ONTAP® 9

Performance Monitoring Power Guide

October 2016 | [215-11609_A0]
doccomments@netapp.com

Updated for ONTAP 9.1
Release Candidate Documentation - Contents Subject To Change

NetApp®

Contents

Deciding whether to use the Performance Monitoring Power Guide

This guide describes how to install and configure both OnCommand Unified Manager and OnCommand Performance Manager, how to set up basic performance management tasks, and how to identify and resolve common performance issues.

You should use this guide if you want to monitor cluster performance, and the following assumptions apply to your situation:

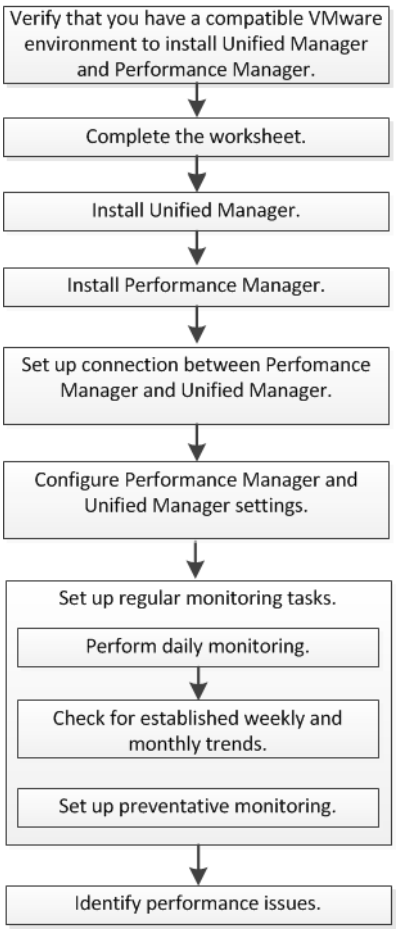
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.
- You want to display system status and alerts by using Unified Manager 7.0, in addition to the ONTAP command-line interface.
- You want to monitor cluster performance and perform root-cause analysis by using Performance Manager 7.0, in addition to the ONTAP command-line interface.
- You want to install the performance software by using a virtual appliance, instead of a Linux or Windows-based installation.
- You want to use a static configuration rather than DHCP to install the software.
- You want to connect one instance of Performance Manager to Unified Manager.
- You can access ONTAP commands at the advanced privilege level.
- You have determined that the cause of the performance issue is storage-related.
- You have ruled out any client-side protocol and network issues.

If these assumptions are not correct for your situation, you should see the following resources:

- *OnCommand Unified Manager 7.0 Installation and Setup Guide for VMware Virtual Appliances*
- *OnCommand Performance Manager 7.1 Installation and Administration Guide for VMware Virtual Appliances*
- *System administration*
- *Performance monitoring express setup*

Performance monitoring workflow

Monitoring cluster performance involves installing software, setting up basic monitoring tasks, and identifying performance issues.



Steps

1. Verifying that your VMware environment is supported on page 7
   For successful installation of Unified Manager and Performance Manager, you must verify that your VMware environment meets the necessary requirements.
2. Completing the worksheet on page 8
   Before you install, configure, and connect Unified Manager and Performance Manager, you should have specific information about your environment readily available. You can record the information in the worksheet.
3. Installing Unified Manager on page 9
   This guide assumes that you will install Unified Manager before installing Performance Manager and monitoring cluster performance.
4. Installing Performance Manager on page 10
   To install the Performance Manager software, you must download the virtual appliance (VA) installation file, and then use a VMware vSphere Client to deploy the file to a VMware ESXi server. The VA is available in an `OVA` file.

5. Setting up a connection between Performance Manager and Unified Manager on page 11
   After installing the Performance Manager software, you must create a user with Event Publisher privileges on Unified Manager, and then pair Performance Manager to run in the full integration connection mode with a Unified Manager server.
6. Configuring Performance Manager and Unified Manager settings on page 13
   You must add clusters to the Performance Manager server and Unified Manager server to monitor cluster performance. Additionally, you must configure alert settings to report critical events and warnings.
7. Setting up basic monitoring tasks on page 16
   You can monitor your systems for performance issues by checking the systems daily, thereby establishing weekly and monthly performance trends. You can also create thresholds to receive notifications about potential performance issues to prevent critical performance issues.

Verifying that your VMware environment is supported

For successful installation of Unified Manager and Performance Manager, you must verify that your VMware environment meets the necessary requirements.

Steps

1. Verify that your VMware infrastructure meets the sizing requirements for the installation of both Unified Manager and Performance Manager.
2. Go to the Interoperability Matrix to verify that you have a supported combination of the following components:
   - ONTAP version
   - ESXi operating system version
   - VMware vCenter Server version
   - VMware Tools version
   - Browser type and version

   Note: The Interoperability Matrix lists the supported configurations for both Unified Manager and Performance Manager.
3. Click the configuration name for the selected configuration.

   Details for that configuration are displayed in the Configuration Details window.
4. Review the information in the following tabs:
   - Notes
     Lists important alerts and information that are specific to your configuration.
   - Policies and Guidelines
     Provides general guidelines for all configurations.

Completing the worksheet

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

Unified Manager installation information

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

Unified Manager configuration information

Setting	Your value
Maintenance user email address	
NTP server	
SMTP server host name or IP address	
SMTP user name	
SMTP password	
SMTP default port	25 (Default value)
Username for user with Event Publisher role	
Password for user with Event Publisher role	
Email from which alert notifications are sent	
Active Directory administrator name	
Active Directory password	
Base distinguished name	
Active Directory server host name or IP address	

Performance Manager installation information

Virtual machine on which software is deployed	Your value
Host fully qualified domain name	
IP address	
Network mask	
Gateway IP address	
DNS address	
Maintenance user name	
Maintenance user password	

Performance Manager configuration information

Setting	Your value
Email from which alert notifications are sent	
SMTP server host name or IP address	
SMTP user name	
SMTP password	
SMTP default port	25 (Default value)
Active Directory administrator name	
Active Directory password	
Base distinguished name	
Active Directory server host name or IP address	

Cluster information

Cluster	Your value
Host name or cluster-management IP address	
ONTAP administrator user name	
ONTAP administrator password	
Protocol (HTTP or HTTPS)	

Installing Unified Manager

This guide assumes that you will install Unified Manager before installing Performance Manager and monitoring cluster performance.

Downloading and deploying Unified Manager

To install the software, you must download the virtual appliance (VA) installation file and then use a VMware vSphere Client to deploy the file to a VMware ESXi server. The VA is available in an OVA file.

Steps

1. Go to the NetApp Support Site Software Download page and locate OnCommand Unified Manager for Clustered Data ONTAP.

   NetApp Downloads: Software

2. Select **VMware vSphere** in the Select Platform drop-down menu and click **Go!**
3. Save the `OVA` file to a local or network location that is accessible to your VMware vSphere Client.
4. In VMware vSphere Client, click **File > Deploy OVF Template**.
5. Locate the `OVA` file and use the wizard to deploy the virtual appliance on the ESXi server.

   You can use the Properties tab in the wizard to enter your static configuration information.
6. Power on the VM.
7. Click the **Console** tab to view the initial boot process.
8. Follow the prompt to install VMware Tools on the VM.
9. Configure the time zone.
10. Enter a maintenance user name and password.
11. Go to the URL displayed by the VM console.

Configuring initial Unified Manager settings

The OnCommand Unified Manager Initial Setup dialog box appears when you first access the web UI, which enables you to configure some initial settings and to add clusters.

Steps

1. Enable AutoSupport.
2. Enter the NTP server details, the maintenance user email address, the SMTP server host name, and additional SMTP options, and then click **Save**.
3. Click **Add Cluster**, and add all of your clusters for monitoring.

Installing Performance Manager

To install the Performance Manager software, you must download the virtual appliance (VA) installation file, and then use a VMware vSphere Client to deploy the file to a VMware ESXi server. The VA is available in an `OVA` file.

Steps

1. Go to the NetApp Support Site Software Download page, and locate OnCommand Performance Manager (Unified Manager Performance Pkg).

   NetApp Downloads: Software

2. Select **VMware vSphere** from the **Select Platform** drop-down menu, and click **Go!**
3. Save the `OVA` file to a local or network location that is accessible to your VMware vSphere Client.
4. In the VMware vSphere Client, click **File > Deploy OVF Template**.
5. Locate the `OVA` file, and use the wizard to deploy the virtual appliance on the ESXi server.
6. Power on the VM.
7. Click the **Console** tab to view the initial boot process.
8. Follow the prompt to install VMware Tools on the VM.
9. Configure the VM.
    a. Enter the time zone information.
    b. Enter the fully qualified domain name.
    c. Enter the IP address and netmask.
    d. Enter the DNS server IP address.
    e. Enter the gateway IP address.
    f. Enter the maintenance user name and password.
    g. Enter the OnCommand login.

