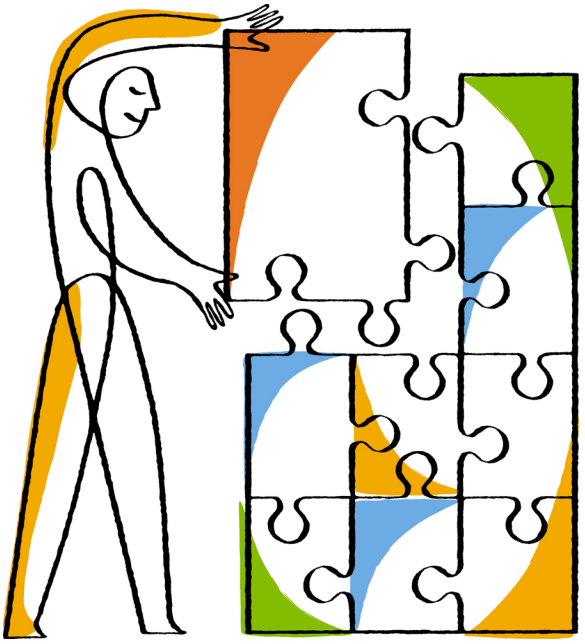
# OnCommand® Performance Manager 1.0

## Installation and Administration Guide



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

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

Part number: 215-08188_A0
February 2014

# Contents

# Introduction to OnCommand Performance Manager

OnCommand Performance Manager provides performance monitoring and incident root-cause analysis of a system running clustered Data ONTAP. It is the performance management part of OnCommand Unified Manager.

Performance Manager helps you identify workloads that are over-using cluster components and decreasing the performance of other workloads on the cluster. It alerts you to these performance issues, called incidents, so that you can take corrective action and return performance back to normal operation. You can view and analyze incidents in the Performance Manager GUI or view them in the Unified Manager Dashboard.

Performance Manager is an analytics-based IT management software solution that helps you monitor the performance of FlexVol volumes, also called user-defined workloads, and internal workload activity, called system-defined workloads, on a system running clustered Data ONTAP. All monitored volumes must be in a QoS policy group. Infinite Volumes are not supported. Performance Manager collects and analyzes workload activity to learn the expected range, or what it perceives to be normal activity for your environment. It uses the expected range and a dynamic performance threshold to monitor the I/O response time of each volume on a cluster. A high, or slow, response time indicates which volumes are performing slower than normal. Slow response time also indicates when the performance of client applications that are using a volume has decreased. Performance Manager identifies the specific cluster component that is in contention, which is the location in the cluster with the highest pain point where the performance issue lies. Performance Manager also provides a list of suggested actions you can take to try and address any performance issues on your own.

## OnCommand Performance Manager features

OnCommand Performance Manager collects and analyzes performance statistics from a system running clustered Data ONTAP. It uses a dynamic performance threshold to monitor the I/O response time of each volume on a cluster. A high, or slow, response time indicates which volumes are performing slower than normal. Performance Manager provides suggestions for addressing performance issues, called incidents, on your own.

OnCommand Performance Manager includes the following features:

- Operates as a virtual machine (VM) that runs on a VMware ESX or ESXi Server.
- Monitors and analyzes workload performance statistics from a system running clustered Data ONTAP.
- Uses a dynamic performance threshold that learns about your workload activity to identify and alert you to performance issues.
- Clearly identifies the cluster component that is in contention.

- Displays detailed graphs that plot workload activity over time, including I/O response time, the operations of user- and system-defined workloads, and cluster component usage.
- Identifies workloads that are over-using cluster components and the workloads whose performance is impacted by the increased activity.

# OnCommand Performance Manager product documentation

OnCommand Performance Manager is accompanied by a set of guides.

| | |
|---|---|
| ***OnCommand Performance Manager Installation and Administration Guide*** | Provides instructions for setting up Performance Manager in your datacenter, including deploying and configuring the virtual appliance and accessing the web-based interface. |
| ***OnCommand Performance Manager User Guide*** | Provides an overview of Performance Manager, including reference information that explains the web-based interface, and instructions for monitoring, analyzing, and troubleshooting performance issues for workloads on a system running clustered Data ONTAP. |

# Planning your installation

Performance Manager is distributed as a self-contained, fully-formed virtual appliance (VA) available in an Open Virtualization Appliance (OVA) file. You use a VMware vSphere Client to deploy the OVA file to a VMware ESX or ESXi Server that meets the minimum requirements. Once deployed the VA converts to a virtual machine (VM).

You need to identify the username and password for the person who will configure the administrative account after installation. You also need to select a supported browser to run the installed software.

The initial configuration process requires you to identify the geographic area and time zone for the VM. Then you create the maintenance user's login name and password. At the end of the initial configuration, if you are using DHCP, you receive the IP address of the newly created VM.

To open the Performance Manager GUI, you copy that IP address into a supported browser and log in with the maintenance user account. See the browser requirements for the list of supported browsers.

#### Related concepts

*Virtual infrastructure requirements* on page 10
*Virtual appliance requirements* on page 11

#### Related tasks

*Downloading the installation file* on page 13
*Deploying Performance Manager* on page 13

#### Related references

*Browser requirements* on page 12

## System requirements

Before you deploy the Performance Manager virtual appliance, you must ensure that your storage system conforms to all supported platform requirements. Servers must meet specific software, hardware, CPU, and memory requirements.

For the most current information, see the Interoperability Matrix.

#### Related information

*Interoperability Matrix: support.netapp.com/matrix*

# License requirements for Performance Manager

You must have appropriate licenses to use VMware vSphere for Enterprise. No additional licenses are required for the Performance Manager server.

# Supported cluster configurations

A single instance of Performance Manager supports a specific number of clusters and volumes. If Performance Manager is monitoring an environment that exceeds the supported configuration, there might be problems with collecting and analyzing configuration and performance data from the cluster. You can install multiple instances of Performance Manager to monitor larger configurations.

The following table lists the supported number of clusters and volumes that Performance Manager can reliably support.

| **Storage objects** | **Maximum supported** |
|---|---|
| Clusters | 6 |
| Nodes | • For a single cluster: 6<br>• For 2 clusters: 4<br>• For 3 or more clusters: 2 |
| Volumes per node | • For a single cluster with 6 nodes: 200<br>• For up to 2 clusters and up to 4 nodes per cluster: 500<br>• For 3 to 6 clusters with no more than 2 nodes per cluster: 200 |

# Virtual infrastructure requirements

Your virtual infrastructure must meet minimum requirements before you can begin deployment.

Memory page swapping negatively impacts performance of the virtual appliance and the management application. Competing for CPU resources that are unavailable due to overall host utilization can degrade performance. Reserving the listed values for memory and CPU resources for the virtual appliance guarantees that the required minimum amount is always available to the virtual machine, and is required for running this virtual appliance.

The following table displays the minimum values required for memory and CPU resources in the default configuration. These values have been qualified for the virtual appliance to meet minimum acceptable performance levels.

| Default hardware configuration | Minimum Requirement |
|---|---|
| Disk space needed for thin provisioning | 5 GB |
| Disk space needed for thick provisioning<br>**Note:** If deploying an NFS datastore on a storage system running clustered Data ONTAP, without the NetApp NFS Plug-in for VMware VAAI, you cannot use the thick provisioning option. | 300 GB |
| Memory needed for the Performance Manager virtual appliance | 12 GB and Reservation 12 GB |
| Processors needed for the Performance Manager virtual appliance | 4 virtual CPUs |
| Process cycles (CPU speed) needed for the Performance Manager virtual appliance | 9572 MHz and Reservation 9572 MHz |

VMware High Availability for the Performance Manager virtual appliance is not supported. The virtual appliance can be deployed on a VMware server that is a member of a VMware High Availability environment, but utilizing the VMware High Availability functionality is not supported.

#### Related concepts

*Virtual appliance requirements* on page 11

#### Related tasks

*Deploying Performance Manager* on page 13

## Virtual appliance requirements

The virtual appliance is deployed on a VMware ESX server, which must meet minimum resource requirements.

The following versions of VMware ESXi are supported:

- ESXi 4.0
- ESXi 5.0
- ESXi 5.0 (update 1)
- ESXi 5.0 (update 2)
- ESXi 5.1
- ESX 5.1 (update 1)
- ESX 5.5

The following versions of vSphere are supported:

- VMware vCenter Server 4.0
- VMware vCenter Server 4.1
- VMware vCenter Server 5.0
- VMware vCenter Server 5.1

The VMware ESX server must use the same time as the NTP server so that the virtual appliance functions correctly. Synchronizing the VMware ESX server time with the NTP server time avoids a time failure.

### Related concepts

*Virtual infrastructure requirements* on page 10

### Related tasks

*Deploying Performance Manager* on page 13

## Browser requirements

You must use a supported browser to display the web-based GUI.

You need one of the following browsers:

- Mozilla Firefox versions 24 and 25.
- Microsoft Internet Explorer (IE) 9 or 10.
- Google Chrome versions 30 and 31.

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

For all browsers, disabling any popup blockers allows software features to display properly.

### Related concepts

*Getting started* on page 17

# Installing Performance Manager

The installation process contains three steps: downloading the virtual appliance (VA) installation file, deploying the VA, and performing the initial configuration.

You download the VA as an OVA installation file from the NetApp Support Site. You need a customer account to access the site.

You also need to be familiar with the operations of the VMware vSphere Client in order to deploy the OVA installation file that creates the virtual machine (VM). After the initial configuration using the vSphere Client, you can copy the IP address for your new VM into a supported browser and then start using the software to monitor your NetApp storage systems.

## Downloading the installation file

To set up the software installation, you need to download the virtual appliance (VA) installation file and then use a VMware vSphere Client to deploy the file to a VMware ESX or ESXi Server. The VA is available in an OVA file.

#### Steps

1. Download the OVA installation file from the NetApp Support Site.

   You need to log into the Support website to access this file.
2. Save the OVA file to a local or network location that is accessible to your vSphere Client.
3. Verify the checksum on the Download page to ensure you have the correct installation file.

### What a virtual appliance does

A virtual appliance is a prebuilt software bundle containing an operating system and software applications that are integrated, managed, and updated as a package. Virtual appliances simplify the installation process.

Upon deployment, the virtual appliance creates a virtual machine containing Performance Manager, third-party applications, and all configuration information pre-installed on the virtual machine.

## Deploying Performance Manager

You use a VMware vSphere Client to deploy the virtual appliance (VA) to an ESX or ESXi Server. Once deployed, the VA converts to a virtual machine (VM).

#### Before you begin

- You have downloaded the OVA installation file from the NetApp Support Site.

- The ESX or ESXi Server meets the requirements to host the VM.

### About this task

**Note:**

### Steps

1. In the vSphere Client, select **File > Deploy OVF Template**.
2. Browse to the downloaded OVA file.
3. Use the Deploy OVF Template wizard to deploy the VA.

   **Note:** For the VM disk format, "Thin Provisioned" is the default for back-end storage that supports thin provisioning. Thin provisioning allows the software database to grow efficiently to the maximum available capacity as you add storage objects to your data center. If you destroy a Performance Manager virtual machine (VM) and then install a new instance using the same IP address assigned to the previous VM, adding the clusters from the previous VM to the new VM will display an error message that the clusters are already monitored. You can ignore this error message.

4. After the VA has successfully deployed to the ESX or ESXi Server, power on the VM. You can click the **Console** tab to watch the VM power-up.

