the following command:

   ```
   dfm option set localHostName=fqdn-of-cluster
   ```

   FQDN is the fully qualified domain name of the cluster.

Configuring OnCommand Unified Manager server in MSCS manually

You can manually configure OnCommand Unified Manager server in MSCS, which allows you to customize the setup of the cluster. For example, you can move different OnCommand Unified Manager server data files to different shared data disks. However, you cannot move the data files using the configuration scripts.

Configuring OnCommand Unified Manager server services on the first node in MSCS

You must configure the OnCommand Unified Manager server by manually adding the OnCommand Unified Manager server services.

Before you begin

You must be logged in as a domain user, with administrative privileges on the local system, to access the shared data drive. By default, the OnCommand Unified Manager server services run using the local system account, and therefore do not provide access to the shared drive where the database files and other files reside.

Steps

1. In the **Cluster Administrator** interface, select the **Owner** field of the **Resources** folder.
2. Verify that the first node owns the resource group named Cluster Group.
3. Stop the OnCommand Unified Manager server services by entering the following command:

```
dfm service stop
```

Attention: You should perform all cluster operations by using either Cluster Administrator or `cluster.exe`. Except where specifically indicated in installation and configuration procedures, you must not use the `dfm service start` and `dfm service stop` commands. These commands interfere with cluster operations.

4. Specify a user account in the **Logon As** field:
    a. Open the **Services** page from Windows **Control Panel**.
    b. Double-click **DFM Sybase ASA**.
    c. In the **General** tab, change the **Startup type** option to **Manual**.
    d. Click **Apply**.
5. Click the **Log On** tab.
6. Enter the name of the domain user account that you want to use to access the OnCommand Unified Manager server service from the shared drive.
7. Click **OK**.
8. Repeat Steps 4 through 7 to add the cluster services.

    You must add the following services in the **Administrative Tools**: DFM Monitor, DFM Apache, DFM Watchdog, DFM Event, DFM Server, DFM Scheduler, DFM WebUI

After you finish

You must move the OnCommand Unified Manager server data files to a shared disk.

Moving OnCommand Unified Manager server data files to a shared disk

You must configure the OnCommand Unified Manager server to allow access to data files in a shared disk.

Steps

1. For the first node, move the database files to a nonroot folder in the shared data drive.

    The default location for database files is `*installation_directory*\data`.

    Example

    ```
    S:\dfm\data
    ```

2. Ensure that the OnCommand Unified Manager server points to the relocated database by entering the following command:

    ```
    dfm database set dbDir=S:\dfm\data
    ```

3. Verify that all the services are stopped by entering the following command:

    ```
    dfm service list
    ```

4. Move the following data files to appropriate folders in the shared disk:
    - Performance Advisor data files
      The default location is *`installation_directory`*`\perfdata` (for example, `S:\dfm\perfdata`).
    - Script plug-in files

The default location is *installation_directory*\script-plugins (for example, S:\dfm\script-plugins).

- Configuration Management plug-in files
  The default location is *installation_directory*\plugins (for example, S:\dfm\plugins).
- Archived reports
  The default location is *installation_directory*\reports (for example, S:\dfm\reports).

5. Start the SQL service by entering the following command:

   ```
   dfm service start sql
   ```

6. Set the options to point to the new location of the relocated files by entering the following commands:

   a. **dfm option set *perfArchiveDir*=S:\dfm\perfdata**

   b. **dfm option set *pluginsDir*=S:\dfm\plugins**

   c. **dfm option set *scriptDir*=S:\dfm\script-plugins**

   d. **dfm option set *reportsArchiveDir*=S:\dfm\reports**

   Note: The dfm option set command prompts you to start the services after setting each option. However, you must start the services only after you complete setting all the options.

7. Stop the SQL service by entering the following command:

   ```
   dfm service stop sql
   ```

Configuring OnCommand Unified Manager server services on the second node in MSCS

After the first node is configured to allow access to all data files from a shared disk, you must configure the second node to allow the same access.

Before you begin

You must be logged in as a domain user, with administrative privileges on the local system, to access the shared data drive. By default, the OnCommand Unified Manager server services run using the local system account, and therefore do not provide access to the shared drive where the database files and other files reside.

Steps

1. In the **Cluster Administrator** interface, select the **Owner** field of the **Resources** folder.
2. Verify that the first node owns the resource group named Cluster Group.
3. Stop the OnCommand Unified Manager server services by entering the following command:

   ```
   dfm service stop
   ```

   Attention: You should perform all cluster operations by using either Cluster Administrator or cluster.exe. Except where specifically indicated in installation and configuration procedures, you must not use the dfm service start and dfm service stop commands. These commands interfere with cluster operations.

4. Specify a user account in the **Logon As** field:

   a. Open the **Services** page from Windows **Control Panel**.

   b. Double-click **DFM Sybase ASA**.
   c. In the **General** tab, change the **Startup type** option to **Manual**.
   d. Click **Apply**.

5. Click the **Log On** tab.
6. Enter the name of the domain user account that you want to use to access the OnCommand Unified Manager server service from the shared drive.
7. Click **OK**.
8. Repeat Steps 3 through 6 to add the cluster services.

   You must configure all the services for the cluster to start working. You must enter the following cluster service names in the **Services** tab in **Administrative Tools**:

   - DFM Monitor
   - DFM Apache
   - DFM Watchdog
   - DFM Event
   - DFM Server
   - DFM Scheduler
   - DFM WebUI
9. Verify that all the services are stopped by entering the following command:

   ```
   dfm service list
   ```

Configuring OnCommand Unified Manager server services as cluster resources in MSCS

After you install the OnCommand Unified Manager server services, you have to configure them as cluster resources and make them available to both nodes.

Before you begin

- The dependencies that exist between the various cluster resources must be determined.
  A dependency requires that one service must be running before its associated service can be brought online. For example, most services cannot function unless Sybase ASA is already running.
- You must be logged in to the node as a domain use, with administrator privileges on the local system.