Setting up a connection between Performance Manager and Unified Manager

After installing the Performance Manager software, you must create a user with Event Publisher privileges on Unified Manager, and then pair Performance Manager to run in the full integration connection mode with a Unified Manager server.

Creating a user that has Event Publisher privileges

Before setting up the connection, you must create a local user in Unified Manager that has the Event Publisher role and privileges. This user receives the performance incident notifications.

Steps

1. Log in to Unified Manager and navigate to the **Health** dashboard.
2. Click **Administration > Manage Users**.
3. Click **Add**.
4. Select **Local User** as the type and **Event Publisher** as the role.
5. Finish entering the information in the dialog box and click **Add**.

Pairing a Performance Manager server with a Unified Manager server

You must pair a Performance Manager server with a Unified Manager server to display performance statistics and events that are discovered by the Performance Manager server in the Unified Manager web UI. The process of pairing is also known as a full integration connection.

Before you begin

- The Unified Manager server must be running Unified Manager 7.0.
- You must have a user ID that is authorized to log in to the maintenance console of the Performance Manager server.
- You must have the following information about the Unified Manager server:
  - Unified Manager server name or IP address
  - Unified Manager Administrator user name and password
  - Unified Manager Event Publisher user name and password

  Important: When Unified Manager is installed in a high-availability configuration, you must use the global IP address; you cannot use the Unified Manager server name or fully qualified domain name (FQDN). When using the FQDN, the last part cannot be a single letter—for example, `vm.company.a` is invalid.
- The Unified Manager server, Performance Manager servers, and the clusters that are being managed either must be set to the same absolute (UTC) time or must use the same NTP server; otherwise, new performance events are not correctly identified.

About this task

You can configure connections between a single Unified Manager server and up to five Performance Manager servers.

Steps

1. Log in using SSH as the maintenance user to the Performance Manager host to access the maintenance console.

   The Performance Manager maintenance console prompts are displayed.
2. Type the number of the menu option labeled **Unified Manager Integration**.
3. If prompted, enter the maintenance user password again.
4. Select **Full Integration** > **Enable Full Integration**.
5. When prompted, enter the requested Unified Manager server name or IP address (IPv4 or IPv6).

   The maintenance console checks the validity of the specified Unified Manager server name or IP address (IPv4 or IPv6) and, if necessary, prompts you to accept the Unified Manager server trust certificate to support the connection.
6. When prompted, enter the Unified Manager Administrator user name and password.
7. When prompted, enter the Unified Manager Event Publisher user name and password.
8. When prompted, enter the unique name for this instance of Performance Manager.

   This name enables you to identify the Performance Manager instance that you want to manage when multiple Performance Manager instances are integrated with Unified Manager.
9. When prompted, enter **y** to confirm that the information that you entered is correct.

10. When pairing is complete, press any key to return to the **Unified Manager Integration** menu.
11. Type **x** to exit the maintenance console.

    The virtual appliance is restarted automatically.

Configuring Performance Manager and Unified Manager settings

You must add clusters to the Performance Manager server and Unified Manager server to monitor cluster performance. Additionally, you must configure alert settings to report critical events and warnings.

Adding a cluster to a Performance Manager server and Unified Manager server

You must add a cluster to a Performance Manager server and a Unified Manager server simultaneously to monitor the cluster performance.

Adding a cluster to a Unified Manager server

You must add a cluster to a Unified Manager server to monitor the cluster, view the cluster discovery status, and monitor its performance by using the Performance Manager software.

Before you begin

- You must have the following information:
  - Host name or cluster-management IP address
    The host name is the fully qualified domain name (FQDN) or short name that Unified Manager uses to connect to the cluster. This host name must resolve to the cluster-management IP address.
    The cluster-management IP address must be the cluster-management LIF of the administrative Storage Virtual Machine (SVM). If you use a node-management LIF, the operation fails.
  - ONTAP administrator user name and password
  - Type of protocol (HTTP or HTTPS) that can be configured on the cluster and the port number of the cluster
- You must have the OnCommand Administrator or Storage Administrator role.
- The ONTAP administrator must have the ONTAPI and SSH administrator roles.
- The Unified Manager FQDN must be able to ping ONTAP.
  You can verify this by using the ONTAP command `ping -node` *`node_name`* `-destination` *`Unified_Manager_FQDN`*.

About this task

For a MetroCluster configuration, you must add both the local and remote clusters, and the clusters must be configured correctly.

Steps

1. Click **Storage > Clusters**.
2. From the Clusters page, click **Add**.

3. In the **Add Cluster** dialog box, specify the required values, such as the host name or IP address (IPv4 or IPv6) of the cluster, user name, password, protocol for communication, and port number.

   By default, the HTTPS protocol is selected.

   You can change the cluster-management IP address from IPv6 to IPv4 or from IPv4 to IPv6. The new IP address is reflected in the cluster grid and the cluster configuration page after the next monitoring cycle finishes.

4. Click **Add**.

5. If HTTPS is selected, perform the following steps:

   a. In the **Authorize Host** dialog box, click **View Certificate** to view the certificate information about the cluster.

   b. Click **Yes**.

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

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

6. Optional: View the cluster discovery status:

   a. Click the **Data Sources** link from the discovery status message that is displayed in the **Clusters** page.

   b. Review the cluster discovery status from the **Manage Data Sources** page.

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

7. Click the **Performance** link to configure an instance of Performance Manager and select the required Performance Manager instance from the **Select Application Instance** drop-down list.

8. Click **Save**.

Adding a cluster to a Performance Manager server

You must add a cluster to a Performance Manager server to monitor the cluster.

Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- The Performance Manager server to which you want to add the cluster must be running Performance Manager 7.0.
- You must have logged in to the Unified Manager server that is paired with the Performance Manager server.
- The user name and password that are used to access the cluster must have the *admin* role, with Application access set to *ontapi*, *ssh*, and *http*.

About this task

A cluster should be managed by only one instance of Performance Manager.

While adding the first cluster, you must perform the Performance Manager initialization tasks. Both procedures are described in the following steps.

A single instance of Performance Manager supports a specific number of clusters and storage objects. If Performance Manager is monitoring an environment that exceeds the supported configuration, it

might have difficulty collecting and analyzing configuration and performance data from the clusters. See the *OnCommand Performance Manager Release Notes* for the number of clusters, nodes, and volumes that Performance Manager can reliably support.

Steps

1. Use a web browser to log in to the Unified Manager web UI by using the IP address or URL and an appropriate user name and password.
2. From the **Managed Clusters** list, select the cluster that you want to add, and then click  > **Edit**.

   The Edit Cluster page is displayed in the right pane.
3. From the **Link Performance Manager** section, select the Performance Manager server that will monitor the cluster.
4. Click **Save**.
5. If you selected the HTTPS protocol, perform the following steps:
   a. In the **Authorize Host** dialog box, click **View Certificate** to view the certificate information of the cluster.
   b. Click **Yes** to authorize Performance Manager to communicate with the cluster.

   The result depends on whether the Performance Manager server is initialized:

   - If the server is initialized, the cluster is added to the server.
     After the initial cluster inventory and data collection has completed (which might take up to 30 minutes), performance statistics are displayed in the UI.
   - If the server is not initialized, a new browser window is displayed.
6. If the server is not initialized, follow the instructions in the new browser window to set up email and AutoSupport:
   a. Specify an initial email recipient to which email alerts will be sent, and the SMTP server that will handle email communications.
   b. Specify whether AutoSupport is enabled to send information about your Performance Manager installation to technical support.
   c. Click **Save and Complete Initialization**.
7. Return to the **Edit Cluster** page in the original browser window.
8. Click **Save**.

Result

After all of the objects are discovered, Performance Manager gathers historical performance data for the previous 24 hours. This enables you to view a full day of historical performance information for a cluster immediately after it is added. After the historical data is collected, real-time cluster performance data is collected every five minutes, by default.

Configuring alert settings

You can specify which events from Performance Manager trigger alerts, the email recipients for those alerts, and whether the events should be reported to Unified Manager.

Before you begin

You must have the OnCommand Administrator role.

About this task

You can configure unique alert settings for the following types of performance events:

- Critical events triggered by breaches of user-defined thresholds
- Warning events triggered by breaches of user-defined thresholds, system-defined thresholds, or dynamic thresholds

By default, email alerts are sent to Performance Manager Admin users for all new events. You can have email alerts sent to other users by adding those users' email addresses.