### After you finish

With the VA powered on in the vSphere Client, you need to use the maintenance console to complete the initial settings configuration.

### Related concepts

*Planning your installation* on page 9
*Virtual infrastructure requirements* on page 10
*Virtual appliance requirements* on page 11
*Using the maintenance console* on page 66

### Related tasks

*Downloading the installation file* on page 13
*Configuring initial settings for Performance Manager* on page 15

# Configuring initial settings for Performance Manager

After deploying the virtual appliance (VA), you use the maintenance console to perform the initial configuration. At the end of the initial configuration, you set up the user login for the virtual machine (VM) and receive the IP address assigned to the VM.

### Before you begin

- You have downloaded the OVA installation file and deployed it to an ESX or ESXi Server.
- You have powered-on the VM.

### Steps

1. In the vSphere Client, select the VM for Performance Manager.
2. Click the **Console** tab.
3. The configuration program displays a command prompt for you to enter the following configuration settings:
   - Geographic area
   - Time zone

     **Note:** Following time zone selection, the program uses DHCP to search for the IP address. If the IP address cannot be found, you are asked, "Do you want to set up a static configuration?" The following information is required for a static configuration:
   - Fully-qualified domain name (FQDN) of the VM
   - IP address and netmask of the VM
   - IP address of the DNS server for the VM
   - IP address of the gateway for the VM
   - Maintenance user's username and password (if the IP address was found)
   - OnCommand login (if the IP address was found)

### Result

After the deploying the OVA, the first time you start the VM it receives a unique ID, called the System ID. The System ID identifies your installation of Performance Manager. The System ID and IP address assigned to the VM are displayed. You use this IP address and the maintenance user login information to access the software in a supported web browser.

### After you finish

If you have installed OnCommand Unified Manager, you can use the maintenance console to connect it to Performance Manager. Incidents from Performance Manager will be displayed in OnCommand Unified Manager.

### Related concepts

*Using the maintenance console* on page 66
*What the maintenance user does* on page 37

### Related tasks

*Configuring a connection between a Performance Manager server and the Unified Manager server* on page 75

### Related references

*Browser requirements* on page 12

# Getting started

After deploying and configuring the virtual appliance, the first time you log in to the Performance Manager GUI, a setup wizard is displayed. You must complete the wizard before you can start using Performance Manager.

Until you complete the steps associated with the setup wizard, other areas of the Performance Manager GUI are unavailable.

The setup wizard displays the following options:

| | |
|---|---|
| **Set Up Email and Time Zone** | Options for configuring email settings to specify where email alerts will be sent. You can specify an initial email recipient, an SMTP server to handle email communication, and a Network Time Protocol (NTP) server to synchronize Performance Manager server time with the time of the NTP server. After configuring the settings, you can click **Test** to confirm whether recipients can receive email alerts. |
| **Set Up AutoSupport** | Options for enabling AutoSupport to have information about your installation of Performance Manager sent to technical support. Support personnel can use this information to stay current with the configuration and operation of your installation of Performance Manager, which can be useful when helping you to troubleshoot or manage the product. |
| **Change Admin Credentials** | Options for changing the password for the administrative account. This is the password you assigned to the maintenance user account when you installed and configured the virtual appliance. You cannot change the Administrator account name. |
| **Connect to ONTAP Cluster** | Options for adding one or more clusters you want to monitor. You can enter the fully-qualified name (FQDN) or IP address and access credentials for each system running clustered Data ONTAP. Each cluster must meet minimum configuration requirements.<br><br>**Note:** The first time you add a cluster it can take up to 15 minutes for Performance Manager to fully discover the cluster. Until the discovery process has completed, you will not be able to search for objects, such as volumes, on the cluster. |

### Related concepts

*What AutoSupport does* on page 21
*Supported cluster configurations* on page 10
*How the discovery process works* on page 30

### Related tasks

*Adding clusters* on page 28
*Configuring initial settings for Performance Manager* on page 15

### Related references

*Browser requirements* on page 12

# Configuring your environment after deployment

After you deploy the Performance Manager virtual appliance and complete the setup wizard, there are several configuration tasks that you might want to perform before you start monitoring your clusters, such as changing the host name, configuring alerts, and adding users.

### Before you begin

- You must have deployed the virtual appliance and completed the initial setup of Performance Manager.
- You must be logged in as the OnCommand Administrator to complete all tasks in this workflow.

### Choices

- *Changing the Performance Manager host name* on page 19

  When you deployed Performance Manager, an SSL certificate was generated for HTTPS access. A host name was associated with the certificate, allowing you to use the host name to access the Performance Manager GUI. You might want to change this host name after deployment.
- *Configuring Performance Manager to send alert notifications* on page 20

  After the clusters have been added to Performance Manager, you can monitor them, but you cannot receive notifications about events in your cluster environment until you configure several options, such as the email address from which notifications are sent, the users to receive the alerts, and so on. You might also want to modify the default threshold settings at which events are generated.
- *Adding users* on page 40

  You must manually add users to Performance Manager to create user accounts and control user access.

## Changing the Performance Manager host name

When the Performance Manager virtual appliance is first deployed, the network host is assigned a name. You can change the host name after deployment. If you change the host name, you should also regenerate the HTTPS certificate.

### Before you begin

You must be signed in to Performance Manager as the maintenance user or have the OnCommand Administrator or Storage Administrator role assigned to you to perform these tasks.

### About this task

You can use the host name (or the host IP address) to access the Performance Manager GUI. If you configured a static IP address for your network during deployment, then you would have designated a name for the network host. If you configured the network using DHCP, the host name should be taken from the DNS. If DHCP or DNS are not properly configured, the host name “OnCommand” is automatically assigned and associated with the security certificate.

Regardless of how the host name was assigned, if you change the host name and intend to use the new host name to access the Performance Manager GUI, you must generate a new security certificate.

If you access the Performance Manager GUI by using the server's IP address instead of the host name, you do not have to generate a new certificate if you change the host name. However, it is the best practice that you do update the certificate, so that the host name in the certificate matches the actual host name.

The new certificate does not take effect until the Performance Manager virtual machine is restarted.

### Steps

1. *Edit the host name in Network Settings* on page 23

   You can change the host name from the Configure Network Settings dialog box, accessed from the Administration menu.

2. *Generate an HTTPS security certificate* on page 58

   If you want to use the new host name to access the Performance Manager GUI, you must regenerate the HTTPS certificate to associate it with the new host name.

3. *View the HTTPS security certificate* on page 57

   You should verify that the correct information is displayed after generating a new security certificate, then restart Performance Manager virtual machine.

4. *Restart the Performance Manager virtual machine* on page 57

   If you regenerate the HTTPS certificate, then you must restart the virtual machine.

## Configuring Performance Manager to send alert notifications

You can configure Performance Manager to send notifications that alert you about events in your environment. Before notifications can be sent, you must first configure several other Performance Manager options.

### Before you begin

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### About this task

After deploying the virtual appliance and completing the initial configuration of Performance Manager, you should consider configuring your environment to trigger alerts and generate notification email or SNMP traps.

You can complete the following tasks to properly configure your environment to send alert notifications.

### Steps

1. *Configure email settings* on page 62

   If you want alert notifications sent when certain events occur in your environment, you must supply an email address from which the alert notification can be sent. If your configuration uses an SMTP server for email authentication, then you must provide the user name and password for the server.

2. *Enable remote authentication* on page 48

   If you want remote LDAP or Active Directory users to access the Performance Manager GUI and receive alert notifications, then you must enable remote authentication.

3. *Add authentication servers* on page 50

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

4. *Add users* on page 40

   You can add several different types of local or remote users and assign specific roles. When you create an alert, you assign a user to receive the alert notifications.

5. *Configure email alerts* on page 63

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

# Customizing your environment

After you deploy the Performance Manager virtual appliance and access the GUI, you can customize the configuration of several options to meet the needs of your cluster environment.

## Enabling periodic AutoSupport

You can choose to have specific, predefined messages sent automatically to technical support to ensure correct operation of your environment and to assist you in maintaining the integrity of your environment.

#### Before you begin

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

#### Steps

1. Click **Administration > Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server > AutoSupport**.
3. To read about what periodic AutoSupport entails, click **View AutoSupport Description**.

   The dialog box also displays the product System ID, which is the number that technical support uses to find your AutoSupport messages.
4. Select the **Enable Periodic AutoSupport** check box, and then click **Save and Close**.

### What AutoSupport does

With the help of the AutoSupport feature, Performance Manager sends information to technical support personnel to help with troubleshooting. AutoSupport (ASUP) messages are scanned for potential problems and are available to technical support personnel when they assist you in resolving issues.

When you generate the ASUP message from OnCommand Performance Manager, the following configuration and analytical data is included in the ASUP message:

- Number of incidents that have a state of new or obsolete over the last seven days.
- Top three cluster components with the highest number of incidents over the last seven days.
- Configuration changes caused by HA takeover, policy group limit modifications, or volume moves.
- Minimum, maximum, and average times for configuration and analytical data to be collected.
- Minimum, maximum, and average times for incident analysis to complete.
- Details about the virtual machine (VM), database, disk storage usage, and the number of errors and exceptions specific to Performance Manager.

ASUP or support messages that you generate through the maintenance console will not include the configuration and analytical data from Performance Manager.

## Sending an on-demand AutoSupport message

You can choose to have Performance Manager send an on-demand message to technical support for assistance with troubleshooting issues. The AutoSupport message sent by Performance Manager contains diagnostic system information and detailed data about the Performance Manager server.

### Before you begin

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### Steps

1. Click **Administration > Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server > AutoSupport**.
3. To read about what periodic AutoSupport entails, click **View AutoSupport Description**.

   The dialog box also displays the product System ID, which is a unique ID for your Performance Manager instance that technical support uses to find your AutoSupport messages.
4. Click **Generate and Send AutoSupport**.

## Configuring NTP settings

You can use the NTP Server dialog box to specify the Network Time Protocol (NTP) server you want to use with Performance Manager. The Performance Manager server synchronizes its time with the time on the NTP server.

### Before you begin

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### Steps

1. Click **Administration > Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server > NTP Server**.
3. In the **NTP Server** dialog box, type the host name/FQDN or IP address of the NTP server.
4. Click **Save and Close** to apply the setting.

   Host names and FQDNs are resolved to IP addresses and stored as IP addresses. When you open the NTP Server dialog box, it displays the IP address.

## Configuring the network settings

You might want to edit network settings if an IP address of a virtual machine (VM), for example, changes or if you switch from a DHCP to a static IP configuration.

### Before you begin

- You might need one or more of the following: host name or FQDN, IP address, DHCP, network mask, gateway, primary and secondary DNS addresses, and search domains.
- If you are changing your network settings from DHCP-enabled to static IP, you should have done the following:
  - Ensured that the IP address does not contain a duplicate address.
  - Ensured that the gateway is reachable.
  - Verified that the primary and secondary DNS addresses are ready and available to send and receive network traffic.
- You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### About this task

The self-signed SSL certificate generated during deployment is associated with the host name (or FQDN) and the IP address. If you change either of these values and want to use that new host name or IP address to connect to Performance Manager, then you must generate a new certificate and restart the Performance Manager virtual machine. The new certificate does not take effect until the Performance Manager virtual machine is restarted.

### Steps

1. Click **Administration > Configure Network Settings**.
2. In the **Configure Network Settings** dialog box, modify the host and network settings, as required.