About this task

You can use the following table to add the resource name, dependencies, and service name when configuring each new cluster service:

Resource name field	Dependencies field	Service name field
DFM Sybase ASA	Cluster IP, Cluster Name, Shared Data Disk, Data Disk	DFMSybase
DFM Apache	DFM Sybase ASA, DFM WebUI	DFMApache
DFM Scheduler	DFM Sybase ASA	DFMScheduler

Resource name field	Dependencies field	Service name field
DFM Watchdog	DFM Sybase ASA	DFMWatchdog
DFM Server	DFM Sybase ASA	DFMServer
DFM Event	DFM Sybase ASA	DFMEvent
DFM Monitor	DFM Event	DFMMonitor
DFM WebUI	DFM Sybase ASA	DFMWebUI

Steps

1. In the **Cluster Administrator** interface, select the **Owner** field of the Resources folder and verify that the node owns all the cluster resources.
2. In the console tree, double-click the **Groups** folder.
3. In the **Details** pane, click the group named **Cluster Group**.
4. Select **File** menu, and then select **New > Resource**.
5. On the **New Resource** page, complete the following steps:
   a. Enter the resource name in the **Name** field.
   b. Select **Generic Service** as the **Service Type**.
   c. Select **Cluster Group** as the group.
   d. Click **Next**.
6. On the **Possible Owners** page, complete the following steps:
   a. Add both nodes as the possible owners of the resource.
   b. Click **Next**.
7. On the **Dependencies** page, complete the following steps:
   a. Add dependencies related to the new service in the **Dependencies** field.

      Example

      Set **DFM Sybase ASA Dependencies** as the cluster IP address, cluster name, disk S:, and data disk.

   b. Click **Next**.
8. On the **Generic Service Parameters** page, complete the following steps:
   a. Enter the name of the service in **Service Name**.

      Example

      Set the name to DFM Sybase.

   b. Clear the **Use Network name for computer name** option.
9. On the **Registry Replication** page, click **Finish**.

   Note: You do not have to perform registry replication.
10. Repeat Steps 5 through 9 for every OnCommand Unified Manager server service.

Related references

OnCommand Unified Manager server service resources added to MSCS on page 62

Bringing OnCommand Unified Manager server cluster services online in MSCS

After you add the OnCommand Unified Manager server services to MSCS, you must bring the services online.

Steps

1. In the MSCS interface, select **Cluster Group** under the Groups folder.
2. Click **File**, and then click **Bring Online**.

Configuring a host service in MSCS

When you add a new host service in a cluster environment, you must ensure that both nodes in a cluster pair have access to the keys folder. This ensures that when one node fails, the second node of the cluster pair starts functioning.

Steps

1. Copy the keys folder from one node to the other in the cluster pair at `installation_directory\conf`.
2. In the **Cluster Administrator** interface, select the cluster group and click **Move group**, or manually move the cluster group to the second node and verify that the second node owns the resources.
3. Enter the following command on the second node to start using the new setting:

   ```
   dfm ssl service reload
   ```
4. Launch the OnCommand console and verify that the host service status is Up in the **Host Services** tab.

Managing OnCommand Unified Manager server in an MSCS environment

You can create and restore backups, set HTTPS options, and configure OnCommand Unified Manager server to share data on the OnCommand Unified Manager server cluster nodes.

Best practices to start and stop OnCommand Unified Manager server services in MSCS

After you set up OnCommand Unified Manager server in MSCS, do not use the `dfm service start` and `dfm service stop` commands, except where specifically indicated in installation and configuration procedures. These commands interfere with the working of MSCS.

You must start or stop all operations by using either the Cluster Administrator in MSCS or the `cluster.exe` command.

Note: Do not change the Service startup type to `Automatic` in the Service Control Manager on any of the nodes. You must ensure that this option is set to `Manual`.

Restoring the OnCommand Unified Manager server database in MSCS

Restoring a database enables the OnCommand Unified Manager server to use the current settings. You can restore the database by using Cluster Administrator.

Steps

1. Log in to the node that currently owns the cluster resources.
2. In **Cluster Administrator**, take the services offline by completing the following steps:
   a. Right-click the **DFM Sybase** service.
   b. Select **Take offline**.
      The other services are also taken offline.
3. Restore the database by entering the following command in the OnCommand console:
   ```
   dfm backup restore
   ```
4. Stop all the services by entering the following command in the OnCommand console:
   ```
   dfm service stop
   ```
5. In **Cluster Administrator**, bring the OnCommand Unified Manager server services online:
   a. Select **Cluster Group** under the Groups folder.
   b. Click **File**, and click **Bring Online**.

Configuring OnCommand Unified Manager server to use HTTPS in MSCS

You can configure OnCommand Unified Manager server to use HTTPS on both the cluster nodes for secure data transfers.

About this task

HTTPS is first set up with an SSL certificate, and then the HTTPS option is enabled on both the nodes.

Steps

1. Log in to the first node in the cluster.
2. In **Cluster Administrator**, take the OnCommand Unified Manager server services offline:
   a. Right-click the **DFM Sybase** service.
   b. Select **Take offline**.
      The other services are also taken offline.
3. Start the SQL service by entering the following command in the OnCommand console:
   ```
   dfm service start sql
   ```
4. Create an SSL certificate for HTTPS by entering the following command:
   ```
   dfm ssl server setup
   ```
   This creates two files, `server.crt` and `server.key`, in the *`installation_directory`* `\conf` folder.
5. Set the OnCommand Unified Manager server option to enable HTTPS by entering the following command:

```
dfm option set httpsEnabled=yes
```

6. Start the HTTP service by entering the following command:

   ```
   dfm service start http
   ```

   Starting the service using `dfm service start` re-creates the `httpd.conf` file with the changed options.

   Attention: You should perform all cluster operations by using either Cluster Administrator or `cluster.exe`. Except where specifically indicated in installation and configuration procedures, you must not use the `dfm service start` and `dfm service stop` commands. These commands interfere with cluster operations.

7. Ensure that the OnCommand Unified Manager server services are offline.

   If the services are not offline, the HTTP service is not enabled on the other node, because the configuration is not complete.

8. Stop all the services by entering the following command:

   ```
   dfm service stop
   ```

9. In **Cluster Administrator**, move the cluster group to the second node by using the **Move Group** option.

10. Log in to the second node in the cluster.

11. Copy the `server.crt` and `server.key` files created on the first node to the *`installation_directory`*`\conf` folder in the second node.

12. Start the services and verify that they are operating as required by entering the following command:

    ```
    dfm service start
    ```

    Starting the service by using `dfm service start` re-creates the `httpd.conf` file with the changed options.

13. Stop the services by entering the following command:

    ```
    dfm service stop
    ```

14. In **Cluster Administrator**, bring the OnCommand Unified Manager server services online:

    a. Select **Cluster Group** under the Groups folder.

    b. Click **File**, and click **Bring Online**.