You can choose to send the alerts to Unified Manager as Critical, Error, Warning, or Information events. If you have configured Unified Manager to send alert emails when it receives performance events, the email recipients might receive notifications from both Performance Manager and Unified Manager.

Note: To disable alerts from being sent for certain types of events, clear all of the check boxes in an event category. This action does not stop events from appearing in the Performance Manager user interface.

Steps

1. From the Performance Manager navigation bar, select **Configuration > Event Handling**.

   The Event Handling page is displayed.

2. In the **Event Handling** page, configure the appropriate settings for each of the event types.

   To have email alerts sent to multiple users, enter a comma between each email address.

3. Click **Save**.

Setting up basic monitoring tasks

You can monitor your systems for performance issues by checking the systems daily, thereby establishing weekly and monthly performance trends. You can also create thresholds to receive notifications about potential performance issues to prevent critical performance issues.

Performing daily monitoring

You can perform daily monitoring to ensure that you do not have any immediate performance issues that require attention.

Steps

1. From the Performance Manager UI, go to the **Event Inventory** page and view all current and obsolete events.

2. Click on the new Critical or Warning events and determine what action is required.

Using weekly and monthly performance trends to identify performance issues

Identifying performance trends can assist you in identifying whether the cluster is being overused or underused by analyzing volume latency. You can use similar steps to identify CPU, network, or other system bottlenecks.

Steps

1. Locate the volume you suspect is being underused or overused.
2. On the **Details** tab, click **30 days** to display the historical data.
3. In the "Break down data by" drop-down menu, select **Latency** and click **Submit**.
4. Deselect Aggregate in the Compare the Cluster Components chart and compare with the Latency chart.
5. Select Aggregate and deselect all other components in the Compare the Cluster Components chart and compare with the Latency chart.
6. Compare the reads/writes latency chart to the Latency chart.
7. Determine if client application loads have caused a workload contention and rebalance workloads as needed.
8. Determine if the aggregate is overused and causing contention and rebalance workloads as needed.

Preventing performance issues

You can set user-defined thresholds to prevent performance issues from being critical. For example, if you have a Microsoft Exchange Server and you know that it will crash if volume latency goes above 20 milliseconds, you can set warning and critical thresholds to keep the server from crashing.

Steps

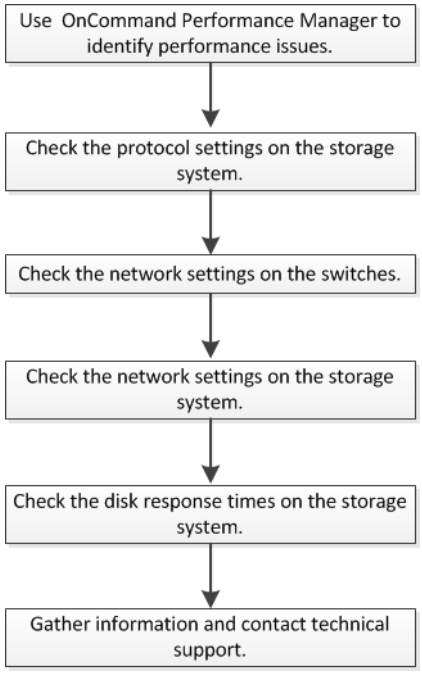
1. Create the Warning and Critical event thresholds:
   a. Select **Configuration > Threshold Policies**.
   b. Click **Create**.
   c. Select the object type and specify a name and description of the policy.
   d. Select the object counter condition and specify the limit values that define Warning and Critical events.
   e. Select the duration of time that the limit values must be breached for an event to be sent and click **Save**.
2. Assign the threshold policy to the storage object.
   a. Go to the Inventory page for the same cluster object type that you previously selected.
   b. Select the object to which you want to assign the threshold policy and click **Assign Threshold Policy**.
   c. Select the policy you previously created and click **Assign Policy**.

Example

You want to prevent your Microsoft Exchange Server from crashing due to average volume latency exceeding 20 milliseconds. The following example displays the Warning threshold set to 12 milliseconds and the Critical threshold to 15 milliseconds.

Identifying and resolving performance issues workflow

Identifying and resolving performance issues includes using Performance Manager to troubleshoot the issue, and then checking network and protocol settings to locate the source of the performance issue.



Steps

1. Using Performance Manager to identify performance issues on page 20
   If you receive an email notification or someone notifies you that there is a performance issue, you can locate the source of the issue within Performance Manager and resolve it by using other tools. If the issue is not resolved by using the remediation option in Performance Manager, you can perform other checks to identify the source of the issue and resolve it.
2. Identifying remaining performance capacity on page 21
   Knowing the available performance capacity in the cluster helps you provision workflows and balance them. Performance capacity is how much work you can place on a node or an aggregate before performance of all workloads begins to be affected by latency.
3. Measuring latency and throughput between nodes on page 22
   You can use the `network test-path` command to identify network bottlenecks, or to prequalify network paths between nodes. You can run the command between intercluster nodes or intracluster nodes.
4. Checking protocol settings on the storage system on page 24
   You can check that a performance issue is not related to protocol settings on your storage system. If the settings are the issue, you can take corrective action and then verify that the performance issue is resolved.
5. Checking the network settings on the data switches on page 26

You must maintain the same network settings on your clients, storage systems, and switches to ensure that performance is not impacted. All components in the network must have the same MTU setting for best performance.

6. Checking the MTU network setting on the storage system on page 26
   You can change the network settings on the storage system if they are not the same as on the client or data switches. Whereas the management network MTU setting is set to 1500, the data network MTU size should be 9000.
7. Checking the disk response times on page 26
   You can check to see what the disk response times are, and whether the aggregate I/O workload is sequential or random, to assist you in troubleshooting.
8. Collecting and viewing performance statistics on page 27
   You can use `statistics`*`object`*`show` commands to collect and view performance data for any storage system object.
9. Filtering performance statistics on page 28
   You can use filters to help you track resource utilization for a specific object, or narrow down the amount of statistics collected. Collecting statistics from 30,000 LUNs, for example, could take a long time to complete. You can save time by filtering LUN statistics by volume name.
10. Sorting performance statistics on page 29
    You can sort performance statistics by any counter to diagnose a performance issue or identify a hot spot. You might want to collect volume statistics and sort by total operations to get a list of the most active volumes.
11. Importing a performance preset configuration (cluster administrators only) on page 29
    You can create a custom performance preset or modify a writable performance preset by importing a performance preset configuration in XML file format. You can also use this method to modify what data is collected and stored in performance archives.
12. Viewing performance data for a time period on page 30
    You can monitor cluster or SVM performance by collecting and viewing data for a specific time period (a sample). You can view data for several objects and instances at a time.
13. Viewing continuously updated performance data on page 31
    You can monitor cluster or SVM performance by viewing data that continuously updates with the latest status. You can view data for only one object and one instance at a time.

Using Performance Manager to identify performance issues

If you receive an email notification or someone notifies you that there is a performance issue, you can locate the source of the issue within Performance Manager and resolve it by using other tools. If the issue is not resolved by using the remediation option in Performance Manager, you can perform other checks to identify the source of the issue and resolve it.

About this task

Monitoring the remaining performance capacity for a node or aggregate helps you with the following:

- Provisioning and balancing workflows.
  This information helps you make decisions about the placement of new volumes or the movement of volumes.
- Preventing a node from being overloaded.
- Preventing the resources of a node from being pushed beyond the optimal point.

You can monitor the performance capacity used for all nodes or for all aggregates in a cluster, or you can view details for a single node or aggregate. These values appear in the Dashboard, Inventory pages, Top Performers page, Create Threshold Policy page, Explorer pages, and detail charts.

You might have to use a combination of tools—such as System Manager, Unified Manager, Workflow Automation (WFA), or the command-line interface (CLI)—to resolve any other issues.

Steps

1. Click the link in the email notification, which takes you directly to the **Event Details** page.
2. If the performance issue is due to a system-defined threshold event, perform the actions suggested in the UI.
3. In the Performance Manager **Events Summary** page, verify that the issue has been resolved.

Identifying remaining performance capacity

Knowing the available performance capacity in the cluster helps you provision workflows and balance them. Performance capacity is how much work you can place on a node or an aggregate before performance of all workloads begins to be affected by latency.

About this task

You can also complete this task using OnCommand tools to obtain the remaining performance capacity.