   **Tip:** You can enter multiple comma-separated values in the Secondary DNS Address and Search Domains fields.
3. Click **Save and Close**.

### After you finish

After you have modified the settings of your network configuration, you can use the updated configuration to access Performance Manager.

## Working with HTTPS security certificates

You can view and regenerate an existing HTTPS certificate or download and install new certificates.

### Before you begin

You must be signed in to Performance Manager as the maintenance user or have the OnCommand Administrator or Storage Administrator role assigned to you to perform these tasks.

### About this task

During deployment of the virtual appliance, a self-signed SSL certificate is generated and is associated with the “OnCommand” host name and a user-specified IP address. You can use this certificate, generate a new one, or download a certificate signing request and install a certificate signed by a Certificate Authority. You can also view the content of the certificate you are using.

### Choices

- *Generating an HTTPS security certificate* on page 58

  You might generate a new HTTPS security certificate for multiple reasons, including if you want to sign with a different Certificate Authority or if the current security certificate has expired. The new certificate replaces the existing certificate.
- *Downloading an HTTPS certificate signing request* on page 59

  You can download a certification request for the current HTTPS security certificate so that you can provide the file to a Certificate Authority to sign. A CA-signed certificate helps prevent man-in-the-middle attacks and provides better security protection than a self-signed certificate.
- *Installing an HTTPS security certificate* on page 59

  You can upload and install a security certificate after a Certificate Authority has signed and returned it. The file that you upload and install must be a signed version of the existing self-signed certificate. A CA-signed certificate helps prevent man-in-the middle attacks and provides better security protection than a self-signed certificate.
- *Viewing the HTTPS security certificate* on page 57

  You can compare the HTTPS certificate details to the retrieved certificate in your browser to ensure that your browser's encrypted connection to Performance Manager is not being intercepted. You can also view the certificate to verify the content of a regenerated certificate or to view alternate URL names from which you can access Performance Manager.

# Protocol and port requirements

Using a browser, API client, or SSH, the required ports must be accessible to the Performance Manager GUI and APIs. The required ports and protocols enable communication between the

Performance Manager virtual machine and the managed storage systems, servers, and other components.

### Connections to the Performance Manager server

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

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

| Interface | Protocol | Port | Description |
|---|---|---|---|
| Performance Manager GUI | HTTP | 80 | Used to access the Performance Manager GUI; automatically redirects to the secure port 443. |
| Performance Manager GUI and programs using APIs | HTTPS | 443 | Used to securely access the Performance Manager GUI or to make API calls; API calls can only be made using HTTPS. |
| Maintenance console | SSH/ SFTP | 22 | Used to access the maintenance console and retrieve support bundles. |

### Connections from the Performance Manager server

You must configure your firewall to open ports that enable communication between the Performance Manager server and managed storage systems, servers, and other components. If a port is not open, communication fails.

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

The Performance Manager server connects using the following protocols and ports to the managed storage systems, servers, and other components:

| Destination | Protocol | Port | Description |
|---|---|---|---|
| Storage system | HTTPS | 443/TCP | Used to monitor and manage storage systems |
| AutoSupport server | HTTPS | 443 | Used to send AutoSupport information. Requires internet access to perform this function. |
| Authentication server | LDAP | 389 | Used to make authentication requests, and user and group lookup requests. |
| Mail server | SMTP | 25 | Used to send alert notification email. |
| NTP server | NTP | 123/UDP | Used to synchronize the time on the Performance Manager server with an external NTP time server. |

# Page descriptions for system setup

You use the pages and dialog boxes in the GUI for configuring communication between the Performance Manager server and your network, and for enabling or disabling AutoSupport. When enabled, AutoSupport routinely sends information about your Performance Manager instance to technical support.

## AutoSupport dialog box

The AutoSupport dialog box enables you to view the AutoSupport description, enable periodic AutoSupport, or send an on-demand AutoSupport message. The dialog box also displays the product System ID, which is a unique ID for your Performance Manager instance that technical support uses to find your AutoSupport messages.

### Information

You can perform the following operations:

| | |
|---|---|
| **View AutoSupport Description** | Displays the AutoSupport description, including the customer benefits and security description. |

### Actions

You can perform the following operations:

| | |
|---|---|
| **Enable Periodic AutoSupport** | Enables you to have specific, predefined messages to technical support periodically generated for issue diagnosis and resolution. |
| **Generate and Send AutoSupport** | Enables you to generate an on-demand message to send to technical support for any issues that have recently occurred. |

## NTP Server dialog box

You can use this dialog box to specify the NTP server that you want to use with Performance Manager. The Performance Manager server synchronizes its time with the time on the NTP server.

You can enter the host name or IP address of the NTP server and click **Save** to save the setting.

Host names and FQDNs are resolved to IP addresses and stored as IP addresses. When you open the NTP Server dialog box, it displays the host names.

## Configure Network Settings dialog box

You must configure the required network settings to connect to the Performance Manager server. You can use the Configure Network Settings dialog box to modify the settings of your network configuration.

### Host

The Host area provides the host name:

| | |
|---|---|
| **Host Name** | Displays the host name of the system on which the management server is installed. |

### Network

The Network area provides information about the network, such as the IP address, network mask, and DNS information:

| | |
|---|---|
| **DHCP Enabled** | Specifies whether DHCP is enabled.<br>**Note:** If DHCP is enabled, the system populates the IP address, network mask, and gateway fields with values from the network, and these fields appear dimmed. Also, you cannot change the values for the primary DNS address, secondary DNS address, or the search domains. |
| **IP Address** | Specifies the IP address of the Performance Manager server. |
| **Network Mask** | Specifies the network mask. |
| **Gateway** | Specifies the IP address of the gateway. |
| **Primary DNS Address** | Specifies the IP address of the primary DNS server. |
| **Secondary DNS Address** | Specifies the IP address of the secondary DNS server. |
| **Search Domains** | Specifies the domain names (as comma-separated values) that are used by the DNS server to search for the host name. |

# Managing data sources

You can manage the Data ONTAP clusters you want to use in Performance Manager, including adding, editing, and removing clusters.

## Adding clusters

You can add an existing cluster to Performance Manager to monitor the cluster and obtain information about its status and configuration.

### Before you begin

- The following information must be available:
  - Host name or cluster management IP address
    The host name is the FQDN or short name that Performance Manager uses to connect to the cluster. This host name must resolve to the cluster-management IP address.
    The cluster management IP address must be the cluster-management LIF. If you use a node-management LIF, the operation fails.
  - User name and password to access the cluster. This account must have the *Admin* role with Application access set to *ontapi*.
  - Type of protocol (HTTP or HTTPS) that is be configured on the cluster and the port number of the cluster
  - OnCommand Performance Manager requires that any volumes that you want to monitor be in a QoS policy group. Volumes that are not in a policy group are automatically added to the default policy group when you add the cluster. When Performance Manager analyzes the cluster for configuration changes every 15 minutes, it adds any new volumes not in a policy group to the default policy group. If an SVM is in a policy group, Performance Manager cannot monitor the volumes contained in the SVM and the overall analysis is impacted. Removing the SVM from the policy group corrects this issue.
- You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### About this task

**Attention:** Adding the same cluster to more than one instance of Performance Manager impacts the performance of the cluster. When attempting to add a cluster that Performance Manager instance is already monitoring, a warning message is displayed in the GUI.

### Steps

1. Click **Administration > Manage Data Sources**.

2. On the **Manage Data Sources** page, click **Add**.
3. In the **Add Cluster** dialog box, specify the values as required and then click **Save and Close**.

### Result

The cluster is added to the Performance Manager database after the default monitoring interval of approximately 15 minutes. If you destroy a Performance Manager virtual machine (VM) and then install a new instance using the same IP address assigned to the previous VM, adding the clusters from the previous VM to the new VM will display an error message that the clusters are already monitored. You can ignore this error message.

**Note:** If the UUID of a monitored cluster changes, due to a cluster rebuild, for example, Performance Manager does not associate the new UUID with the cluster and the cluster is no longer monitored. To associate the cluster to the new UUID, you must remove the cluster from Performance Manager and then re-add it.

### Related concepts

*Supported cluster configurations* on page 10

### Related references

*Performance Manager user roles and capabilities* on page 40
*Manage Data Sources page* on page 34

## Supported cluster configurations

A single instance of Performance Manager supports a specific number of clusters and volumes. If Performance Manager is monitoring an environment that exceeds the supported configuration, there might be problems with collecting and analyzing configuration and performance data from the cluster. You can install multiple instances of Performance Manager to monitor larger configurations.

The following table lists the supported number of clusters and volumes that Performance Manager can reliably support.

| Storage objects | Maximum supported |
|---|---|
| Clusters | 6 |
| Nodes | • For a single cluster: 6<br>• For 2 clusters: 4<br>• For 3 or more clusters: 2 |

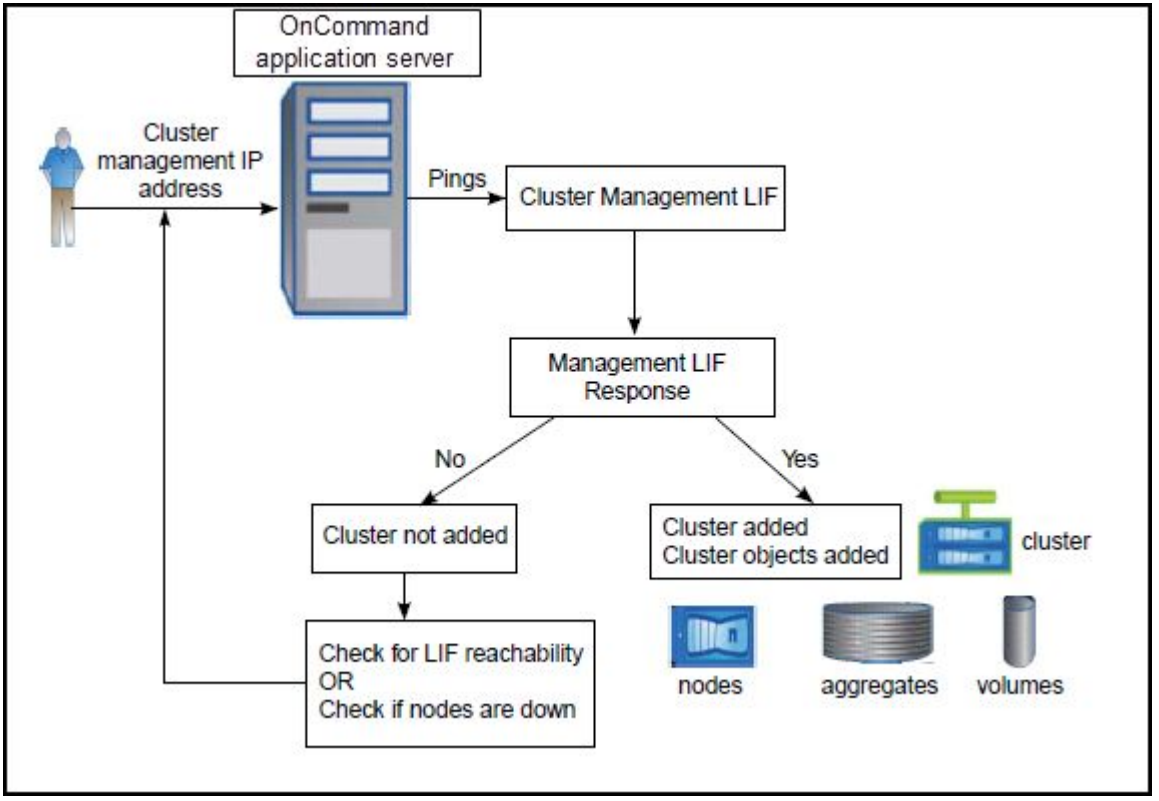
| Storage objects | Maximum supported |
| --- | --- |
| Volumes per node | • For a single cluster with 6 nodes: 200<br>• For up to 2 clusters and up to 4 nodes per cluster: 500<br>• For 3 to 6 clusters with no more than 2 nodes per cluster: 200 |

## How the discovery process works

After you have added the cluster to Performance Manager, the server discovers the cluster objects and adds them to its database. Understanding how the discovery process works helps you to manage your organization's clusters and their objects.