Changing HTTP options in an MSCS environment

You can change the HTTP options to enable HTTPS, or change the default HTTP and HTTPS ports.

Steps

1. Log in to the first node in the cluster.

2. In **Cluster Administrator**, take the OnCommand Unified Manager server services offline:

   a. Right-click the DFM Sybase service.

   b. Select **Take offline**.

   The other services are also taken offline.

3. Start the SQL service by entering the following command:

   ```
   dfm service start sql
   ```

> **Attention:** You should perform all cluster operations by using either Cluster Administrator or `cluster.exe`. Except where specifically indicated in installation and configuration procedures, do not use `dfm service start` and `dfm service stop`. These commands interfere with cluster operations.

4. Set the required HTTP option by entering the following command:

   ```
   dfm option set option-name=option-value
   ```

   Example

   ```
   dfm option set httpsPort=443
   ```

5. Start the HTTP service by entering the following command:

   ```
   dfm service start http
   ```

   Starting the service by using `dfm service start` re-creates the `httpd.conf` file with the changed options.

6. Stop all the services by entering the following command:

   ```
   dfm service stop
   ```

   > **Note:** You must ensure that OnCommand Unified Manager server services are offline before proceeding. Otherwise, HTTP is not enabled on the other node because the configuration is not complete.

7. In **Cluster Administrator**, move the cluster group to the second node by using the **Move Group** option.

8. Log in to the second node in the cluster.

9. Start the services by entering the following command:

   ```
   dfm service start
   ```

10. Stop the services by entering the following command:

    ```
    dfm service stop
    ```

11. In **Cluster Administrator**, bring the OnCommand Unified Manager server services online:

    a. Select **Cluster Group** under the Groups folder.

    b. Click **File**, and click **Bring Online**.

OnCommand Unified Manager server monitoring in MSCS

Microsoft provides the Server Clusters Management Pack as part of Microsoft Operations Manager. You can monitor the cluster server, and report node status, resource status, and alerts by using Cluster Administrator in MSCS. OnCommand Unified Manager server does not provide any additional cluster monitoring or alerting functionality.

Data shared by MSCS cluster nodes

You must configure the OnCommand Unified Manager server Microsoft Cluster Server (MSCS) nodes to access files from a shared disk. Using a shared disk ensures that any updates to these files are reflected in the files of the other nodes in the cluster after a failover.

The MSCS cluster nodes share the following files:

***installation_directory*\data**

Sybase database files

***installation_directory*\perfdata**

Performance Advisor data files

***installation_directory*\scriptplugins**

Installed script plug-ins and related files

***installation_directory*\plugins**

Storage system configuration plug-ins

***installation_directory*\reports**

Archived reports

***installation_directory*\dataExport**

OnCommand Unified Manager server and Performance Advisor data

***installation_directory*\jetty**

Libraries and Web application files

***installation_directory*\conf\keys**

Encryption keys

Data that is not shared by MSCS cluster nodes

Files such as executables, configuration files, and licenses are not shared by the MSCS cluster nodes. This ensures that the same version is maintained in the cluster nodes.

The following files are not shared:

***installation_directory*\bin**

Executable files

***installation_directory*\conf**

Configuration files

***installation_directory*\docs**

Third-party licenses

***installation_directory*\examples**

Cluster configuration scripts, and so on

***installation_directory*\log**

Log files

***installation_directory*\misc**

Configuration files

***installation_directory*\sbin**

Third-party executables

***installation_directory*\scripts**

Sybase_install.sql

***installation_directory*\src**

Storage system configuration plug-ins

***installation_directory*\web\clients**

Performance Advisor clients

***installation_directory*\web\com**

JAR files for applets

***installation_directory*\web\help**
Help files

***installation_directory*\web\man**
Manual pages

***installation_directory*\web\media**
Images used on Web interfaces

***installation_directory*\web\scripts**
Java script files

***installation_directory*\web\styles**
CSS style sheets

***installation_directory*\perfExport**
Exported performance counter data for specified objects

Uninstalling the OnCommand Unified Manager Core Package in an MSCS environment

You can uninstall the OnCommand Unified Manager Core Package from a cluster by deleting the cluster services from each cluster node.

Steps

1. In **Cluster Administrator**, delete all the OnCommand Unified Manager server services:
    a. Right-click the **DFM Sybase** resource.
    b. Select **Delete**.

    The other OnCommand Unified Manager server services are also deleted.
2. Log in to any one of the cluster nodes.
3. From the Windows Add or Remove Programs utility, uninstall the OnCommand Unified Manager Core Package.
4. Repeat Steps 2 through 3 for the other nodes.

Upgrading OnCommand Unified Manager Core Package in an MSCS environment

You must ensure that all of the nodes in the cluster are upgraded to the correct OnCommand Unified Manager Core Package version.

Before you begin

- The OnCommand Unified Manager Core Package installer must be downloaded from the NetApp Support Site.
- You must have created a backup of the existing OnCommand Unified Manager server database.
- The database must be present in the following path: `INSTALL_DIR/DFM/data`.
  The database files `monitordb.db` and `monitordb.log` must be available on the shared disk.
- The DFM WebUI services must be added to OnCommand Unified Manager server.

Steps

1. From **Cluster Administrator**, take the OnCommand Unified Manager server services offline:

   a. Right-click the DFM Sybase service.

   b. Select **Take offline**.

   The other services are also taken offline.

2. Select the **Owner** field of the **Resources** folder so that the first node owns the resource group named Cluster Group.

3. Upgrade to the OnCommand Unified Manager Core Package installation on the first node:

   a. Run the executable file.

   b. Follow the setup prompts to complete the installation.

4. Stop all OnCommand Unified Manager server services:

   ```
   dfm service stop
   ```

   Attention: You should perform all cluster operations by using either Cluster Administrator or the `cluster.exe` command. Except where specifically indicated in installation and configuration procedures, you must not use the `dfm service start` and `dfm service stop` commands. These commands interfere with cluster operations.

5. Disable the automatic service start-up during reboot:

   ```
   dfm service enable -m
   ```

6. In **Cluster Administrator**, move the cluster group to the second cluster node by selecting the group name in **Services and Applications**, and then click **Move this service or application to other node**.

7. Select the **Owner** field of the **Resources** folder to upgrade the second node.

   You must ensure that the second node owns all the cluster resources.