Steps

1. Change to advanced privilege level:

   `set -privilege advanced`

2. Start the statistics command line prompt:

   `statistics start –object resource_headroom_`*`cpu`*

3. Display real-time headroom information:

   `statistics show -object resource_headroom`

4. Return to administrative privilege:

   `set -privilege admin`

Sample Output

```
sti2520-2131454963690::*> stat show -obj resource_headroom_cpu -raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                     -
                               ops                               4376
                           latency                              37719
                       utilization                                 86
                  optimal_point_ops                              2573
              optimal_point_latency                              3589
         optimal_point_utilization                                 72
     optimal_point_confidence_factor                                1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
```

```
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                     -
                                 ops                                0
                             latency                                0
                         utilization                                0
                    optimal_point_ops                               0
                optimal_point_latency                               0
           optimal_point_utilization                               71
     optimal_point_confidence_factor                                1
2 entries were displayed.
```

You compute the available performance capacity by subtracting the `optimal_point_counter` from the `current_counter`. In this example, the utilization capacity for `CPU_sti2520-213` is -14% (72%-86%). This suggests that the node's CPU has been overutilized on average for the past one hour.

Additionally, you could have specified `ewma_daily`, `ewma_weekly`, or `ewma_monthly` to get the same information, but averaged over a longer period of time.

Note: The `resource_headroom_cpu` Counter Manager (CM) object in this example represents the entire node (all CPUs collectively). You can get the available performance capacity on aggregates using the same `stat` command syntax but with the `resource_headroom_aggr` CM object.

```
sti2520-2131454963690:::*> statistics show -object resource_headroom_aggr -counter
ewma_weekly -raw

Object: resource_headroom_aggr
Instance: DISK_HDD_aggr1_2acca201-3b24-4b9e-abcc-39e624461822
Start-time: 2/26/2016 14:33:46
End-time: 2/26/2016 14:33:46
Scope: qos-3270-2

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_weekly                                                     -
                                 ops                              303
                    optimal_point_ops                             794
                             latency                            16121
                optimal_point_latency                           19123
                         utilization                               36
           optimal_point_utilization                               85
     optimal_point_confidence_factor                                3
1 entries were displayed.
```

Measuring latency and throughput between nodes

You can use the `network test-path` command to identify network bottlenecks, or to prequalify network paths between nodes. You can run the command between intercluster nodes or intracluster nodes.

Before you begin

- You must be a cluster administrator to perform this task.
- Advanced privilege level commands are required for this task.
- For an intercluster path, the source and destination clusters must be peered.

About this task

Occasionally, network performance between nodes may not meet expectations for your path configuration. A 1 Gbps transmission rate for the kind of large data transfers seen in SnapMirror replication operations, for example, would not be consistent with a 10 GbE link between the source and destination clusters.

You can use the `network test-path` command to measure latency and throughput between nodes. You can run the command between intercluster nodes or intracluster nodes.

Note: The test saturates the network path with data, so you should run the command when the system is not busy and when network traffic between nodes is not excessive. The test times out after ten seconds. The command can be run only between ONTAP 9 nodes.

The `session-type` option identifies the type of operation you are running over the network path—for example, "AsyncMirrorRemote" for SnapMirror replication to a remote destination. The type dictates the amount of data used in the test. The following table defines the session types:

Session Type	Description
Default	SnapMirror replication between nodes in different clusters
AsyncMirrorLocal	SnapMirror replication between nodes in the same cluster
AsyncMirrorRemote	SnapMirror replication between nodes in different clusters
SyncMirrorRemote	SyncMirror replication between nodes in different clusters
RemoteDataTransfer	Data transfer between nodes in the same cluster (for example, an NFS request to a node for a file stored in a volume on a different node)

Steps

1. Change to advanced privilege level:

   `set -privilege advanced`

2. Measure latency and throughput between nodes:

   `network test-path -source-node` *`source_nodename`*`|local -destination-cluster` *`destination_clustername`* `-destination-node` *`destination_nodename`* `-session-type Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer`

   The source node must be in the local cluster. The destination node can be in the local cluster or in a peered cluster. A value of "local" for `-source-node` specifies the node on which you are running the command.

   #### Example

   The following command measures latency and throughput for SnapMirror-type replication operations between "node1" on the local cluster and "node3" on "cluster2":

   ```
   cluster1::> network test-path -source-node node1 -destination-cluster
   cluster2 -destination-node node3 -session-type AsyncMirrorRemote
   Test Duration:      10.88 secs
   Send Throughput:    18.23 MB/sec
   Receive Throughput: 18.23 MB/sec
   MB sent:            198.31
   MB received:        198.31
   Avg latency in ms:  2301.47
   Min latency in ms:  61.14
   Max latency in ms:  3056.86
   ```

3. Return to administrative privilege level:

   `set -privilege admin`

After you finish

If performance does not meet expectations for the path configuration, you should check node performance statistics, use available tools to isolate the problem in the network, check switch settings, and so forth.

Checking protocol settings on the storage system

You can check that a performance issue is not related to protocol settings on your storage system. If the settings are the issue, you can take corrective action and then verify that the performance issue is resolved.

Checking the NFS TCP read/write size

For NFS, you can check the TCP read/write size to determine if the size setting is creating a performance issue. If the size is the source of an issue, you can correct it.

About this task

Advanced privilege level commands are required for this task.

Steps

1. For NFS, check the TCP receive window size:

   vserver nfs show -vserver *vserver_name* -instance

2. Change the TCP maximum read size:

   vserver nfs modify -vserver *vserver_name* -v3-tcp-max-read-size *integer*

3. Change the TCP maximum write size:

   vserver nfs modify -vserver *vserver_name* -v3-tcp-max-write-size *integer*

Example

The following example changes the maximum read and write size of vs1 to 1048576:

```
cluster1::*> vserver nfs modify -vserver vs1 -v3-tcp-max-read-size
1048576  -v3-tcp-max-write-size 1048576
```

Related information

ONTAP 9 man page: vserver nfs modify

Checking the iSCSI TCP read/write size

For iSCSI, you can check the TCP read/write size to determine if the size setting is creating a performance issue. If the size is the source of an issue, you can correct it.

About this task

Advanced privilege level commands are required for this task.

Steps

1. Check the TCP window size setting:

vserver iscsi show -vserver *vserver_name* -instance

2. Modify the TCP window size setting:

   vserver iscsi modify -vserver *vserver_name* -tcp-window-size *integer*

> **Example**
>
> The following example changes the TCP window size of vs1 to 131,400 bytes:
>
> ```
> cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size
> 131400
> ```

Related information

ONTAP 9 man page: vserver iscsi modify

Checking the CIFS multiplex settings

If slow CIFS network performance causes a performance issue, you can modify the multiplex settings to improve and correct it.

Steps

1. Check the CIFS multiplex setting:

   vserver cifs options show -vserver *-vserver_name* -instance

2. Modify the CIFS multiplex setting:

   vserver cifs options modify –vserver *-vserver_name* –max-mpx *integer*

> **Example**
>
> The following example changes the maximum multiplex count on SVM1 to 255:
>
> ```
> cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
> ```

Checking the FC adapter port speed

The adapter target port speed should match the speed of the device to which it connects, to optimize performance. If the port is set to autonegotiation, it can take longer to reconnect after a takeover and giveback or other interruption.

Before you begin

All LIFs that use this adapter as their home port must be offline.

Steps

1. Take the adapter offline:

   network fcp adapter modify -node *nodename* -adapter *adapter* -state *down*

2. Check the maximum speed of the port adapter:

   fcp adapter show -instance

3. Change the port speed, if necessary:

```
network fcp adapter modify -node nodename -adapter adapter -speed {1|2|
4|8|10|16|auto}
```

4. Bring the adapter online:

   ```
   network fcp adapter modify -node nodename -adapter adapter -state up
   ```

5. Bring all the LIFs on the adapter online:

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port
   e0c } -status-admin up
   ```

Example

The following example changes the port speed of adapter 0d on node1 to 2 Gbps:

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -
speed 2
```

Checking the network settings on the data switches

You must maintain the same network settings on your clients, storage systems, and switches to ensure that performance is not impacted. All components in the network must have the same MTU setting for best performance.

Step

1. For data switches, check that the MTU size is set to 9000.

   For more information, see the switch vendor documentation.

Checking the MTU network setting on the storage system

You can change the network settings on the storage system if they are not the same as on the client or data switches. Whereas the management network MTU setting is set to 1500, the data network MTU size should be 9000.

Steps

1. Check the MTU port settings on the storage system:

   ```
   network port show -instance
   ```

2. Change the MTU port settings to 9000:

   ```
   network port modify -node nodename -port port -mtu 9000
   ```

Checking the disk response times

You can check to see what the disk response times are, and whether the aggregate I/O workload is sequential or random, to assist you in troubleshooting.

About this task

Advanced privilege level commands are required for this task.