The default monitoring interval for cluster configuration information is 15 minutes. For example, after you have added a cluster, it takes 15 minutes to display the cluster details in the Performance Manager GUI.

The following image illustrates the discovery process:




### Related tasks

*Adding clusters* on page 28

## Viewing the clusters list

You can use the Manage Data Sources page to view your inventory of clusters. You can view details about the clusters, such as their name or IP address and communication status.

### Before you begin

You must be assigned one of the following roles to perform this task: Operator, OnCommand Administrator, or Storage Administrator.

### Step

1. Click **Administration > Manage Data Sources**.

### Related references

*Performance Manager user roles and capabilities* on page 40
*Manage Data Sources page* on page 34

# Editing clusters

You can modify the settings of an existing cluster, such as the host name or IP address, user name, password, protocol, and port by using Performance Manager. For example, you can change the protocol from HTTP to HTTPS using the Edit Cluster dialog box.

### Before you begin

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### About this task

**Attention:** If you change the IP address of a cluster to an IP address of an existing monitored cluster, all data for the existing cluster is lost when the former cluster is discovered. An error message is not displayed to warn you.

### Steps

1. Click **Administration** > **Manage Data Sources**.
2. On the **Manage Data Sources** page, select the cluster you want to edit and click **Edit**.
3. In the **Edit Cluster** dialog box, modify the values as required.
4. Click **Save**.

### Related references

*Performance Manager user roles and capabilities* on page 40
*Manage Data Sources page* on page 34

# Removing clusters

You can remove a cluster from Performance Manager by using the Manage Data Sources page. For example, you can remove a cluster when you want to decommission a storage system.

### Before you begin

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### About this task

The passwords for the maintenance user and for the remote user cannot be changed from the web UI. To change the maintenance user password, use the maintenance console. To change the remote user password, contact your password administrator.

### Steps

1. Click **Administration** > **Manage Data Sources**.
2. On the **Manage Data Sources** page, select the cluster that you want to remove and click **Remove**.
3. Click **Yes** to confirm the remove request.

### Result

The cluster, its storage objects along with the history, and all associated events are removed, and the cluster is no longer monitored by Performance Manager. The instance of Performance Manager registered with the removed cluster is also unregistered from the cluster.

### Related references

*Performance Manager user roles and capabilities* on page 40
*Manage Data Sources page* on page 34

## Searching for storage objects

You can use the search bar to find your storage objects. Search results are sorted by storage object type, and you can filter them using the drop-down menu. A valid search must contain at least three characters.

### Step

1. Type your search parameters into the search bar. You can use the filter to select a specific storage object type for your search. If you want to search for one of your volumes, select **Volumes** from the filter, and then type the name of the volume or type any three characters in the volume's name in the search bar. You can then select the appropriate volume from the drop-down list.

## Page descriptions for data source management

You can view and manage your clusters, including adding, editing, and removing clusters, from a single page.

The topics below display when you click **Help** on the appropriate page.

## Manage Data Sources page

The Manage Data Sources page enables you to add clusters and to view detailed information about the clusters that you are monitoring.

### Command buttons

The command buttons enable you to perform the following tasks for a selected cluster:

**Add** Opens the Add Cluster dialog box, which enables you to add clusters.

**Edit** Opens the Edit Cluster dialog box, which enables you to edit the settings of the selected cluster.

**Remove** Removes the selected cluster and all the associated events and storage objects. After the cluster is removed, it is no longer monitored.

**Attention:** The cluster, its storage objects, and all associated events are removed, and the cluster is no longer monitored by Performance Manager. The instance of Performance Manager registered with the removed clustered, is also unregistered from the cluster.

### Clusters list

The Clusters list displays, in tabular format, the properties of all the discovered clusters. You can use the column filters to customize the data that is displayed:

**Host Name or IP Address** Displays the host name, Fully Qualified Domain Name (FQDN), short name, or the IP address of the cluster-management LIF that is used to connect to the cluster.

**Protocol** Displays the type of protocol that can be configured on the cluster: HTTP or HTTPS (for a secure connection). Connection is established with the cluster by using both protocols and HTTPS is chosen over HTTP. The default is HTTPS with port 443.

**Port** Displays the port number of the cluster. If the port is not specified, the default port for the selected protocol is used (80 for HTTP or 443 for HTTPS).

**User Name** Displays the user name that can be used to log in to the cluster.

**Status** Displays the current status of the cluster. Possible values are:

- Normal—Cluster is operating normally.
- Authorization failure—Invalid credentials for accessing the cluster.
- Network access failure—Network connection issue or a network timeout occurred.
- LIF error—Issue with a node-management or cluster-management LIF.

- Duplicate datasource—Duplicate data sources, such as clusters, are being monitored.
- ZAPI error—Issue with the cluster that is preventing data collection.
- Internal error
- Unknown

| | |
|---|---|
| **Status Message** | Brief description of the current cluster status. |

## Add Cluster dialog box

You can add an existing cluster to monitor the cluster and obtain information about its health, capacity, and configuration.

You can add a cluster by specifying the following options:

| | |
|---|---|
| **Host Name or IP Address** | Enables you to specify the host name (preferred) or the IP address of the cluster-management LIF that is used to connect to the cluster. By specifying the host name you will be able to match the name of the cluster across the GUI, rather than trying to correlate an IP address on one page to a host name on another page, for example. |
| **User Name** | Enables you to specify a user name that can be used to log in to the cluster. |
| **Password** | Enables you to specify a password for the specified user name. |
| **Protocol** | Enables you to specify the type of protocol that can be configured on the cluster. You can enable HTTP or HTTPS (for a secure connection). Connection is established with the cluster by using both protocols and HTTPS is chosen over HTTP. By default, HTTPS is enabled with the default port 443. |
| **Port** | Enables you to specify the port number of the cluster. If the port is not specified, the default port for the selected protocol is used (80 for HTTP or 443 for HTTPS). |

### Related concepts

*Supported cluster configurations* on page 10

### Related tasks

*Adding clusters* on page 28

### Related references

*Performance Manager user roles and capabilities* on page 40
*Manage Data Sources page* on page 34

## Edit Cluster dialog box

The Edit Cluster dialog box enables you to modify the settings of an existing cluster, including the IP address, port, and protocol. For example, you can change the protocol from HTTP to HTTPS.

You can edit the following fields:

| | |
|---|---|
| **Host Name or IP Address** | Enables you to specify the FQDN, short name, or the IP address of the cluster-management LIF that is used to connect to the cluster. |
| **User Name** | Enables you to specify a user name that can be used to log in to the cluster. |
| **Password** | Enables you to specify a password for the specified user name. |
| **Protocol** | Enables you to specify the type of protocol that can be configured on the cluster. You can enable HTTP or HTTPS (for a secure connection). Connection is established with the cluster by using both protocols and HTTPS is chosen over HTTP. By default, HTTPS is enabled with the default port 443. |
| **Port** | Enables you to specify the port number of the cluster. If the port is not specified, the default port for the selected protocol is used (80 for HTTP or 443 for HTTPS). |

### Related tasks

*Editing clusters* on page 32
*Adding clusters* on page 28

# Managing users

You can manage the users who use Performance Manager, including setting up user accounts, configuring user authentication, and assigning user roles for controlling access to specific features.

## What the maintenance user does

Created during initial configuration, the maintenance user can create subsequent users and assign them roles. The maintenance user can also access the maintenance console and has the role of OnCommand Administrator in the GUI.

The maintenance user can perform the following functions using the maintenance console:

- Configure network access
- Upgrade to newer versions of Performance Manager
- Shut down virtual appliances (only from VMware console)
- Increase data disk or swap disk size
- Change the time zone
- Send on-demand AutoSupport messages to technical support from the maintenance console
- Generate support bundles to send to technical support

#### Related concepts

*Using the maintenance console* on page 66

#### Related references

*Definitions of user types* on page 38
*Definitions of user roles in Performance Manager* on page 39
*Performance Manager user roles and capabilities* on page 40

## What RBAC is

RBAC (role-based access control) provides the ability to control who has access to various features and resources in Performance Manager.

### What RBAC does

Role-based access control (RBAC) enables administrators to manage groups of users by defining roles. If you need to restrict access for specific functionality to selected administrators, you must set up administrator accounts for them. If you want to restrict the information that administrators can

view and the operations they can perform, you must apply roles to the administrator accounts you create.

The management server uses RBAC for user login and role permissions. If you have not changed the management server's default settings for administrative user access, you do not need to log in to view them.

When you initiate an operation that requires specific privileges, the management server prompts you to log in. For example, to create administrator accounts, you must log in with Administrator account access.

## Authentication with Active Directory or OpenLDAP

You can enable remote authentication on the management server and configure the management server to communicate with your authentication servers so that users within the authentication servers can access Performance Manager.

The following LDAP servers are compatible with the management server:

- Microsoft Active Directory
- OpenLDAP
- IBM Lotus LDAP
- Netscape LDAP Server

You can use one of the following predefined authentication services or specify your own authentication service:

- Microsoft Active Directory

  **Note:** You cannot use Microsoft Lightweight Directory Services.

- OpenLDAP

You can select the required authentication service and add the appropriate authentication servers to enable the remote users in the authentication server to access Performance Manager. The credentials for remote users or groups are maintained by the authentication server. The management server uses the Lightweight Directory Access Protocol (LDAP) to authenticate remote users within the configured authentication server.

For local users who are created in Performance Manager, the management server maintains its own database of user names and passwords. The management server performs the authentication and does not use Active Directory or OpenLDAP for authentication.

## Definitions of user types

A user type specifies the kind of account the user holds, and includes remote users, remote groups, local users, database users, and maintenance users. Each of these types has its own role, which is assigned by a user with the role of OnCommand Administrator.

Your Performance Manager user types are as follows:

| | |
|---|---|
| **Maintenance user** | Created from the maintenance console during the initial configuration of Performance Manager and its credentials are stored on the Performance Manager server. The maintenance user then creates additional users and assigns roles. The maintenance user is also the only user with access to the maintenance console. |
| **Local user** | Accesses the Performance Manager GUI using the credentials stored on the Performance Manager server. User perform functions based on the role given by the maintenance user or a user with the OnCommand Administrator role. |
| **Remote group** | Groups of users that access the Performance Manager GUI using the credentials stored on the authentication server. The name of this account should match the name of a group stored on the authentication server. All users within the remote group are given access to the Performance Manager GUI using their individual user credentials. Remote groups can perform functions according to their assigned roles. |
| **Remote user** | Accesses the Performance Manager GUI using the credentials stored on the authentication server. A remote user performs functions based on the role given by the maintenance user or a user with the OnCommand Administrator role. |
| **Database user** | Has read-only access to data in the Performance Manager database, has no access to the Performance Manager GUI or the maintenance console, and cannot execute API calls. |

#### Related concepts

*What the maintenance user does* on page 37

## Definitions of user roles in Performance Manager

The maintenance user or OnCommand administrator assigns a role to every user. Each role contains certain privileges. The scope of activities that you can perform in Performance Manager depends on the role you are assigned and which privileges the role contains.