8. Repeat step *3* on page 76 to upgrade to the OnCommand Unified Manager Core Package installation on the second node.

9. Stop all OnCommand Unified Manager server services:

   ```
   dfm service stop
   ```

10. Optional: Move the OnCommand Unified Manager server data to the shared data disk:

    ```
    dfm datastore setup -n -d INSTALL_DIR/DFM/data
    ```

    Important: You must perform this step if you are upgrading to OnCommand Unified Manager Core Package 5.1 or later from any version from OnCommand Unified Manager server 3.8 through OnCommand Unified Manager Core Package 5.0.

    Note: The `-n` option forces the server to use the database present at the specified path.

11. Point the Sybase database to use the new database:

    ```
    dfm datastore setup -n -d LUN_PATH
    ```

12. Check the status of the SQL service:

    ```
    dfm service list sql
    ```

    If the service is not running, you must run the `dfm service start sql` command.

13. Disable the automatic service start-up during reboot:

```
dfm service enable -m
```

14. In **Cluster Administrator**, click the console tree, and then double-click the **Groups** folder.
15. In the **Details** pane, click the group named **Cluster Group**.
16. Select the **File** menu, and then select **New > Resource**.
17. On the **New Resource** page, complete the following steps:
    a. In the **Name** field, enter the following name:

       ```
       DFM WebUI
       ```

    b. Select **Generic Service** as the **Service Type**.

    c. Select **Cluster Group** as the group.

    d. Click **Next**.
18. On the **Possible Owners** page, add both the nodes as the possible resource owners, and then click **Next**.
19. On the **Dependencies** page, add DFM Sybase ASA as a dependency on DFM WebUI, and then click **Next**.
20. On the **DFM Apache Properties page**, set DFM WebUI to be dependent on DFM Apache.
21. On the **Generic Service Parameters** page, complete the following steps:
    a. In the **Service Name** field, enter the following name:

       ```
       DFM WebUI
       ```

    b. Clear the **Use Network name for computer name** option.
22. Bring the OnCommand Unified Manager server services online:
    a. Select **Cluster Group** under the **Groups** folder.

    b. Click **File**, and then click **Bring Online**.
23. Set the database path back to the upgraded database on the LUN:

    ```
    dfm datastore setup -n -d LUN_PATH
    ```

Related tasks

Configuring OnCommand Unified Manager server on the cluster nodes in VCS on page 83

Installing and configuring the Core Package in a VCS environment

Veritas Cluster Server (VCS) provides high-availability protection for cluster configurations.

As part of the OnCommand Unified Manager Core Package installation process, the OnCommand Unified Manager server and its associated services are installed on your system. The cluster resources, including the services for the OnCommand Unified Manager server, the network name, the network address, and the shared data disks, are always online and available on one of the nodes. You must configure the network name and address, and the shared data disks, during the OnCommand Unified Manager Core Package installation process.

When a resource node failure is detected, all the resources are automatically moved, or failed over, to the partner node by VCS.

Preparing to install OnCommand Unified Manager Core Package in a VCS environment

To ensure high availability of the OnCommand Unified Manager server, you must configure the services to be accessible through a network name and a network address. The OnCommand Unified Manager server can also use this network name or network address; therefore, you do not have to add new network resources for the services.

A VCS cluster configured with the OnCommand Unified Manager server consists of two nodes, each node running the same version of the OnCommand Unified Manager server. All of the OnCommand Unified Manager server data (database files, Performance Advisor files, and so on) is configured to be accessed from a shared data disk.

Prerequisites for installing OnCommand Unified Manager Core Package in VCS

Before installing OnCommand Unified Manager Core Package in Veritas Cluster Server (VCS), you must ensure that the VCS configuration requirements are met.

VCS must be installed according to the instructions provided in the *Veritas Cluster Server 5.0 Installation Guide*

Related information

Veritas Cluster Server - http://www.symantec.com/business/cluster-server
Symantec Support - http://www.symantec.com/business/support

Configuration requirements for OnCommand Unified Manager Core Package in VCS

Before installing OnCommand Unified Manager Core Package in Veritas Cluster Server (VCS), you must ensure that the cluster nodes are properly configured to support the OnCommand Unified Manager software.

You must ensure that the VCS configuration meets the following requirements:

- Both of the cluster nodes must be running a supported operating system version.
  The minimum supported operating systems are Red Hat Enterprise Linux 5.6 and SUSE Linux Enterprise Server 10 with SP3.

- The same version of OnCommand Unified Manager Core Package must be installed using the same path on both of the cluster nodes.
- Native ext3 File System and Logical Volume Manager (LVM) must be used.
- The OnCommand Unified Manager server should be connected to the storage system using Fibre Channel (FC).

  You must also ensure that the FC link is active and that the LUNs created on the storage systems are accessible to both of the cluster nodes.
- The shared data disk must have enough space to accommodate the OnCommand Unified Manager server database, performance data, and script plug-in folders.
- A minimum of two network interfaces must be set up on each system: one for node-to-node communication and the other for node-to-client communication.

  The name of the network interface used for node-to-client communication should be the same on both the systems.
- A separate heartbeat link must be established between the cluster nodes; otherwise, the network interface is used to communicate between the cluster nodes.

Configuration limitations for the OnCommand Unified Manager Core Package in VCS

You must be aware of the configuration limitations before you install the OnCommand Unified Manager Core Package in a VCS environment.

The following are configuration limitations in VCS:

- Only two-node clusters are supported.
- The OnCommand Unified Manager Core Package in VCS is not supported on VMware.
- For shared disks, the storage back-end must be an FC-based storage only.
- iSCSI storage is not supported for the OnCommand Unified Manager Core Package in VCS.

Installing OnCommand Unified Manager Core Package in a VCS environment

You must install Veritas Storage Foundation first and then install OnCommand Unified Manager Core Package in VCS. After you install these on both the nodes, you must configure the OnCommand Unified Manager server on the cluster node.

Configuring VCS to install the OnCommand Unified Manager Core Package

Before you install the OnCommand Unified Manager Core Package in VCS, you must install SnapDrive, a Fibre Channel adapter, and Veritas Storage Foundation. You must then configure VCS and use SnapDrive for UNIX to create file systems.

Before you begin

- All requirements and guidelines for configuring cluster servers must be met, according to the VCS documentation.
- SnapDrive for UNIX must be installed.