Step

1. Check the disk throughput and latency metrics:

   `statistics disk show -sort-key latency`

Example

The following example displays the totals in each user read or write operation for node2 on cluster1:

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                    Busy Total Read  Write  Read    Write
*Latency
  Disk       Node  (%)   Ops   Ops   Ops   (Bps)    (Bps)
(us)
------------ ----   ---- ----   ----- ----- ------   -----    -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

Related information

ONTAP 9 man page: statistics disk show

Collecting and viewing performance statistics

You can use `statistics` ***`object`*** `show` commands to collect and view performance data for any storage system object.

Before you begin

You must be a cluster or SVM administrator to perform this task.

About this task

An object is any of the following:

- Physical entities such as disks, processors, and ports (cluster level only)
- Logical entities such as LUNs, volumes, and workloads
- Protocols such as CIFS, NFS, iSCSI, and FC

Each object has zero or more instances. A counter is a predefined performance metric that provides data about the object. Performance presets define what counters collect data for objects and whether any of the data is added to performance archives.

Step

1. Collect and view performance data for volumes:

   `statistics volume show -interval` ***`interval`*** **`-iterations`** ***`iterations`*** **`-max`** ***`maximum_instances`***

   If the number of iterations is 0, the command continues to run until you interrupt it by pressing Ctrl-C.

Example

In the following example, performance data for 25 volumes (the default) are collected five times over ten-second intervals:

```
cluster1::> statistics volume show -interval 10 -iterations 5
```

In the following example, performance data for 25 volumes is collected over five-second intervals (the default) until you manually stop data collection by pressing Ctrl-C:

```
cluster1::> statistics volume show -iterations 0
```

Filtering performance statistics

You can use filters to help you track resource utilization for a specific object, or narrow down the amount of statistics collected. Collecting statistics from 30,000 LUNs, for example, could take a long time to complete. You can save time by filtering LUN statistics by volume name.

Before you begin

You must be a cluster or SVM administrator to perform this task.

Step

1. Filter performance data for a volume:

   statistics volume show -volume *volume_name* -vserver *SVM_name* -interval *interval* -iterations *iterations* -max *maximum_instances*

   By default, the output includes the most important counters and sorts the results by the most active instances of the object you specify.

Example

In the following example, the output shows the volumes reporting the highest IOP values:

```
cluster1::> statistics volume show
cluster1 : 12/31/2013
16:00:04



                         *Total Read Write Other  Read Write
Latency
Volume Vserver Aggregate    Ops  Ops   Ops   Ops (Bps) (Bps)
(us)
------ ------- --------- ------ ---- ----- ----- ----- -----
-------
vol0       -   aggr0         58   13    15    29 9585   3014
39
vol1       -   aggr0_n0      56    0    11    45 8192  28826      47
```

In the following example, the output shows performance statistics only for vol1:

```
cluster1::> statistics volume show –volume
vol1
cluster1 : 12/31/2013
16:00:04



                         *Total Read Write Other   Read Write
Latency
Volume Vserver Aggregate    Ops  Ops   Ops   Ops  (Bps) (Bps)
(us)
------ ------- --------- ------ ---- ----- ----- ------ -----
```

```
-------
vol1       -   aggr0_n0      56    0    11    45   8192 28826      47
```

Sorting performance statistics

You can sort performance statistics by any counter to diagnose a performance issue or identify a hot spot. You might want to collect volume statistics and sort by total operations to get a list of the most active volumes.

Before you begin

Advanced privilege level commands are required for this task.

Step

1. Sort volume performance statistics:

   statistics volume show -volume *volume_name* -vserver *SVM_name* -sort-key *sort_counter* -interval *interval* -iterations *iterations* -max *maximum_instances*

Example

In the following example, the output is sorted by the `read_ops` counter:

```
 ::>statistics show -volume vol1 -sort-key read_ops

Object: volume
Instance: vol1
Start-time: 05/23/2014 4:00 PM
End-time: 05/23/2014 4:10 PM
Cluster: cluster1
Number of Constituents: 1 (complete_aggregation)
  Counter                             Value
  --------------------------- -----------
  read_ops                             20
  write_ops                            90

Object: volume
Instance: vol2
Start-time: 05/23/2014 4:00 PM
End-time: 05/23/2014 4:10 PM
Cluster: cluster1
Number of Constituents: 1 (complete_aggregation)
  Counter                             Value
  --------------------------- -----------
  read_ops                             40
  write_ops                            30
```

Importing a performance preset configuration (cluster administrators only)

You can create a custom performance preset or modify a writable performance preset by importing a performance preset configuration in XML file format. You can also use this method to modify what data is collected and stored in performance archives.

Before you begin

- Advanced privilege level commands are required for this task.

- You must have a performance preset configuration in XML file format.
  Technical support can help you create the XML file of performance preset definitions.

About this task

Data ONTAP includes a performance archive that automatically collects and stores performance statistics at predefined times. With the help of technical support, you can modify what data is collected for the performance archive by importing a performance preset.

You cannot modify read-only performance presets. You can only modify performance presets that have the `read-only` parameter set to **`false`**.

Step

1. Import a performance preset configuration:

   `statistics preset import -source-uri` ***`source_URI`*** **`-comment`** ***`comment`***

   #### Example

   In the following example, a performance preset configuration is imported from the NetApp support site:

   ```
   cluster1::*> statistics preset import -source-uri http://
   www.netapp.com/support/
   nfs_monitor.xml -comment "New NFS Monitor preset."
   ```

Viewing performance data for a time period

You can monitor cluster or SVM performance by collecting and viewing data for a specific time period (a sample). You can view data for several objects and instances at a time.

Before you begin

Advanced privilege level commands are required for this task.

About this task

You can collect more than one data sample at a time. You can collect more than one sample from the same object at the same time.

Note: You cannot collect and view data for an object that has more than 5,000 instances. If an object has more than 5,000 instances, you need to specify the specific instances for which you want data. This applies to all `statistics` commands, including `statistics` views.

For more information about the `statistics` commands, see the man pages.

Steps

1. Start collecting data:

   `statistics start -object` ***`object_name`*** **`-counter`** ***`counter_name`*** **`-sample-id`** ***`sample_ID`***

   If you do not specify the `-sample-id` parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. If you run this command again during the same CLI session and do not specify the `-sample-id` parameter, the command can overwrite the previous default sample. You are prompted to confirm whether to overwrite the previous default sample.

2. Optional: Stop collecting data:

   `statistics stop -sample-id sample_ID`

   You can view data from the sample if you do not stop data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify performance trends.

3. Use the `statistics show` command to view the sample data.

Example: Monitoring NFSv3 performance

The following example shows performance data for the NFSv3 protocol.

The following command starts data collection for a new sample:

```
cluster1::*> statistics start -object nfsv3 -sample-id nfs_sample
```

The following command shows data from the sample by specifying counters that show the number of successful read and write requests versus the total number of read and write requests:

```
cluster1::*> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                                 Value
    ---------------------------- ----------------------------
    read_success                                            40042
    read_total                                              40042
    write_success                                         1492052
    write_total                                           1492052
```

Viewing continuously updated performance data

You can monitor cluster or SVM performance by viewing data that continuously updates with the latest status. You can view data for only one object and one instance at a time.

Before you begin

Advanced privilege level commands are required for this task.

About this task

For more information about the `statistics show-periodic` command, see the man page.

Note: The `statistics show-periodic` command is deprecated, but you can still use it to view performance data.

You can also use the `statistics show` command with the `-tab` parameter to display continuously updated data.

Step

1. View continuously updated performance data:

   statistics show-periodic -object *object_name* -instance *object_instance* -counter *counter_name*

   If you do not specify the `-object` parameter, the command returns summary data for the cluster.