The following predefined roles exist in Performance Manager:

| | |
|---|---|
| **Operator** | Views storage system information and other data collected by Performance Manager. |
| **Storage Administrator** | Configures storage management operations within Performance Manager. The role enables the storage administrator to create alerts and configure other storage management-specific options. |
| **OnCommand Administrator** | Configures settings unrelated to storage management. The role enables the management of users, database access, and administrative options, including authentication, SMTP, networking, and AutoSupport. |

## Performance Manager user roles and capabilities

Based on your assigned role, you can determine which operations you can perform in Performance Manager.

The following table displays the functions that each role can perform:

| Function | Operator | Storage Administrator | OnCommand Administrator |
|---|---|---|---|
| View storage system information | • | • | • |
| View events | • | • | • |
| Define alerts | | • | • |
| Manage storage management options | | • | • |
| Manage users | | | • |
| Manage administrative options | | | • |
| Manage database access | | | • |

#### Related concepts

*What the maintenance user does* on page 37

# Adding users

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

#### Before you begin

- To add a remote user or group, you must have enabled remote authentication and configured your authentication server.
- You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### About this task

If you add a group from active directory, then all direct members and nested subgroups can authenticate to Performance Manager. If you add a group from OpenLDAP or Other authentication services, then only direct members of that group can authenticate to Performance Manager.

### Steps

1. Click **Administration** > **Manage Users**.
2. In the **Manage Users** page, click **Add**.
3. In the **Add User** dialog box, select the type of user that you want to create and enter the required information.
4. **Note:** The specified email address must be unique to the instance of Performance Manager.

   Click **Save and Close**.

### Related tasks

*Enabling remote authentication* on page 48
*Setting up authentication services* on page 48
*Adding authentication servers* on page 50

### Related references

*Performance Manager user roles and capabilities* on page 40
*Manage Users page* on page 44

## Viewing users

You can use the Manage Users page to view the list of users who manage storage objects and data using Performance Manager. You can view details about the users, such as the name, type of user, email address, and role assigned to the users.

### Before you begin

### Step

1. Click **Administration** > **Manage Users**.

   The list of users is displayed in the Manage Users page.

### Related references

*Performance Manager user roles and capabilities* on page 40
*Manage Users page* on page 44

# Editing the user settings

You can edit user settings, such as the email address and role specified for users on the Manage Users page. For example, you might want to change the role of a user who is a storage operator, and assign storage administrator privileges to that user.

### Before you begin

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### About this task

When you modify the role assigned to a user, the changes are applied when either of the following occurs:

- The user logs out and logs back in to Performance Manager
- Session timeout of 24 hours has occurred

### Steps

1. Click **Administration** > **Manage Users**.
2. In the **Manage Users** page, select the user that you want to edit and click **Edit**.
3. In the **Edit User** dialog box, edit the appropriate settings that are specified for the user.
4. Click **Save and Close**.

### Related references

*Performance Manager user roles and capabilities* on page 40
*Manage Users page* on page 44

# Changing the local user password

You can change your login password to prevent potential security risks.

### Before you begin

You are logged in as a local user.

### About this task

The passwords for remote users or members of remote groups cannot be changed from the GUI. To change the remote user password, contact your password administrator.

### Steps

1. Log in to the Performance Manager GUI.
2. Click ***user_name*** > **Change Password**.

   The **Change Password** option is not displayed if you are a remote user.
3. In the **Change Password** dialog box, enter the details as required.
4. Click **Save**.

### Related references

*Performance Manager user roles and capabilities* on page 40

## Deleting users or groups

You can delete one or more users from the management server database to prevent the users from accessing Performance Manager.

### Before you begin

- When you are deleting remote groups, you must first have reassigned the events that are assigned to users of those remote groups.
- You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### About this task

**Attention:** To ensure that you have at least one user account for accessing Performance Manager, do not delete the maintenance user account.

### Steps

1. Click **Administration** > **Manage Users**.
2. In the **Manage Users** page, select the users or groups that you want to delete and click **Delete**.
3. Click **Yes** to confirm the delete request.

### Related references

*Performance Manager user roles and capabilities* on page 40

# Page descriptions for user management

You can manage user access to Performance Manager, including adding, editing, and removing users, from a single page.

The topics below display when you click **Help** on the appropriate page.

## Manage Users page

The Manage Users page displays a list of users and groups, and provides information such as the name, type of user, email address, and role. You can also perform tasks such as adding, editing, deleting, and testing users.

### Command buttons

The command buttons enable you to perform the following tasks for selected users:

**Add** Displays the Add User dialog box, which enables you to add a local user, remote user, remote group, or a database user.

You can add remote users or groups only if your authentication server is enabled and configured.

**Edit** Displays the Edit User dialog box, which enables you to edit the settings for the selected user.

**Remove** Removes the selected users from the management server database.

### List view

The List view displays, in tabular format, information about the users that are created. You can use the column filters to customize the data that is displayed.

**Name** Displays the name of the user or group.

**Type** Displays the type of user. The user type can be Local User, Remote User, Remote Group, Database User, or Maintenance User.

**Email** Displays the email address of the user.

**Role** Displays the type of role that is assigned to the user. The role can be Operator, Storage Administrator, or OnCommand Administrator.

**Note:** This option is disabled for the Database User type.

#### Related tasks

*Viewing users* on page 41

*Adding users* on page 40
*Editing the user settings* on page 42
*Deleting users or groups* on page 43

## Add User dialog box

You can create local users or database users, or add remote users or remote groups and assign roles so that these users can efficiently manage the storage objects and data using Performance Manager.

You can add a user by completing the following fields:

| | |
|---|---|
| **Type** | Enables you to specify the type of user you want to create. |
| **Name** | Enables you to specify a user name that a user can use to log in to Performance Manager. |
| **Password** | Enables you to specify a password for the specified user name. This field is displayed only when you are adding a local user or a database user. |
| **Confirm Password** | Enables you to reenter your password to ensure the accuracy of what you entered in the Password field. This field is displayed only when you are adding a local user or a database user. |
| **Email** | Enables you to specify an email address for the user. This field is displayed only when you are adding a remote user or a local user.<br>**Note:** The specified email address must be unique to the instance of Performance Manager. |
| **Role** | Enables you to assign a role to the user and defines the scope of activities that the user can perform. The role can be OnCommand Administrator, Storage Administrator, or Operator. |

### Related tasks

*Adding users* on page 40

### Related references

*Manage Users page* on page 44
*Performance Manager user roles and capabilities* on page 40

## Edit User dialog box

The Edit User dialog box enables you to edit the email address or role of a selected user.

### Details

The Details area enables you to edit the following information about a selected user:

**Type** Enables you to modify the type of user.

**Name** Enables you to change the user name of the selected user.

**Email** Enables you to edit the email address of the selected user.

**Role** Enables you to edit the role that is assigned to the user. This field is displayed only when the selected user is a local user, remote user, or remote group.

### Related tasks

*Editing the user settings* on page 42

### Related references

*Performance Manager user roles and capabilities* on page 40
*Manage Users page* on page 44

# Managing user authentication

You can configure Performance Manager to use an authentication server, using LDAP or Active Directory, for authenticating user access to Performance Manager.

## Authentication with Active Directory or OpenLDAP

You can enable remote authentication on the management server and configure the management server to communicate with your authentication servers so that users within the authentication servers can access Performance Manager.

The following LDAP servers are compatible with the management server:

- Microsoft Active Directory
- OpenLDAP
- IBM Lotus LDAP
- Netscape LDAP Server

You can use one of the following predefined authentication services or specify your own authentication service:

- Microsoft Active Directory

  **Note:** You cannot use Microsoft Lightweight Directory Services.

- OpenLDAP

You can select the required authentication service and add the appropriate authentication servers to enable the remote users in the authentication server to access Performance Manager. The credentials for remote users or groups are maintained by the authentication server. The management server uses the Lightweight Directory Access Protocol (LDAP) to authenticate remote users within the configured authentication server.

For local users who are created in Performance Manager, the management server maintains its own database of user names and passwords. The management server performs the authentication and does not use Active Directory or OpenLDAP for authentication.

# Enabling remote authentication

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

### Before you begin

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### About this task

If remote authentication is disabled, remote users or groups will no longer be able to access Performance Manager. The only two supported remote authentication methods are Active Directory and Open LDAP.

### Steps

1. Click **Administration > Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server > Authentication**.
3. In the **Authentication** dialog box, select **Enable Remote Authentication**.
4. Optional: Add authentication servers and test the authentication.
5. Click **Save and Close**.

### Related references

*Performance Manager user roles and capabilities* on page 40

# Setting up authentication services

Authentication services enable the authentication of remote users or groups in an authentication server before providing them access to Performance Manager. You can authenticate users by using the predefined authentication services, such as Active Directory or OpenLDAP, or by configuring your own authentication mechanism.

### Before you begin

- You must have enabled remote authentication.
- You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### Steps

1. Click **Administration** > **Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server** > **Authentication**.
3. In the **Authentication** dialog box, select one of the following authentication services:

| If you select... | Then do this... |
|---|---|
| Active Directory | **a.** Enter the administrator name and password. You can specify the administrator name in one of the following formats:<br>• domainname\username<br>• username@domainname<br>• Bind Distinguished Name, using the appropriate LDAP notation.<br>**b.** Specify the base distinguished name of the authentication server.<br>For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is `dc=ou,dc=domain,dc=com`. |
| OpenLDAP | **a.** Enter the bind distinguished name and bind password.<br>**b.** Specify the base distinguished name of the authentication server.<br>For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is `dc=ou,dc=domain,dc=com`. |
| Others | **a.** Enter the bind distinguished name and bind password.<br>**b.** Specify the base distinguished name of the authentication server.<br>For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is `dc=ou,dc=domain,dc=com`.<br>**c.** Specify the LDAP protocol version that is supported by the authentication server.<br>**d.** Enter the user name, group membership, user group, and member attributes. |

**Note:** If you want to modify the authentication service, ensure that you first delete any existing authentication servers and then add new authentication servers.

4. Click **Save and Close**.

### Related tasks

*Enabling remote authentication* on page 48

### Related references

*Performance Manager user roles and capabilities* on page 40

# Adding authentication servers

You can add authentication servers and enable remote authentication on the management server to enable remote users within the authentication server to access Performance Manager.

### Before you begin

- The following information must be available:
  - Host name or IP address of the authentication server
  - Port number of the authentication server
- You must have enabled remote authentication and configured your authentication service so that the management server can authenticate remote users or groups in the authentication server.
- You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### About this task

If the authentication server that you are adding is part of a high-availability pair (using the same database), you can also add the partner authentication server. This enables the management server to communicate with the partner when one of the authentication servers is unreachable.

### Steps

1. Click **Administration > Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server > Authentication**.
3. In the **Authentication** dialog box, in the Servers area, click **Add**.
4. In the **Add Authentication Server** dialog box, specify either the host name or IP address of the server, and the port details.
5. Click **Save and Close**.