Steps

1. Install Veritas Storage Foundation and High Availability Solutions 5.0 with Maintenance Pack 1 (MP 1).

   When you install Veritas Storage Foundation and High Availability Solutions 5.0, VCS is also installed.

2. Configure VCS by entering the following command:

   ```
   installvcs -configure
   ```

3. Enter the network address (virtual IP address).

4. Use SnapDrive for UNIX to create file systems and logical volumes.

Related information

Veritas Cluster Server: www.symantec.com/business/cluster-server
Veritas Storage Foundation: www.symantec.com/en/in/business/storage-foundation
SnapDrive for UNIX: mysupport.netapp.com/documentation/productsatoz/index.html

Installing OnCommand Unified Manager Core Package on VCS

To ensure high availability, you must install OnCommand Unified Manager Core Package on the two cluster nodes of VCS.

Before you begin

- VCS must be installed and configured on both the nodes of the cluster.
- The same version of OnCommand Unified Manager Core Package must be installed on both the nodes.
- The installation directory is the same on both the nodes: for example, `/opt/NTAPdfm`.
- The first node must own the cluster resources.
- You must have root privileges to log in to the OnCommand Unified Manager server.
- The OnCommand Unified Manager Core Package installer must be downloaded from the NetApp Support Site
- You must have set the environment variable on both nodes as `VCS PATH: PATH=/opt/VRTSvcs/bin:$PATH`.

About this task

During a new installation, you must specify the OnCommand Unified Manager Core license key. If you are upgrading from an earlier licensed version of OnCommand Unified Manager server, you do not require a license key.

The two OnCommand Unified Manager server nodes are configured to use the same database and to monitor the same set of nodes. Therefore, you can use the same license on both the nodes.

The installation and upgrade process automatically installs the AutoSupport feature with AutoSupport enabled and displays a message about how to disable the feature.

Steps

1. Log in to the first node.

2. Run the executable file.

3. Follow the setup prompts to complete the installation.
4. Disable the automatic start-up of the OnCommand Unified Manager server by entering the following command:

   ```
   dfm service enable -m
   ```

   Attention: You must perform all cluster operations using Cluster Manager. Other than in installation and configuration procedures, you must not use the `dfm service start` and `dfm service stop` commands. These commands interfere with cluster operations.

5. When the installation is complete, enter the following command to stop the OnCommand Unified Manager server services:

   ```
   dfm service stop
   ```

6. Log in to the second node.
7. Start the cluster service on the second node by entering the following command:

   ```
   hastart
   ```

8. Perform a manual failover to the second node by entering the following command on the second node:

   ```
   hagrp -switch cluster_group -to node2
   ```

   ```
   hastop -sys node1 –force
   ```

9. Run the executable file on the second node.
10. Follow the setup prompts to complete the installation.
11. Retart the cluster service on the second by entering the following command:

    ```
    hastart
    ```

12. Disable the automatic start-up of the OnCommand Unified Manager server by entering the following command:

    ```
    dfm service enable -m
    ```

13. Stop all services on the second node by entering the following command:

    ```
    dfm service stop
    ```

Related information

NetApp Support Site: mysupport.netapp.com

Configuring OnCommand Unified Manager Core Package in a VCS environment

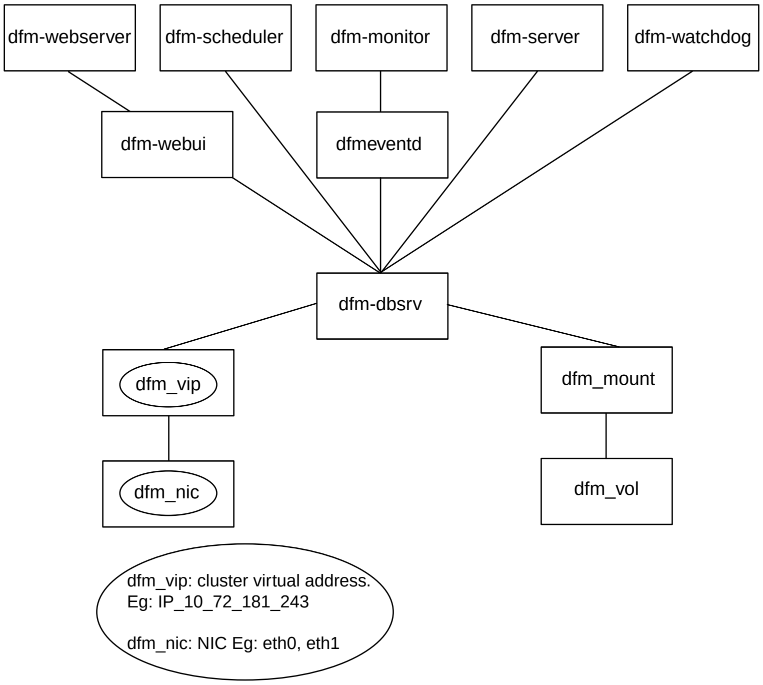
After installing OnCommand Unified Manager Core Package, you have to configure the OnCommand Unified Manager server in VCS.

OnCommand Unified Manager server service resources added to VCS

You must add the OnCommand Unified Manager server cluster service resources to VCS. There are dependencies among the various resources.

These services are used for various purposes, such as monitoring storage systems, scheduling jobs, processing events, and monitoring all the other services.

The following illustration shows the services and the dependencies among the various resources:



Script options for configuring services in VCS

You have to configure the OnCommand Unified Manager server to add its service resources to VCS. You can add the services manually, or by using the Perl configuration script.

The command to add services to the OnCommand Unified Manager server is as follows:

`perl dfmcluster_add_resources.pl -t` ***`cluster_type`*** **`option ...`**

The `perl dfmcluster_add_resources.pl` includes the following options:

`-t` ***`cluster_type`***

Cluster solution used for high availability. The possible values are **`vcs`** (default value on UNIX) and **`mscs`**.

`-h` ***`cluster_node1 cluster_node2`***

Nodes used for cluster setup, separated by a space.

`-g` ***`cluster_group_name`***

Name of the cluster service group to which the resources are added.

`-e` ***`nic_resource_name`***

Name of the network interface card. This must be the same on both cluster nodes.

`-i` ***`cluster_ip_resource_name`***

Name of the cluster IP resource.

`-n` ***`cluster_name_resource_name`***

Host name of the cluster, which is mapped to the cluster virtual IP address.

`-f` ***`mount_point_resource_name`***

Name of the mount resource.