Example: Monitoring volume performance

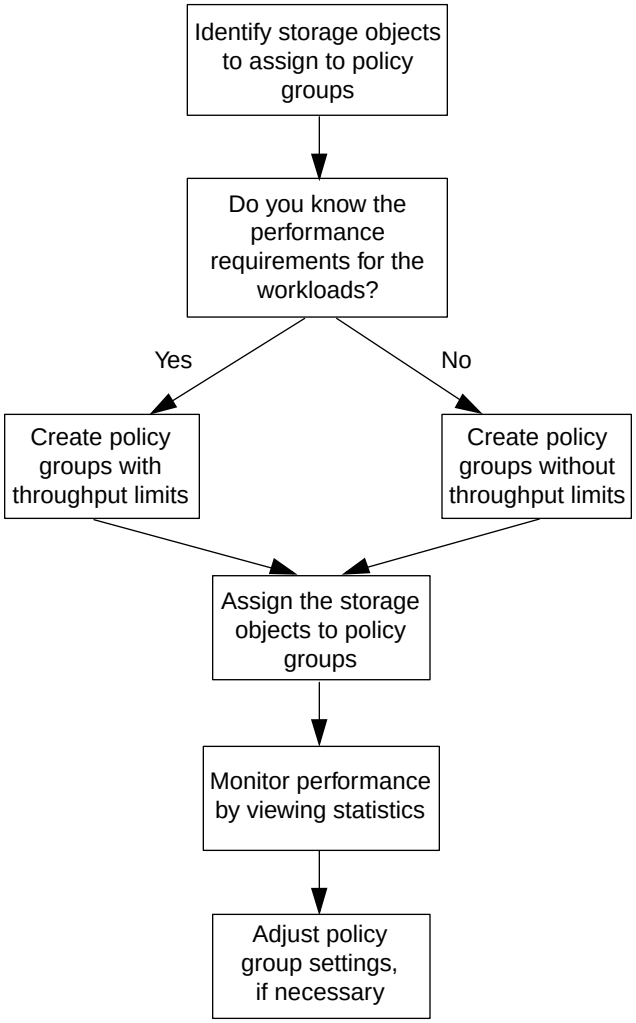
The following examples shows performance data for a volume by the number of operations per second and their latency:

```
cluster1::*> statistics show-periodic -object volume -instance
vol0  -counter write_ops|read_ops|total_ops|read_latency|
write_latency|avg_latency
cluster1: volume.vol0: 1/7/2013 20:15:51
      avg     read             total    write    write
  latency  latency read_ops      ops  latency      ops
 -------- -------- -------- -------- -------- --------
    202us    218us        0       22    303us        7
     97us     43us       31       71    149us       34
     39us      0us        0        3      0us        0
    152us      0us        0       16    152us       16
    162us      0us        0      342    144us      289
    734us      0us        0       15      0us        0
     49us      0us        0        1      0us        0
cluster: volume.vol0: 1/7/2013 20:16:07
      avg     read             total    write    write
  latency  latency read_ops      ops  latency      ops
 -------- -------- -------- -------- -------- --------
Minimums:
     39us      0us        0        1      0us        0
Averages for 7 samples:
    205us     37us        4       67    106us       49
Maximums:
    734us    218us       31      342    303us      289
```

Storage QoS workflow

You can use Storage QoS (Quality of Service) to monitor workload performance and, if necessary, limit throughput for workloads. A workload represents the I/O operations for a volume or LUN, or for all the volumes or LUNs in an SVM.

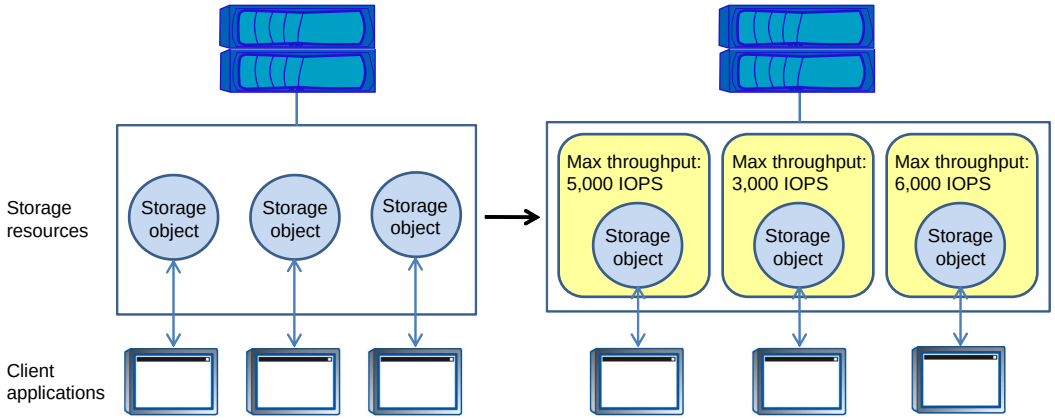
You assign one or more workloads to a *policy group*. You can specify a maximum throughput limit when you create the policy group, or you can wait until after you monitor the workloads to specify a throughput limit.



How Storage QoS works

Storage QoS controls workloads that are assigned to policy groups by throttling and prioritizing client operations (SAN and NAS data requests) and system operations.

The following illustration shows an example environment before and after using Storage QoS. On the left, workloads compete for cluster resources to transmit I/O. These workloads get "best effort" performance, which means you have less performance predictability (for example, a workload might get such good performance that it negatively impacts other workloads). On the right are the same workloads assigned to policy groups that enforce maximum throughput limits.



How the maximum throughput limit works

You can specify one service-level objective for a Storage QoS policy group: a maximum throughput limit. A maximum throughput limit, which you define in terms of IOPS, MBps, or both, specifies the throughput that the workloads in the policy group cannot collectively exceed.

When you specify a maximum throughput for a policy group, Storage QoS controls client operations to ensure that the combined throughput for all workloads in the policy group does not exceed the specified maximum throughput.

For example, assume that you create the policy group “untested_apps” and specify a maximum throughput of 300 MBps. You assign three volumes to the policy group. The combined throughput to those three volumes cannot exceed 300 MBps.

Note: The combined throughput to the workloads in a policy group might exceed the specified limit by up to 10 percent. A deviation might occur if you have a workload that experiences rapid changes in throughput (sometimes called a *bursty workload*).

Note the following about specifying a maximum throughput:

- You must not set the limit too low because you might underutilize the cluster.
- You must consider the minimum amount of throughput that you want to reserve for workloads that do not have limits.

  For example, you can ensure that your critical workloads get the throughput that they need by limiting noncritical workloads.
- You might want to provide room for growth.

  For example, if you see an average utilization of 500 IOPS, you might specify a limit of 1,000 IOPS.

How throttling a workload can affect non-throttled workload requests from the same client

In some situations, throttling a workload (I/O to a storage object) can affect the performance of non-throttled workloads if the I/O requests are sent from the same client.

If a client sends I/O requests to multiple storage objects and some of those storage objects belong to Storage QoS policy groups, performance to the storage objects that do not belong to policy groups might be degraded. Performance is affected because resources on the client, such as buffers and outstanding requests, are shared.

For example, this might affect a configuration that has multiple applications or virtual machines running on the same host.

This behavior is likely to occur if you set a low maximum throughput limit and there are a high number of I/O requests from the client.

If this occurs, you can increase the maximum throughput limit or separate the applications so they do not contend for client resources.

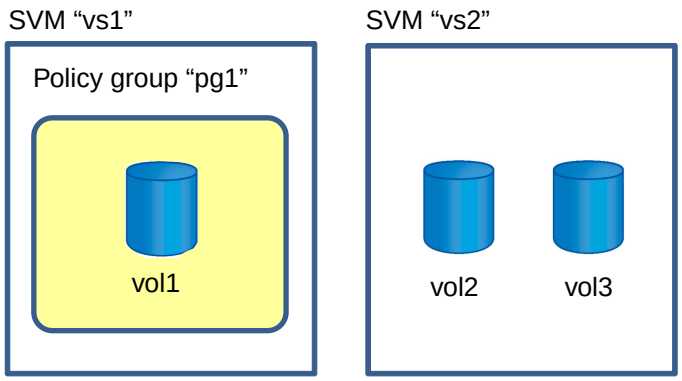
Rules for assigning storage objects to policy groups

You should be aware of rules that dictate how you can assign storage objects to Storage QoS policy groups.

Storage objects and policy groups must belong to the same SVM

A storage object must be contained by the Storage Virtual Machine (SVM) to which the policy group belongs. You specify the SVM to which the policy group belongs when you create the policy group. Multiple policy groups can belong to the same SVM.

In the following illustration, the policy group pg1 belongs to SVM vs1. You cannot assign volumes vol2 or vol3 to policy group pg1 because those volumes are contained by a different SVM.

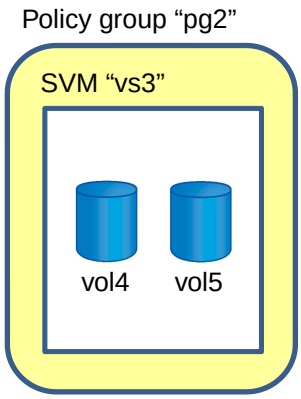


Nested storage objects cannot belong to policy groups

You cannot assign a storage object to a policy group if its containing object or its child objects belong to a policy group. The following table lists the restrictions.

If you assign the...	Then you cannot assign...
Volume to a policy group	The volume's containing SVM or any child LUNs to a policy group
LUN to a policy group	The LUN's containing volume or SVM to a policy group

In the following illustration, the SVM vs3 is assigned to policy group pg2. You cannot assign volumes vol4 or vol5 to a policy group because an object in the storage hierarchy (SVM vs3) is assigned to a policy group.