### Result

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

### After you finish

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

### Related concepts

*Authentication with Active Directory or OpenLDAP* on page 38

### Related tasks

*Enabling remote authentication* on page 48
*Setting up authentication services* on page 48
*Testing the configuration of authentication servers* on page 51

### Related references

*Performance Manager user roles and capabilities* on page 40

# Editing authentication servers

You can change the port that Performance Manager uses to communicate with your authentication server. You cannot configure Secure LDAP (LDAPS).

### Before you begin

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### Steps

1. Click **Administration > Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server > Authentication**.
3. In the **Authentication** dialog box, in the Servers area, select the authentication server that you want to edit, and then click **Edit**.
4. In the **Edit Authentication Server** dialog box, edit the port details.
5. Click **Save and Close**.

### Related references

*Performance Manager user roles and capabilities* on page 40

# Testing the configuration of authentication servers

You can validate the configuration of your authentication servers to ensure that the management server is able to communicate with the authentication servers. You can test the configuration by searching for a remote user or group from your authentication servers and authenticate the user or group using the configured settings.

### Before you begin

- You must have enabled remote authentication and configured your authentication service so that Performance Manager can authenticate the remote user or group.

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

### About this task

If the authentication service is set to Active Directory and if you are testing the authentication of remote users who belong to the primary group of the authentication server, information about the primary group is not displayed in the authentication results.

### Steps

1. Click **Administration > Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server > Authentication**.
3. In the **Authentication** dialog box, click **Test**.
4. In the **Test User** dialog box, specify the user name and password of the remote user or group, and then click **Test**.

   If you are authenticating a remote group, you must not enter the password.

### Related tasks

*Enabling remote authentication* on page 48
*Setting up authentication services* on page 48
*Adding authentication servers* on page 50

# Deleting authentication servers

You can delete an authentication server if you want to prevent Performance Manager from communicating with the authentication server. For example, if you want to change an authentication server that the management server is communicating with, you can delete the authentication server and add a new authentication server.

### Before you begin

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### About this task

When you delete an authentication server, remote users or groups of the authentication server will no longer be able to access Performance Manager.

### Steps

1. Click **Administration** > **Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server** > **Authentication**.
3. In the **Authentication** dialog box, in the Servers area, select one or more authentication servers that you want to delete, and then click **Delete**.
4. Click **Yes** to confirm the delete request.

### Related references

*Performance Manager user roles and capabilities* on page 40

# Page descriptions for user authentication

You can specify how users are authenticated when accessing Performance Manager.

The topics below display when you click **Help** on the appropriate page.

## Authentication dialog box

You can use the Authentication dialog box to configure the management server to communicate with your authentication server and authenticate remote users in the authentication server.

### Enable Remote Authentication

This area allows you to enable or disable remote authentication. You can enable remote authentication to enable the management server to authenticate remote users within the configured authentication servers.

**Authentication Service**
Enables you to configure the management server to authenticate users in directory service providers, such as Active Directory, OpenLDAP, or specify your own authentication mechanism. You can specify an authentication service only if you have enabled remote authentication.

**Active Directory**

- Administrator Name
  Specifies the administrator name of the authentication server. The name must include the domain name and user name. For example, domain\admin.
- Password
  Specifies the password to access the authentication server.
- Base Distinguished Name
  Specifies the location of the remote users in the authentication server. For example, if the domain name of

the authentication server is ou@domain.com, then the base distinguished name is `dc=ou,dc=domain,dc=com`.

**OpenLDAP**

- Bind Distinguished Name
  Specifies the bind distinguished name that is used along with the base distinguished name to find remote users in the authentication server.
- Bind Password
  Specifies the password to access the authentication server.
- Base Distinguished Name
  Specifies the location of the remote users in the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is `dc=ou,dc=domain,dc=com`.

**Others**

- Bind Distinguished Name
  Specifies the bind distinguished name that is used along with the base distinguished name to find remote users in the authentication server that you have configured.
- Bind Password
  Specifies the password to access the authentication server.
- Base Distinguished Name
  Specifies the location of the remote users in the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is `dc=ou,dc=domain,dc=com`.
- Version
  Specifies the Lightweight Directory Access Protocol (LDAP) version that is supported by your authentication server. You can specify whether the protocol version must be automatically detected or set the version to 2 or 3.
- User Name Attribute
  Specifies the name of the attribute in the authentication server that contains user login names to be authenticated by the management server.
- Group Membership Attribute
  Specifies a value that assigns the management server group membership to remote users based on an attribute and value specified in the user's authentication server.
- UGID
  If the remote users are included as members of a GroupOfUniqueNames object in the authentication server,

this option enables you to assign the management server group membership to the remote users based on a specified attribute in that GroupOfUniqueNames object.

- Member
  Specifies the attribute name that your authentication server uses to store information about the individual members of a group.
- User Object Class
  Specifies the object class of all users in the remote authentication server.
- Group Object Class
  Specifies the object class of all groups in the remote authentication server.

**Note:** If you want to modify the authentication service, you must first delete any existing authentication servers and add new authentication servers.

### Servers

This area displays the authentication servers that the management server communicates with to find and authenticate remote users. The credentials for remote users or groups are maintained by the authentication servers.

**Command buttons** Enables you to add, edit, or delete authentication servers.

- Add
  Displays the Add Server dialog box for adding an authentication server. You specify the name or IP address of the server and the port number.
  If the authentication server that you are adding is part of an high-availability pair (using the same database), you can also add the partner authentication server. This enables the management server to communicate with the partner when one of the authentication servers is unreachable.
- Edit
  Displays the Edit Server dialog box for editing the settings for an authentication server. You can edit the name or IP address of the server and the port number.
- Remove
  Deletes the selected authentication servers.

**Name or IP Address** Displays the host name or IP address of the authentication server that is used to authenticate the user on the management server.

**Port** Displays the port number of the authentication server.

### Test Authentication

This area enables you to test your configuration.

**Test** Validates the configuration of your authentication server by authenticating a remote user or group.

While testing, if you specify only the user name, the management server searches for the remote user in the authentication server, but does not authenticate the user. If you specify both the user name and password, the management server searches and authenticates the remote user.

You cannot test the authentication if remote authentication is disabled.

#### Related tasks

*Enabling remote authentication* on page 48
*Setting up authentication services* on page 48
*Adding authentication servers* on page 50
*Testing the configuration of authentication servers* on page 51
*Deleting authentication servers* on page 52

# Managing security certificates

You can configure HTTPS in the Performance Manager server to monitor and manage your clusters over a secure connection.

## Viewing the HTTPS security certificate

You can compare the HTTPS certificate details to the retrieved certificate in your browser to ensure that your browser's encrypted connection to Performance Manager is not being intercepted. You can also view the certificate to verify the content of a regenerated certificate or to view alternate URL names from which you can access Performance Manager.

#### Before you begin

You must be assigned one of the following roles to perform this task: Operator, OnCommand Administrator, or Storage Administrator.

#### Steps

1. Click **Administration > Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server > HTTPS**.
3. Click **View HTTPS Certificate**.

   The Subject DN field should display the same host name or fully qualified domain name (FQDN) that is displayed in the Configure Network Settings dialog box. The IP addresses should also be the same in the certificate and in the network settings.

   To view more detailed information about the security certificate, you can view the connection certificate in your browser.

## Restarting the Performance Manager virtual machine

You can restart the virtual machine from the maintenance console of Performance Manager. You might need to restart after generating a new security certificate or if there is a problem with the virtual machine.

#### Before you begin

The virtual appliance is powered on.

You are logged in to the maintenance console as the maintenance user of Performance Manager.

### About this task

You can also restart the virtual machine from vSphere by using the Restart Guest option. See the VMware documentation for more information.

### Steps

1. Access the maintenance console.
2. Select **System Configuration > Reboot Virtual Machine.**
3. Start the Performance Manager GUI from your browser and log in.

## Generating an HTTPS security certificate

You might generate a new HTTPS security certificate for multiple reasons, including if you want to sign with a different Certificate Authority or if the current security certificate has expired. The new certificate replaces the existing certificate.

### Before you begin

You must be logged in as the OnCommand Administrator role to perform this task.

### About this task

**Note:** If connections that enable performance monitoring are currently configured between the Unified Manager server and one or more Performance Manager servers, executing this task invalidates those connections and deactivates any further performance monitoring updates from Performance Manager servers to the Unified Manager GUI. You must reactivate those connections after completing this task.

### Steps

1. Click **Administration > Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server > HTTPS**.
3. Click **Regenerate HTTPS Certificate**.

   **Important:** You must restart the Performance Manager virtual machine before the new certificate will take effect. This can be done from the System Configuration option in the NetApp maintenance console or from the VM console.

### After you finish

After generating a new certificate, you can verify the new certificate information by viewing the HTTPS certificate.

If you need to reactivate performance monitoring updates from Performance Manager servers to the Unified Manager server, you must delete the connections that were invalidated by this task and reconfigure new connections.

# Downloading an HTTPS certificate signing request

You can download a certification request for the current HTTPS security certificate so that you can provide the file to a Certificate Authority to sign. A CA-signed certificate helps prevent man-in-the-middle attacks and provides better security protection than a self-signed certificate.

### Before you begin

You must be logged in as the OnCommand Administrator role to perform this task.

### Steps

1. Click **Administration > Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server > HTTPS**.
3. Click **Download HTTPS Certificate Signing Request**.
4. Save the `<hostname>.csr` file.

### After you finish

You can provide the file to a Certificate Authority to sign and then install the signed certificate.

# Installing an HTTPS security certificate

You can upload and install a security certificate after a Certificate Authority has signed and returned it. The file that you upload and install must be a signed version of the existing self-signed certificate. A CA-signed certificate helps prevent man-in-the middle attacks and provides better security protection than a self-signed certificate.

### Before you begin

You must have completed the following actions:

- Downloaded the Certificate Signing Request file and had it signed by a Certificate Authority
- Saved the certificate chain in PEM format
- Included all certificates in the chain, from the server certificate to the root signing certificate

You must be logged in as the OnCommand Administrator role to perform this task.

### Steps

1. Click **Administration > Configure Settings**.

2. In the **Configure Settings** dialog box, click **Management Server > HTTPS**.
3. Click **Install HTTPS Certificate**.
4. In the dialog box that displays, click **Browse** to locate the file to upload.
5. Select the file and click **Install** to install the file.