`-v` ***`volume_resource_name`***

Name of the volume resource that contains the filesystem, represented by the mountpoint resource.

-d ***disk_group_resource_name***

Name of the disk group that contains the volume, represented by the volume resource.

-m ***netmask***

Netmask associated with the cluster IP address.

-l ***installation_directory***

OnCommand Unified Manager Core Package installation directory. The default location is `/opt/NTAPdfm`.

Configuring OnCommand Unified Manager server on the cluster nodes in VCS

You must configure the OnCommand Unified Manager server on two nodes in a cluster to allow failover. You have to configure the OnCommand Unified Manager server on the first node and then on the second node.

Steps

1. Stop the cluster service of the second node by entering the following command on the first node:

   ```
   hastop -sys node2 -force
   ```

2. Move all the shared data, such as database files and performance data files, from the first node by entering the following command:

   ```
   dfm datastore setup /mnt/vcsDisk1
   ```

   `/mnt/vcsDisk1` is the mount point.

3. Stop all services on the first node by entering the following command:

   ```
   dfm service stop
   ```

4. Add the cluster services as cluster resource by entering the following command on the first node:

   ```
   perl dfmcluster_add_resources.pl -t vcs -h node1 node2 -g cluster_group
   -i cluster_ip_resource_name -n cluster_name_resource_name -d
   disk_group_resource_name -v volume_resource_name -f
   mount_point_resource_name -e nic_resource_name -m netmask
   ```

5. Verify the status of the cluster resources on the first node by entering the following commands:

   ```
   hasys –list
   ```

   ```
   hastatus –summ
   ```

   ```
   hagrp –state
   ```

   ```
   hares –state
   ```

   ```
   haclus –state
   ```

6. Start the cluster service on the second node by entering the following command:

   ```
   hastart
   ```

7. Perform a manual failover to the second node by entering the following command on the second node:

   ```
   hagrp -switch cluster_group -to node2
   ```

   ```
   hastop -sys node1 –force
   ```

   Note: You can run the `snapdrive storage list -fs /mnt/vcsDisk1` command on the second node to verify the status of the mount point.

8. Configure the second node to use the shared data by entering the following command:

   `dfm datastore setup -n /mnt/vcsDisk1`

   Using the `-n` option while configuring the second node ensures that the OnCommand Unified Manager server uses the data that was copied during the configuration of the first node.

9. Stop all services on the first node by entering the following command:

   `dfm service stop`

10. Start the cluster services on the first node by entering the following command:

    `hastart`

11. Verify the status of the cluster resources on both nodes by entering the following commands on the two nodes:

    `hasys –list`

    `hastatus –summ`

    `hagrp –state`

    `hares –state`

    `haclus –state`

12. Start the services on the second node by entering the following command on the second node:

    `hagrp -online cluster_group -sys node2`

Configuring OnCommand Unified Manager server in VCS manually

You can manually configure the OnCommand Unified Manager server by using the VCS Application Configuration wizard. Configuring the OnCommand Unified Manager server in VCS manually enables you to customize the cluster.

Before you begin

You must have ensured that the OnCommand Unified Manager server is installed at `/opt/NTAPdfm`.

Steps

1. Run the **VCS Application Configuration** wizard by entering the following command on the node where VCS is set up:

   `hawizard`

2. Select **Create Application Service Group** and click **Next**.
3. Enter a name in **Service Group Name** and select the cluster from the **Available Cluster** list.
4. Click **Next**.
5. Enter the application details:

   a. Specify `/usr/bin/dfm` as the path in **Start Program**.

   b. Select **root** as user.

6. Click **Next**.
7. Select the processes that must be monitored by the OnCommand Unified Manager server by entering the appropriate process monitor string.

   The following table lists the processes and their process monitor string:

Process	Process monitor string
+ dfmmonitor	/opt/NTAPdfm/sbin/dfmmonitor
+ dfmserver	/opt/NTAPdfm/sbin/dfmserver
+ dfmscheduler	/opt/NTAPdfm/sbin/dfmscheduler
+ dfmeventd	/opt/NTAPdfm/sbin/dfmeventd start
+ database server	/opt/NTAPdfm/sbin/dbsrv11 @/opt/NTAPdfm/conf/sybase.conf
+ Apache server	/opt/NTAPdfm/sbin/httpd -f /opt/NTAPdfm/conf/httpd.comf
+Webui	/opt/NTAPdfm/java/bin/java /opt/NTAPdfm/jetty/start.jar /opt/NTAPdfm/conf/jetty.conf

8. Verify the process monitor string for each process by using the `ps -u root -o args` command.
9. Click **Next**.
10. Configure the mount resources and click **Next**.
11. Configure the IP and NIC resources and click **Next**.
12. Repeat Steps 5 through 11 for each OnCommand Unified Manager server process.
13. Open **Cluster Manager** to configure the remaining cluster resources.
14. Select the service group **dfm_sg** in the left pane.
15. In the **Resource** tab, right-click **Resource View**.
16. Enter the details for each **Resource Type**.

    On Linux, you should select only **LVMLogicalVolume** and **Mount** as the resource types. The FSType attribute should be set to **`ext3`** for **Mount**.
17. Select **NIC** from the **Resource Type** list.
18. Right-click the added resources and select **Link**.
19. Create a dependency tree and bring all the services online.
20. Ensure the OnCommand Unified Manager server uses the cluster name (instead of the local system name) by entering the following command:

    ```
    dfm option set localHostName=fqdn-of-cluster
    ```

    The OnCommand Unified Manager server uses the name of the local system to send email alerts to administrators.

Configuring a host services in VCS

When you add a new host service in VCS, you must ensure that both nodes in a cluster pair have access to the keys folder. This ensures that when one node fails, the second node of the cluster starts functioning.

Steps

1. Copy the keys folder from one node to the other in the cluster pair at `installation_directory\conf`.
2. Open the **Cluster Manager** by entering the following command at the command prompt:

   ```
   hagui
   ```
3. In the **Cluster Manager**, right-click the **service group**, click **Switch To**, and select the second cluster node for failover
4. Enter the following command on the second node to start using the new setting:

   ```
   dfm ssl service reload
   ```
5. Launch the OnCommand console, verify that the host service status is Up in the **Host Services** tab.

Best practices to start and stop OnCommand Unified Manager server services in VCS

After you set up OnCommand Unified Manager server in VCS, do not use the `dfm service start` and `dfm service stop` commands, except where specifically indicated in installation and configuration procedures. You must perform all operations by using the Cluster Manager.