Some types of volumes not supported with Storage QoS

You can assign FlexVol volumes to policy groups. Infinite Volumes are not supported with Storage QoS.

The following FlexVol volume variations are not supported with Storage QoS:

- Data protection mirrors
- Load-sharing mirrors
- Node root volumes

How to monitor workload performance when using Storage QoS

To determine an appropriate throughput limit, you should monitor performance from the cluster. You should not use a tool on the host to monitor performance. A host can report different results than the cluster.

Storage QoS limits I/O to and from the cluster. The rate of I/O that the cluster experiences can be different from what an application experiences. For example, reads from the application can go to the file system buffer cache and not to the cluster.

Due to this behavior, you should monitor performance from the cluster and not from a host-side tool.

Supported number of Storage QoS policy groups and workloads

You can create up to 12,000 QoS (quality of service) policy groups per cluster and assign up to 12,000 storage objects to those policy groups. Assigning a storage object to a policy group creates a workload.

Controlling and monitoring workload performance

You control and monitor workload performance to address performance problems and to proactively limit workloads that have defined performance targets.

Before you begin

You must be familiar with:

- *How the maximum throughput limit works* on page 34.
- *Rules for assigning storage objects to QoS policy groups* on page 35.

Steps

1. Identify the storage objects that you want to assign to Storage QoS policy groups.

   A best practice is to assign the same type of storage object to all policy groups.

2. Use the `qos policy-group create` command to create a new policy group or use the `qos policy-group modify` command to modify an existing policy group.

   You can specify a maximum throughput limit when you create the policy group or you can wait until after you monitor the workload. Monitoring the workload first can help you identify the limit that you need to set. If you do not specify a maximum throughput, the workloads get best-effort performance.

   #### Example

   The following command creates policy group pg-vs1 with a maximum throughput of 5,000 IOPS.

   ```
   cluster1::> qos policy-group create pg-vs1 -vserver vs1 -max-
   throughput 5000iops
   ```

   #### Example

   The following command creates policy group pg-app2 without a maximum throughput.

   ```
   cluster1::> qos policy-group create pg-app2 -vserver vs2
   ```

3. To assign a storage object to a policy group, use the create or modify command for the SVM, volume, or LUN.

   #### Example

   The following command assigns the SVM vs1 to policy group pg-vs1.

   ```
   cluster1::> vserver modify -vserver vs1 -qos-policy-group pg-vs1
   ```

   #### Example

   The following command creates the volume app2 and assigns it to policy group pg-app2.

   ```
   cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr2 -
   qos-policy-group pg-app2
   ```

4. To identify whether you are meeting your performance objectives, use the `qos statistics` commands to monitor policy group and workload performance.

   You should monitor performance from the cluster. You should not use a tool on the host to monitor performance.

   #### Example

   The following command shows the performance of policy groups.

   ```
   cluster1::> qos statistics performance show
   Policy Group          IOPS      Throughput   Latency
   -------------------- -------- --------------- ----------
   -total-                12316       47.76MB/s  1264.00us
   pg_app2                 7216       28.19MB/s   420.00us
   pg_vs1                  5008       19.56MB/s     2.45ms
   _System-Best-Effort       62       13.36KB/s     4.13ms
   _System-Background        30           0KB/s        0ms
   ```

Example

The following command shows the performance of workloads.

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

5. If necessary, use the `qos policy-group modify` command to adjust the policy group's maximum throughput limit.

Example

The following command modifies the maximum throughput for policy group pg-app2 to 20 MB/s.

```
cluster1::> qos policy-group modify pg-app2 -max-throughput 20mb/s
```

Identifying remaining performance capacity

Knowing the available performance capacity in the cluster helps you provision workflows and balance them. Performance capacity is how much work you can place on a node or an aggregate before performance of all workloads begins to be affected by latency.

About this task

You can also complete this task using OnCommand tools to obtain the remaining performance capacity.

Steps

1. Change to advanced privilege level:

   `set -privilege advanced`

2. Start the statistics command line prompt:

   `statistics start –object resource_headroom_`*`cpu`*

3. Display real-time headroom information:

   `statistics show -object resource_headroom`

4. Return to administrative privilege:

   `set -privilege admin`

Sample Output

```
sti2520-2131454963690::*> stat show -obj resource_headroom_cpu -raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                    -
                                 ops                            4376
```

```
                            latency                              37719
                        utilization                                 86
                 optimal_point_ops                                2573
              optimal_point_latency                               3589
          optimal_point_utilization                                 72
     optimal_point_confidence_factor                                 1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    ------------------------------ --------------------------------
    ewma_hourly                                                     -
                               ops                                  0
                           latency                                  0
                       utilization                                  0
                 optimal_point_ops                                  0
              optimal_point_latency                                 0
          optimal_point_utilization                                71
     optimal_point_confidence_factor                                 1
2 entries were displayed.
```

You compute the available performance capacity by subtracting the `optimal_point_counter` from the `current_counter`. In this example, the utilization capacity for `CPU_sti2520-213` is -14% (72%-86%). This suggests that the node's CPU has been overutilized on average for the past one hour.

Additionally, you could have specified `ewma_daily`, `ewma_weekly`, or `ewma_monthly` to get the same information, but averaged over a longer period of time.

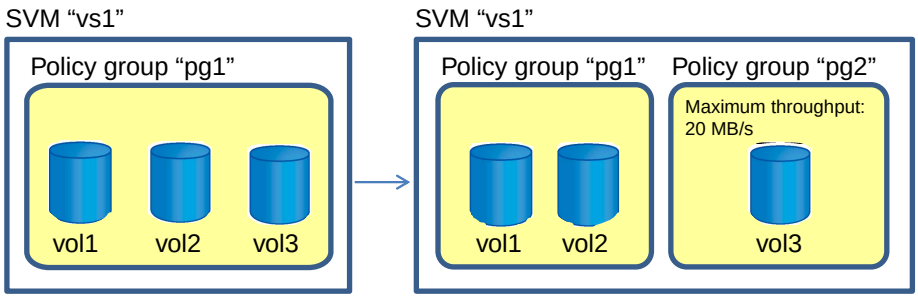
Note: The `resource_headroom_cpu` Counter Manager (CM) object in this example represents the entire node (all CPUs collectively). You can get the available performance capacity on aggregates using the same `stat` command syntax but with the `resource_headroom_aggr` CM object.

```
sti2520-2131454963690:::*> statistics show -object resource_headroom_aggr -counter
ewma_weekly -raw

Object: resource_headroom_aggr
Instance: DISK_HDD_aggr1_2acca201-3b24-4b9e-abcc-39e624461822
Start-time: 2/26/2016 14:33:46
End-time: 2/26/2016 14:33:46
Scope: qos-3270-2

    Counter                                                     Value
    ------------------------------ --------------------------------
    ewma_weekly                                                     -
                               ops                                303
                 optimal_point_ops                                794
                           latency                              16121
              optimal_point_latency                             19123
                       utilization                                 36
          optimal_point_utilization                                85
     optimal_point_confidence_factor                                 3
1 entries were displayed.
```

Example: Isolating a workload

You might have a workload that gets better performance than necessary, which affects the performance of other workloads. To address this problem, you use Storage QoS to throttle the workload, which frees cluster resources for other workloads. In this example, the workloads are at the volume level.

The following illustration shows three volumes. You place each volume in policy group pg1, but you do not set a maximum throughput because you want to monitor the workloads first. When you monitor the workloads, you find that vol3 is getting better performance than other workloads. To limit the workload's resource consumption, you move vol3 to policy group pg2. This should allow the other workloads to speed up.



Using the CLI to isolate a workload

The following command creates a policy group without a maximum throughput.

```
cluster1::> qos policy-group create pg1 -vserver vs1
```

The following command assigns three existing volumes to the policy group.

```
cluster1::> volume modify vol1,vol2,vol3 -vserver vs1 -qos-policy-
group pg1
```

The following command displays performance data for the workloads.

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    16645        64.77MB/s   411.00us
vol3-wid12459    12459    10063        39.31MB/s   410.00us
vol2-wid1445      1445     3505        13.69MB/s   437.00us
vol1-wid11344    11344     3007        11.75MB/s   277.00us
_USERSPACE_APPS     14       40        26.40KB/s     8.68ms
_Scan_Backgro..   5688       30            0KB/s        0ms
```

The vol3 workload is getting such good performance that other workloads cannot meet your performance objectives. You decide to move that workload to a new policy group that has a maximum throughput.

The following command creates a policy group with a maximum throughput.