**Example certificate chain**

The following example shows how the certificate chain file might appear:

```
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

# Page descriptions for certificate management

You can use the Configure Settings dialog box to view the current security certificates and to generate new HTTPS certificates.

The topics below display when you click **Help** on the appropriate page.

## HTTPS Certificate dialog box

You can use the HTTPS Certificate dialog box to view the current security certificate, download a certificate signing request, generate a new HTTPS certificate, or install a new HTTPS certificate.

You must be logged in as the OnCommand Administrator role to perform this task.

### HTTPS Certificate

You can perform the following operations:

| | |
|---|---|
| **View HTTPS Certificate** | Enables you to view the current HTTPS certificate. If you have not generated a new HTTPS certificate, this is the certificate that was generated with your installation. |
| **Regenerate HTTPS Certificate** | Enables you to generate an HTTPS certificate, which replaces the previous security certificate. The new certificate is in effect after you restart the management server. |

| | |
|---|---|
| **Download HTTPS Certificate Signing Request** | Downloads a certification request for the currently installed HTTPS certificate. Your browser prompts you to save the `<hostname>.csr` file so that you can provide the file to a Certificate Authority to sign. |
| **Install HTTPS Certificate** | Enables you to upload and install a security certificate after a Certificate Authority has signed and returned it. The new certificate is in effect after you restart the management server. |

# Managing event notification

You can set up an SMTP server to enable email communication from Performance Manager and configure email alerts. The email alerts notify you about events on the cluster.

## Configuring email settings

You can configure SMTP settings for the Performance Manager server to send email notifications when an event is generated. You can specify the corresponding mail server to be used.

### Before you begin

The following information must be available:

- Email address from which the alert notification is sent
- Host name, user name, password, and default port to configure the SMTP server

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### Steps

1. Click **Administration > Configure Settings**.
2. In the **Configure Settings** dialog box, click **Management Server > Email**.
3. In the **Email** dialog box, configure the appropriate settings.

   You can specify the email address and SMTP server from which the alert notifications are sent.

   **Tip:** If the host name of the SMTP server cannot be resolved, you can specify the IP address of the SMTP server instead of the host name. After configuring the settings, you can click **Test** to confirm whether recipients can receive email alerts. The user name and password are only required if SMTP authorization is enabled.

### Related tasks

*Configuring email alerts* on page 63

### Related references

*Performance Manager user roles and capabilities* on page 40

# Configuring email alerts

You can specify which incidents from Performance Manager to alert on and the email recipients for those alerts. You can receive alerts for all new incidents, disable all email alerts, or exclude email alerts caused by a QoS policy group limit. By default, alerts are sent for all new incidents.

### Before you begin

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

### Steps

1. Click **Administration > Manage Alerts**.
2. In the **Configure Email Alerts** dialog box, configure the appropriate settings.

   **Note:** For Email Recipients, use a comma or semicolon, with or without spaces, to separate the addresses. If you enter several addresses, such as by copying and pasting from an email client, the addresses are automatically separated with commas after you click **Save**.

### Related tasks

*Configuring email settings* on page 62

### Related references

*Performance Manager user roles and capabilities* on page 40

# Page descriptions for notification management

You can manage event notifications, such as setting up an SMTP server and configuring email alerts, to have Performance Manager notify you about various cluster events.

The topics below display when you click **Help** on the appropriate page.

## Email dialog box

You can configure an SMTP server that the Performance Manager server uses to send email notifications when an event is generated. You can also specify a From address.

This dialog box enables you to configure the following SMTP server settings:

| | |
|---|---|
| **From Address** | Specifies the address that recipients will see in the From field of their email client. |

| | |
|---|---|
| **Host Name or IP Address** | Specifies the host name of your SMTP host server, which is used to send the alert notification to the specified recipients. |
| **User Name** | Specifies the SMTP user name. If SMTP authentication is not enabled on the SMTP server, this field is optional. |
| **Password** | Specifies the SMTP password. If SMTP authentication is not enabled on the SMTP server, this field is optional. |
| **Port** | Specifies the port that is used by the SMTP host server to send alert notification.<br>The default value is 25. |
| **Use STARTTLS** | A mechanism to provide secure communication by using the TLS/SSL protocols. Also known as start_tls and StartTLS. |
| **Use SSL** | Checking this box provides secure communication between the SMTP server and the management server. |

#### Related tasks

*Configuring email settings* on page 62

#### Related references

*Performance Manager user roles and capabilities* on page 40

## Configure Email Alerts dialog box

You can specify which incidents from Performance Manager to alert on and the email recipients for those alerts. You can also disable all email alerts for all recipients. Email alerts are sent immediately after an incident is detected.

The following options are displayed:

| | |
|---|---|
| **Send For** | This section lets you select to have email alerts sent for all incidents or to exclude incidents caused by a QoS policy group limit, when workloads have exceeded the throughput limit. You can also disable all email alerts. |
| **Send To** | This section lets you type the address of each email recipient. To remove a recipient, you can delete the appropriate address.<br>**Note:** For Email Recipients, use a comma or semicolon, with or without spaces, to separate the addresses. If you enter several addresses, such as by copying and pasting from an email client, the addresses are automatically separated with commas after you click **Save**. |

### Related tasks

*Configuring email alerts* on page 63

### Related references

*Performance Manager user roles and capabilities* on page 40

# Using the maintenance console

You can use the maintenance console to configure network settings, to configure and manage your virtual appliance, and to view server status to prevent and troubleshoot possible issues.

**Related concepts**

*What the maintenance console does* on page 66
*Diagnostic user capabilities* on page 67

**Related tasks**

*Sending a support bundle to technical support* on page 68

## What the maintenance console does

The maintenance console enables you to maintain the settings on your virtual appliance and to make any necessary changes to prevent issues from occurring.

You can use the maintenance console to perform the following actions:

- Troubleshoot any issues with your virtual appliance, especially if the Performance Manager GUI is not available.
- Upgrade to newer versions of Performance Manager.
- Send on-demand AutoSupport messages.
- Generate Support Bundles to send to technical support.
- Configure network settings.
- Change the maintenance user password.

## What the maintenance user does

Created during initial configuration, the maintenance user can create subsequent users and assign them roles. The maintenance user can also access the maintenance console and has the role of OnCommand Administrator in the GUI.

The maintenance user can perform the following functions using the maintenance console:

- Configure network access
- Upgrade to newer versions of Performance Manager
- Shut down virtual appliances (only from VMware console)
- Increase data disk or swap disk size
- Change the time zone

- Send on-demand AutoSupport messages to technical support from the maintenance console
- Generate support bundles to send to technical support

### Related concepts

*Using the maintenance console* on page 66

### Related references

*Definitions of user types* on page 38
*Definitions of user roles in Performance Manager* on page 39
*Performance Manager user roles and capabilities* on page 40

## Diagnostic user capabilities

The purpose of diagnostic access is to enable technical support to assist you in troubleshooting. You should only use it when directed by technical support personnel.

### Related concepts

*Using the maintenance console* on page 66

## Accessing the maintenance console using Secure Shell

If the Performance Manager GUI is not in operation, or if you need to perform functions that are not available in the user interface, you can access the maintenance console to reconfigure your virtual appliance.

### Before you begin

- You have installed and configured Performance Manager.
- You have the maintenance user role.
- No other maintenance console sessions, either from SSH or vSphere, are currently active.

### Steps

1. Using Secure Shell, connect to the IP address or fully qualified domain name of the Performance Manager virtual appliance.
2. Log in to the maintenance console using your maintenance user name and password.

   After 15 minutes of inactivity, the maintenance console logs you out.

### Related concepts

*Using the maintenance console* on page 66

# Accessing the maintenance console using the vSphere VM console

If the Performance Manager GUI is not in operation, or if you need to perform functions that are not available in the user interface, you can access the maintenance console to reconfigure your virtual appliance.

### Before you begin

You must be the maintenance user. The virtual appliance must be powered on to access the maintenance console.

### Steps

1. In vSphere Client, locate the Performance Manager virtual appliance.
2. Click the **Console** tab.
3. Click inside the console window to log in.
4. Log in to the maintenance console using your user name and password.

   After 15 minutes of inactivity, the maintenance console logs you out.

### Related concepts

*Using the maintenance console* on page 66

# Sending a support bundle to technical support

This workflow shows you how to generate, retrieve, and send a support bundle to technical support using the maintenance console. You should send a support bundle when the issue that you have requires more detailed diagnosis and troubleshooting than an AutoSupport message provides.

### Before you begin

You must be the maintenance user to complete this workflow.

### About this task

For more information about the maintenance console and support bundles, see *Using the maintenance console* on page 66.

Performance Manager stores two generated support bundles at one time. As new support bundles are generated, Performance Manager automatically deletes the older bundles and only keeps the latest two bundles.

### Related tasks

*Accessing the maintenance console using Secure Shell* on page 67

## Generating a support bundle

You can generate a support bundle containing full diagnostic information, so that you can then retrieve it and send it to technical support for troubleshooting help. Because some types of data can use a large amount of cluster resources or take a long time to complete, you can specify data types to include or exclude in the support bundle.

### Before you begin

You must have accessed the maintenance console as the maintenance user.

### About this task

Performance Manager stores two generated support bundles at one time.

### Steps

1. From **Main Menu**, select **Support/Diagnostics menu**.
2. Select **Generate Support Bundle**.

   The generated support bundle resides in the `/support` directory.
3. Select or deselect the following data types to include or exclude in the support bundle:
   - **database dump**- A dump of the MySQL Server database.
   - **heap dump** - A snapshot of the state of the main Performance Manager server processes.
   - **acquisition recordings** - A recording of all communications between the virtual appliance and the monitored clusters.

   **Note:** If you deselect all data types, the support bundle is still generated with other data from the virtual appliance and sent to technical support.
4. Type **g** and press **Enter** to generate the support bundle.

### After you finish

After generating the support bundle, you can retrieve it using an SFTP client or by using UNIX or Linux CLI commands.

### Related concepts

*Diagnostic user capabilities* on page 67

### Related references

*Performance Manager user roles and capabilities* on page 40

*OnCommand maintenance console menus* on page 72

## Retrieving the support bundle using a Windows client

If you are a Windows user, you can download and install a tool to retrieve the support bundle from your virtual appliance. You can send the support bundle to technical support for a more detailed diagnosis of an issue. Filezilla and WinSCP are examples of tools you can use.

### Before you begin

You must be the maintenance user to perform this task.

You must use a tool that supports SCP or SFTP.

### Steps

1. Download and install a tool to retrieve the support bundle.
2. Open the tool.
3. Connect to your Performance Manager management server over SFTP.

   The tool displays the contents of the `/support` directory and you can view all existing support bundles.
4. Select the destination directory and copy the support bundle.
5. Select the support bundle you want to copy and use the tool to copy the file from the Unified Manager server to your local system.

### Related information

*Filezilla - https://filezilla-project.org/*
*WinSCP - http://winscp.net*

## Retrieving the support bundle using a UNIX or Linux client

If you are a UNIX or Linux user, you can retrieve the support bundle from your virtual appliance by using the command-line interface (CLI) on your Linux client server. You can use either SCP or SFTP to retrieve the support bundle.

### Before you begin

You must be the maintenance user to perform this task.

You must have generated a support bundle using the maintenance console and have the support bundle name available.

### Steps

1. Access the CLI through Telnet or the console, using your Linux client server.

2. Access the `/support` directory.
3. Retrieve the support bundle and copy it to the local directory using the following command:

| If you are using... | Then use the following command... |
|---|---|
| SCP | **scp <maintenance-user>@<vApp-name-or-ip>:/support/ support_bundle_file_name.7z <destination-directory>** |
| SFTP | **sftp <maintenance-user>@<vApp-name-or-ip>:/support/ support_bundle_file_name.7z <destination-directory>** |

   The name of the support bundle is provided to you when you generate it using the maintenance console.

4. Enter the maintenance user password.

### Examples

The following example uses SCP to retrieve the support bundle:

```
$ scp admin@10.228.212.69:/support/
support_bundle_20130216_145359.7z .

Password:
maintenance_user_password
support_bundle_20130216_145359.7z    100%  119MB  11.9MB/s   00:10
```

The following example uses SFTP to retrieve the support bundle:

```
$ sftp admin@10.228.212.69:/support/
support_bundle_20130216_145359.7z .