- You should disable the OnCommand Unified Manager server init scripts after installation on both the cluster nodes.
- You should not change the service start-up type to Automatic in Service Control Manager on any of the nodes.

  The OnCommand Unified Manager server reactivates these scripts during an upgrade and then disables them again when the upgrade is complete.

Managing the OnCommand Unified Manager server in a VCS environment

You can create and restore backups, set HTTPS options, and configure OnCommand Unified Manager server to share data on the OnCommand Unified Manager server cluster nodes.

Restoring the OnCommand Unified Manager server database in VCS

Restoring a database enables the OnCommand Unified Manager server to use the current settings. You can restore the OnCommand Unified Manager server database by disabling it through Cluster Manager and using the `dfm backup restore` command.

Steps

1. In **Cluster Manager**, disable the OnCommand Unified Manager server services by right-clicking the name of the service group and then clicking **Offline**.
2. Select the first cluster node in which the services are online. NetApp Management Console

3. Ensure that one of the nodes owns the cluster resources (such as the mount point) by completing the following steps:

    a. Select the service group **dfm_sg**.

    b. In the **Resources** tab, right-click **Resource View**.

    c. Right-click the resource **Mount**, and then click **Online**

4. Restore the database by entering the command in the node that owns the Mount resource:

    ```
    dfm backup restore
    ```

5. In **Cluster Manager**, right-click the service group, click **Online**, and then select the first cluster node that is used for restore.

Changing default port numbers for HTTP and HTTPS protocols

You can change the default port numbers for HTTP and HTTPS protocols.

Before you begin

The DFM Apache service must have been offline before the port numbers are changed in both the nodes.

Steps

1. Log in to the first node.

2. In **Cluster Administrator**, take the OnCommand Unified Manager server services offline:

    a. Right-click the **DFM Sybase** service.

    b. Select **Take offline**.

    All services go offline.

3. Start the SQL service by running the following command:

    ```
    dfm service start sql
    ```

4. Set the new HTTP or HTTPS port numbers by running the following command:

    ```
    dfm option set option_name=value
    ```

    #### Example

    Set the new HTTP port:

    ```
    dfm option set httpPort=8081
    ```

    Set the new HTTPS port

    ```
    dfm option set httpsPort=8089
    ```

5. Restart the HTTP or HTTPS service by running the following commands:

    - The following commands restarts the HTTPS service:

        ```
        dfm service stop webui
        dfm service start webui
        ```

    - The following commands restarts the HTTP service:

        ```
        dfm service stop http
        dfm service start http
        ```

6. Optional: Verify the changed port numbers by viewing the `httpd.conf` file.
7. Stop the HTTP and HTTPS services by running the following commands:

   ```
   dfm service stop http
   ```

   ```
   dfm service stop webui
   ```
8. In **Cluster Administrator**, move the cluster group to the second node by using the **Move Group** option.
9. Log in to the second node.
10. Start the HTTP and HTTPS services on the second node by entering the following commands:

    ```
    dfm service start http
    ```

    ```
    dfm service start webui
    ```
11. Optional: Verify the changed port numbers by viewing the `httpd.conf` file.
12. In **Cluster Administrator**, bring the OnCommand Unified Manager server services online:
    a. Select **Cluster Group** under the **Groups** folder.
    b. Click **File**, and click **Bring Online**.

Configuring the OnCommand Unified Manager server to use HTTPS in VCS

You can configure the OnCommand Unified Manager server to use HTTPS on both the cluster nodes for a secured data transfer.

About this task

You must not take the dfm-dbsrv service offline.

Steps

1. In **Cluster Manager**, take the OnCommand Unified Manager server services offline:
   a. Right-click the service group **dfm-sg**, and click **Offline**.
   b. Select the first cluster node where the services are online.
   c. In the **Resources** tab, right-click **Resource View**.
   d. Right-click the resource **dfm-dbsrv** and click **Online**.
2. Create an SSL certificate by entering the following command:

   ```
   dfm ssl server setup
   ```
3. Copy the files `server.crt` and `server.key` to the second node before starting the services on that node.

   The files are located in the `installation_directory/conf` folder.
4. Enable HTTPS by setting the following OnCommand Unified Manager server option to yes:

   ```
   dfm option set httpsEnabled=yes
   ```
5. Start the HTTP service by entering the following command:

   ```
   dfm service start http
   ```

   This re-creates the `httpd.conf` file with the changed options.
6. Stop all the services by entering the following command:

```
dfm service stop
```

> **Note:** You must ensure that OnCommand Unified Manager server services are offline. Otherwise, the HTTP service fails to be enabled on the other node, because the configuration is not complete.

7. In **Cluster Manager**, move the cluster group to the second node by using the option **Switch To**.
8. Log in to the second node in the cluster.
9. Copy the files `server.crt` and `server.key` created on the first node to the folder *`install-dir`*`/conf`.
10. Start the services and verify that they are operating by entering the following command:

    ```
    dfm service start
    ```

    This creates the `httpd.conf` file with the changed options.
11. Stop the services by entering the following command:

    ```
    dfm service stop
    ```
12. In **Cluster Manager**, reenable the OnCommand Unified Manager server services.

Changing the HTTP options in a VCS environment

You can change the HTTP options to enable HTTPS, or change the default HTTP and HTTPS port.

About this task

You must not take the dfm-dbsrv service offline.

Steps

1. In **Cluster Manager**, take the OnCommand Unified Manager server services offline:
    a. Right-click the service group, and click **Offline**.
    b. Select the first cluster node where the services are online.
    c. In the **Resources** tab, right-click **Resource View**.
    d. Right-click the resource **dfm-dbsrv** and click **Online**.
2. Set the required HTTP option by entering the following command:

    ```
    dfm option set option-name=option-value
    ```

    Example

    ```
    dfm option set httpsPort=443
    ```
3. Restart the HTTP service by entering the following command:

    ```
    dfm service start http
    ```

    > **Attention:** You must perform all cluster operations using Cluster Manager. Apart from installation and configuration procedures, you should not use the commands `dfm service start` and `dfm service stop`. These commands interfere with cluster operations.
4. Stop all the services by entering the following command:

    ```
    dfm service stop
    ```

    This re-creates the file `httpd.conf` with the changed options.

Note: You must ensure that OnCommand Unified Manager server services are offline. Otherwise, the HTTP service fails to come up on the other node because the configuration is not complete.