Password:
maintenance_user_password
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to ./
support_bundle_20130216_145359.7z
/support/support_bundle_20130216_145359.7z
```

## Sending a support bundle to technical support

When directed by technical support, you can send a support bundle using the direction provided in KB article 1010090. You should send a support bundle when the issue requires more detailed diagnosis and troubleshooting than an AutoSupport message provides.

### Before you begin

You must have access to the support bundle to send it to technical support.

You must have a case number generated through the technical support web site.

### Steps

1. Log in to the NetApp Support Site.
2. Search for Knowledge Base article 1010090.
3. Follow the instructions on how to upload a file to technical support.

### Related information

*NetApp Support Site: support.netapp.com*

# OnCommand maintenance console menus

The maintenance console enables you to update Performance Manager, configure and maintain your Performance Manager network settings, and back up Performance Manager.

You access the maintenance console by selecting the virtual machine (VM) for Performance Manager in your vSphere Client and then selecting the **Console** tab. When you first log into the maintenance console, the Main Menu displays the following options:

### Upgrade

Initiates the VM upgrade of Performance Manager.

### Network Configuration

Provides options for configuring and maintaining the network settings for Performance Manager. The following options are displayed:

- **Display IP Address Settings**—Displays the current network settings for Performance Manager, such as the management IP address, netmask, gateway, and so on.
- **Change IP Address Settings**—Enables you to change any of the network settings for the virtual appliance, including the IP address, netmask, gateway, or DNS servers. If you switch your network settings from DHCP to static networking using the maintenance console, you cannot edit

the host name. The host name provided by DHCP is used. Accordingly, it is best to use the Performance Manager GUI. You must select **Commit Changes** for the changes to take place.

**Note:** If you want to change the IP address and Performance Manager has obtained its address using DHCP, in Performance Manager, you can click **Administration > Configure Network Settings** and enter or change the appropriate settings.

- **Display Domain Name Search Settings**—Searches for servers across multiple domains configured in **Change IP Address Settings** and displays the results.
- **Change Domain Name Search Settings**—Provides options for adding or changing domain names you want to use in a search (for example, yourcompany.com, yourcompany.local). Domain names added manually require a space between them, but no commas. If the DHCP server is properly configured, DNS names are added automatically.

  **Note:** The domain names you want to use in a search can be added using this option or through the web client in the Network Adapter section at **Administration > Configure Network Settings**. Performance Manager must then be rebooted.
- **Display Static Routes**—Displays configured static IP routes.
- **Change Static Routes**—Provides options for configuring static IP routes.
- **Disable Network Interface**—Provides options for disabling network adapters.
- **Enable Network Interface**—Provides options for enabling disabled network adapters.
- **Commit Changes**—Applies any changes made in the options above. Changes do not take effect until you commit them with this option. After selecting this option, you are given the opportunity to exit without saving your changes before the commit is performed.
- **Ping A Host**—Pings a target host for confirming IP address changes or proper DNS configuration.
- **Restore to Default Settings**—Resets all network settings to the default settings.

### System Configuration

Provides options for managing Performance Manager. The following options are displayed:

- **Display Server Status**—Determines whether the monitor for Performance Manager is running and the exact start date.
- **Reboot Virtual Machine**—Initiates the correct sequence of events to restart the VM for Performance Manager.
- **Shut Down Virtual Machine**—Initiates the correct sequence of events to shut down the VM for Performance Manager.
- **Change 'admin' User Password**—Changes the password for accessing the maintenance console.
- **Increase Data Disk Size**—Initiates the Performance Manager server to identify the new data disk size set in the vSphere Client.
- **Increase Swap Disk Size**—Initiates the Performance Manager server to identify the new swap disk size set in the vSphere Client.
- **Change Time Zone**—Changes the time zone for Performance Manager.

- **Change NTP Server**—Changes the IP address of the NTP server that Performance Manager uses to synchronize its time.

  **Note:** If you want to change the NTP server in Performance Manager, you can click **Administration > Configure NTP Settings** and enter FQDN/host name or IP address.

### Support/Diagnostics

Provides options for sending information about Performance Manager to NetApp Customer Support Services and accessing the Performance Manager server on the VM. The following options are displayed:

- **AutoSupport Submission**—Sends a file to NetApp Customer Support Services for assistance with troubleshooting issues. The AutoSupport file sent by Performance Manager contains diagnostic system information and detailed data about the Performance Manager server. You can select to email the file or to have it posted directly to AutoSupport.

  **Note:** If you want to send the message from Performance Manager, you can click **Administration > Configure AutoSupport Settings > Generate and Send AutoSupport**.

- **Generate Support Bundle**—Generates a large file that contains a dump of the database and other diagnostic data about Performance Manager and sends it to technical support. You can select or deselect the types of data to include in the support bundle. If you deselect all data types, the support bundle is still generated with other data from the virtual appliance and sent to technical support. For more information, see "Generating a support bundle" below.

When you generate the ASUP message from OnCommand Performance Manager, the following configuration and analytical data is included in the ASUP message:

- Number of incidents that have a state of new or obsolete over the last seven days.
- Top three cluster components with the highest number of incidents over the last seven days.
- Configuration changes caused by HA takeover, policy group limit modifications, or volume moves.
- Minimum, maximum, and average times for configuration and analytical data to be collected.
- Minimum, maximum, and average times for incident analysis to complete.
- Details about the virtual machine (VM), database, disk storage usage, and the number of errors and exceptions specific to Performance Manager.

ASUP or support messages that you generate through the maintenance console will not include the configuration and analytical data from Performance Manager.

### Unified Manager Connection

Provides options for connecting OnCommand Performance Manager to OnCommand Unified Manager. Once you establish the connection, incidents from Performance Manager will display in Unified Manager. The following options are displayed:

- **Display UM Server Connection**—View the current settings for a configured Unified Manager VM.

- **Change UM Server Connection**—Enter new settings for a Unified Manager VM or change existing settings.
- **Delete UM Server Connection**—Delete the existing settings for a Unified Manager VM. Once deleted, OnCommand Performance Manager will lose its connection to Unified Manager.

#### Related concepts

*What AutoSupport does* on page 21

#### Related tasks

*Configuring NTP settings* on page 22
*Configuring the network settings* on page 23
*Sending an on-demand AutoSupport message* on page 22
*Generating a support bundle* on page 69

## Purpose of a connection between Performance Manager and Unified Manager

A connection between a Performance Manager server and the Unified Manager server enables you to monitor through the Unified Manager web UI the performance issues that are detected by the Performance Manager server.

A connection between a Performance Manager server and the Unified Manager server is established through the menu option labeled "Unified Manager Server Connection" in the Performance Manager maintenance console.

#### Related tasks

*Configuring a connection between a Performance Manager server and the Unified Manager server* on page 75

## Configuring a connection between a Performance Manager server and the Unified Manager server

To enable display in the Unified Manager web UI of performance issues discovered by a Performance Manager server, you must configure a connection between that server and the Unified Manager server in the Performance Manager maintenance console.

#### Before you begin

- You must have created a local user with Event Publisher role privileges for the Unified Manager server in the connection you want to create.
- You must have a user ID authorized to log in to the maintenance console of the Performance Manager server for which you want to display performance data in the Unified Manager web UI.
- You must be prepared to specify the following information about the Unified Manager server:

- Unified Manager server name or IP address
- Unified Manager server default port 443
- Event Publisher user name (the name of the local Unified Manager server user assigned Event Publisher role privileges)
- Event Publisher password (the password of the local Unified Manager server user assigned Event Publisher role privileges)

### About this task

You can configure connections between one Unified Manager server and multiple Performance Manager servers.

For each connection, complete the following actions:

### Steps

1. Log in as the maintenance user to the maintenance console of the Performance Manager server for which you want to create the Unified Manager connection.
2. In the maintenance console, type the number of the menu option labeled "Unified Manager Server Connection" and then type the number of the menu option labeled "Add/Modify Unified Manager Server Connection."
3. When prompted, supply the requested Unified Manager server name or IP address and Unified Manager server port information.

   The maintenance console checks the validity of the specified Unified Manager server name or IP address and Unified Manager server port, and, if necessary, prompts you to accept the Unified Manager server trust certificate to support the connection. The default Unified Manager server port 443 must be used.
4. When prompted, supply the requested Event Publisher user name and Event Publisher password and then confirm that the settings are correct.

### Result

After the connection is complete, all new performance incidents discovered by Performance Manager are reflected on the Unified Manager Dashboard page and Events page.

### Related concepts

*Purpose of a connection between Performance Manager and Unified Manager* on page 75

# Troubleshooting common issues

There are common issues that you might encounter when using Performance Manager. You can take corrective actions to resolve these issues on your own.

## Unknown authentication error

**Issue**

When you are performing an authentication-related operation, such as adding, editing, deleting, or testing remote users or groups, the following error message might be displayed: `Unknown authentication error`.

**Cause**

This problem can occur if you have set an incorrect value for the following:

- Administrator Name of the Active Directory authentication service
- Bind Distinguished Name of the OpenLDAP authentication service

**Corrective action**

1. Click **Administration > Configure Settings**
2. In the Configure Settings dialog box, click **Management Server > Authentication**.
3. Based on the authentication service that you have selected, enter the appropriate information for Administrator Name or Bind Distinguished Name in the Authentication dialog box.
4. Click **Save and Close**.

## Icons are misaligned in Internet Explorer

**Issue**

Icons and text are misaligned when you use Internet Explorer.

**Cause**

This problem can occur if you are using Internet Explorer in Compatibility View, which is not a supported browser setting.

**Corrective action**

1. Press F12 to open Internet Explorer Developer Tools.
2. Select **Browser Mode** from the toolbar to display the browser version used to open the application.
3. Select **Document Mode** from the toolbar and select the Standards mode of the browser version used to open the application.

For example, if you are using Internet Explorer 9 to open the application, select **Browser Mode > Internet Explorer 9**, and then select **Document Mode > Internet Explorer 9 Standards**.

## LDAP server slow to respond

**Issue** The LDAP server takes a long time to respond to queries.

**Cause** Supporting nested groups causes the LDAP server to slow down.

**Corrective action** If you use Active Directory, you can speed authentication by disabling support for nested groups in Performance Manager. However, if you choose to disable nested groups, you must ensure that users are direct members of the groups added to Performance Manager.

To disable nested group support, follow these steps:

1. Click **Administration > Configure Settings > Authentication** to display the Authentication dialog box.
2. Select the **Enable Remote Authentication** check box.
3. In the **Authentication Service** drop-down menu, select **Others**.
4. In the **Member** box, type “member”.
5. Click **Save and Close**.

## Issue with adding LDAP using Other authentication services

**Issue** When you select Other in the Authentication dialog box, the user and groupObjectClass retain the values from the previously selected template. If the LDAP server does not use the same values, the operation might fail.

**Cause** The users are not configured correctly in OpenLDAP.

**Corrective action** You can manually fix this issue using one of the following workarounds.

If your LDAP user and object classes are user and group, respectively, then perform the following steps:

1. Click **Administration > Configure Authentication Settings** to display the Authentication dialog box.
2. In the **Authentication Service** drop-down menu, select **Active Directory** and then select **Others**.
3. Complete the text fields.

If your LDAP user and group object classes are posixAccount and posixGroup, respectively, then perform the following steps:

1. Click **Administration > Configure Authentication Settings** to display the Authentication dialog box.
2. In the **Authentication Service** drop-down menu, select **OpenLDAP** and then select **Others**.
3. Complete the text fields.

# Copyright information

# Trademark information

# How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. 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.

You can also contact us in the following ways:

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

# Index

## A



## B



## C

## R



## S

## T



## U



## V



## W