5. In **Cluster Manager**, move the cluster group to the second node by using the option **Switch To**.
6. Log in to the second node in the cluster.
7. Start the services by entering the following command:

   ```
   dfm service start
   ```
8. Stop the services by entering the following command:

   ```
   dfm service stop
   ```
9. In **Cluster Manager**, bring the OnCommand Unified Manager server services online.

Data shared by VCS cluster nodes

You must configure OnCommand Unified Manager server nodes to access files from a shared disk. If each node uses its own local copy of files, any updates to files might not be accessible to the other nodes, after a failover.

The VCS cluster nodes share the following files:

***installation_directory*/data**

Sybase database files

***installation_directory*/perfdata**

Performance Advisor data files

***installation_directory*/scriptplugins**

Installed script plug-ins and related files

***installation_directory*/plugins**

Storage system configuration plug-ins

***installation_directory*/reports**

Archived reports

***installation_directory*/dataExport**

OnCommand Unified Manager server and Performance Advisor data

***installation_directory*/jetty**

Libraries and Web application files

Data that is not shared by VCS cluster nodes

To ensure that the same version is maintained in both the cluster nodes, executable and configuration files, license information, and so on are not shared by the OnCommand Unified Manager server cluster nodes.

The VCS cluster nodes do not share the following files:

***installation_directory*/bin**

Executable files

***installation_directory*/conf**

Configuration files

***installation_directory*/docs**

Third-party licenses

***installation_directory*/examples**
Cluster configuration scripts, and other script files

***installation_directory*/log**
Log files

***installation_directory*/misc**
Configuration files

***installation_directory*/sbin**
Third-party executables

***installation_directory*/scripts**
Location of the `Sybase_install.sql` file

***installation_directory*/src**
Storage system configuration plug-ins

***installation_directory*/web/clients**
Performance Advisor clients

***installation_directory*/web/com**
JAR files for applets

***installation_directory*/web/help**
Help files

***installation_directory*/web/man**
Manual (man) pages

***installation_directory*/web/media**
Images used on Web interfaces

***installation_directory*/web/scripts**
Java script files

***installation_directory*/web/styles**
CSS style sheets

Uninstalling the OnCommand Unified Manager Core Package in a VCS environment

You can uninstall the OnCommand Unified Manager Core Package from a cluster by deleting all the OnCommand Unified Manager server services from the cluster nodes.

Steps

1. In **Cluster Manager**, delete all the OnCommand Unified Manager server services:
   a. Right-click the service group **dfm-sg**.
   b. Select **Delete**.
2. Log in to one of the cluster nodes.
3. Uninstall by entering the one of the following commands:
   - **`rpm -e NTAPdfm`**
   - **`rpm --erase NTAPdfm`**

4. Repeat Steps 2 through 3 for the other cluster nodes.

Upgrading OnCommand Unified Manager Core Package in a VCS environment

When you upgrade the OnCommand Unified Manager Core Package cluster nodes, you must ensure that all the nodes in the cluster are upgraded.

Before you begin

- The OnCommand Unified Manager server installer from the NetApp Support Site must be downloaded.
- A backup of your existing OnCommand Unified Manager server database must be created.
- The database must be present at the following path: `INSTALL_DIR/DFM/data`.
  The database files `monitordb.db` and `monitordb.log` must be available on the shared disk.

Steps

1. From **Cluster Administrator**, take the OnCommand Unified Manager server services offline by running the following commands on the first node:

   ```
   hagrp -offline cluster_group -sys node1
   ```

   ```
   hastatus –summ
   ```

2. Bring the cluster resources online on the first node by running the command:

   ```
   hares -online data_mount -sys node1
   ```

3. Verify that the first node owns the cluster resources by running the command:

   ```
   hastatus –summ
   ```

4. Optional: Update the monitoring process to point to the new database by running the following command:

   ```
   hares -modify dfm-dbserver MonitorProcesses "install_dir/sbin/dbsrv11
   @install_dir/conf/sybase.conf"
   ```

   Important: You must perform this step if you are upgrading to OnCommand Unified Manager Core Package 5.1 or later from any version from OnCommand Unified Manager server 3.8 through OnCommand Unified Manager Core Package 5.0.

5. Upgrade to OnCommand Unified Manager Core Package on the first node:

   a. Run the executable file.

   b. Follow the setup prompts to complete the installation.

6. Stop all the OnCommand Unified Manager server services by entering the following command:

   ```
   dfm service stop
   ```

   Attention: You should perform all cluster operations by using either Cluster Administrator or `cluster.exe`. Except where specifically indicated in installation and configuration procedures, you must not use the `dfm service start` and `dfm service stop` commands. These commands interfere with cluster operations.

7. Disable the automatic service start-up during reboot by entering the following command:

   ```
   dfm service enable -m
   ```

8. Perform a manual failover to the second node by entering the following commands on the second node:

   ```
   hagrp -switch cluster_group -to node2
   ```

   ```
   hastop -sys node1 –force
   ```

9. From **Cluster Administrator**, take the OnCommand Unified Manager server services offline by running the following commands on the second node:

   ```
   hagrp -offline cluster_group -sys node2
   ```

   ```
   hastatus –summm
   ```

10. Bring the cluster resources online on the second node by running the command:

    ```
    hares -online data_mount -sys node2
    ```

11. Optional: Point the Sybase database to the old database by running the following command:

    `dfm datastore setup -n -d` ***`old_monitordb_location`***

    Important: You must perform this step if you are upgrading to OnCommand Unified Manager Core Package 5.1 or later from any version from OnCommand Unified Manager server 3.8 through OnCommand Unified Manager Core Package 5.0.

12. Upgrade to the OnCommand Unified Manager Core Package installation on the second node:

    a. Run the executable file.

    b. Follow the setup prompts to complete the installation.

13. Set Sybase to the shared database location by running the following command:

    `dfm datastore setup -n -d` ***`shared_monitordb_location`***

14. Stop all the OnCommand Unified Manager server services by entering the following command:

    ```
    dfm service stop
    ```

15. Disable the automatic service start-up during reboot by entering the following command:

    ```
    dfm service enable -m
    ```

16. From **Cluster Administrator**, bring the OnCommand Unified Manager server services online by running the following command on the second node:

    ```
    hagrp -online cluster_group -sys node2
    ```

Related tasks

Configuring OnCommand Unified Manager server on the cluster nodes in VCS on page 83

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