```
cluster1::> qos policy-group create pg2 -vserver vs1 -max-
throughput 20mb/s
```

The following command assigns vol3 to the new policy group.

```
cluster1::> volume modify vol3 -vserver vs1 -qos-policy-group pg2
```

Displaying performance data for the workloads shows that limiting vol3 has allowed the other workloads to get better performance.

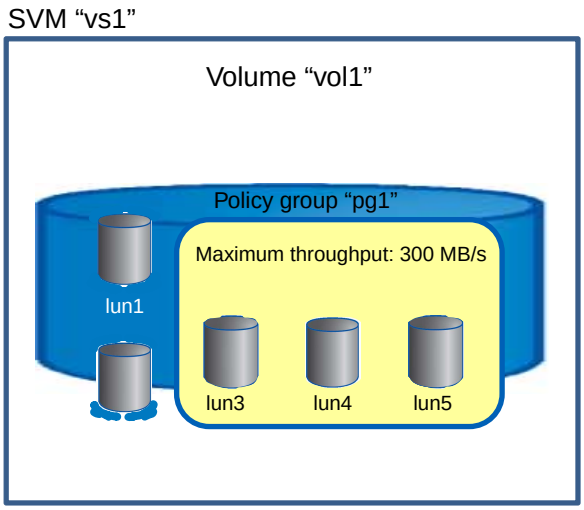
```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    15691        61.17MB/s  1001.00us
vol1-wid11344    11344     6016        23.50MB/s   355.00us
```

```
vol3-wid12459    12459      5133         20.05MB/s     2.42ms
vol2-wid1445      1445      4462         17.43MB/s   253.00us
_USERSPACE_APPS     14        50        204.20KB/s   355.00us
_Scan_Backgro..   5688        30             0KB/s        0ms
```

Example: Proactively setting a limit on non-critical workloads

You might want to ensure that your critical workloads get the best performance possible, so you use Storage QoS to limit the throughput to non-critical workloads. In this example, the workloads are at the LUN level.

The following illustration shows five LUNs in volume vol1. lun1 and lun2 are used for critical applications. lun3, lun4, and lun5 are used for non-critical applications. You want lun1 and lun2 to get best effort performance, so you limit lun3, lun4, and lun5 by assigning them to a policy group with a maximum throughput limit.



Using the CLI to set a limit on non-critical workloads

The following command creates a policy group with a maximum throughput of 300 MB/s.

```
cluster1::> qos policy-group create pg1 -vserver vs1 -max-
throughput 300mb/s
```

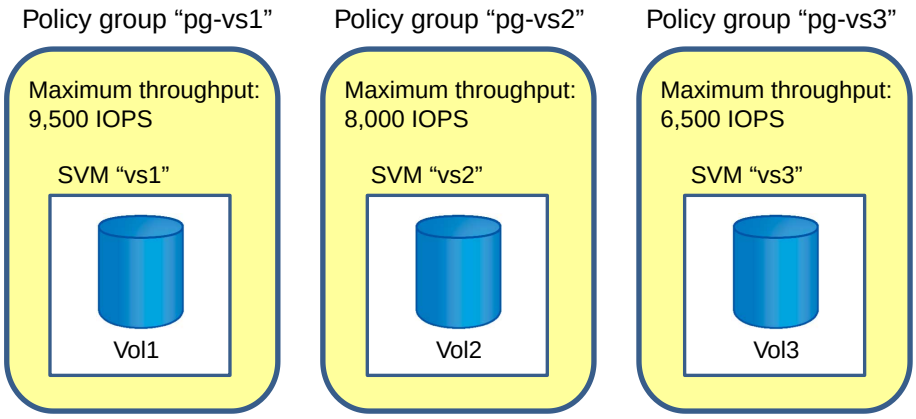
The following commands assign three new LUNs to the policy group.

```
cluster1::> lun create -vserver vs1 -volume vol1 -lun lun3 -size
50GB -ostype windows_2008 -qos-policy-group pg1
cluster1::> lun create -vserver vs1 -volume vol1 -lun lun4 -size
50GB -ostype windows_2008 -qos-policy-group pg1
cluster1::> lun create -vserver vs1 -volume vol1 -lun lun5 -size
50GB -ostype windows_2008 -qos-policy-group pg1
```

Example: Proactively setting a limit on workloads in a shared storage infrastructure

If you have a shared storage infrastructure, you might need to ensure that each workload does not get better performance than necessary. In this example, you use Storage QoS policy groups to set a limit on each workload, all of which are at the Storage Virtual Machine (SVM) level.

The following illustration shows three SVMs assigned to three separate policy groups. You assign each SVM to a policy group because you know the performance objectives for each workload and you do not want one tenant taking system resources from other tenants.



Using the CLI to set a limit on workloads in a shared storage infrastructure

The following commands create three policy groups with maximum throughput limits.

```
cluster1::> qos policy-group create pg-vs1 -vserver vs1 -max-
throughput 9500iops
cluster1::> qos policy-group create pg-vs2 -vserver vs2 -max-
throughput 8000iops
cluster1::> qos policy-group create pg-vs3 -vserver vs3 -max-
throughput 6500iops
```

The following commands assign three existing SVMs to the policy groups.

```
cluster1::> vserver modify -vserver vs1 -qos-policy-group pg-vs1
cluster1::> vserver modify -vserver vs2 -qos-policy-group pg-vs2
cluster1::> vserver modify -vserver vs3 -qos-policy-group pg-vs3
```

Commands for controlling and monitoring workloads

You can use commands to manage Storage QoS policy groups, assign storage objects to policy groups, identify the storage objects that belong to policy groups, and monitor workload, volume performance, and policy group performance.

- *Commands for managing policy groups* on page 43
- *Commands for assigning storage objects to policy groups* on page 43
- *Commands for identifying the storage objects that belong to policy groups* on page 43

- *Commands for monitoring policy group performance* on page 44
- *Commands for monitoring workload performance* on page 44
- *Commands for advanced monitoring of volume performance* on page 44

For more information about these commands, see the man pages.

Commands for managing policy groups

You use the `qos policy-group` commands to manage policy groups. You use policy groups to control and monitor workload performance.

If you want to...	Use this command...
Create a policy group	`qos policy-group create`
Modify a policy group	`qos policy-group modify`
Rename a policy group	`qos policy-group rename`
View all user-defined policy groups	`qos policy-group show`
Delete a policy group	`qos policy-group delete`

Commands for assigning storage objects to policy groups

You use a storage object's `create` command or `modify` command to assign a storage object to a policy group. You assign a storage object to a policy group to control and monitor workload performance.

Note: To remove a storage object from a policy group, you set the `-qos-policy-group` parameter to **none**.

If you want to assign the..	Use this command with the `-qos-policy-group` parameter...
SVM with FlexVol volumes to a policy group	`vserver modify`
New FlexVol volume to a policy group	`volume create`
Existing FlexVol volume to a policy group	`volume modify`
New FlexClone volume to a policy group	`volume clone create`
New LUN to a policy group	`lun create`
Existing LUN to a policy group	`lun modify`
File to a policy group	`volume file modify`
New clone of a file or LUN to a policy group	`volume file clone create`

Commands for identifying the storage objects that belong to policy groups

You use a storage object's `show` command to identify the storage objects that belong to policy groups.

If you want to identify the...	Use this command with the `-qos-policy-group` parameter...
SVMs with FlexVol volumes that belong to a policy group	`vserver show`
FlexVol volumes that belong to a policy group	`volume show`

If you want to identify the...	Use this command with the `-qos-policy-group` parameter...
LUNs that belong to a policy group	`lun show`

Commands for monitoring policy group and workload performance

You use the following commands to monitor policy group and workload performance in terms of IOPS, throughput, and latency.

If you want to view the...	Use this command...
Collective performance of all workloads in a policy group	`qos statistics performance show`
Performance of individual workloads	`qos statistics workload performance show`

Commands for advanced monitoring of policy group performance

You use the following commands to view advanced performance data for policy groups. These commands show the collective performance of all workloads in a policy group.

If you want to view data about...	Use this command...
The client load as it enters the cluster, in terms of request size, read percentage, and concurrency	`qos statistics characteristics show`
Latency across Data ONTAP subsystems, which helps to determine why response time is slow	`qos statistics latency show`
CPU utilization	`qos statistics resource cpu show`
Disk utilization, in terms of the percentage of time spent on the disk during read and write operations	`qos statistics resource disk show`

Commands for advanced monitoring of workload performance

You use the following commands to view advanced performance data for individual workloads.

If you want to view data about...	Use this command...
The client load as it enters the cluster, in terms of request size, read percentage, and concurrency	`qos statistics workload characteristics show`
Latency across Data ONTAP subsystems, which helps to determine why response time is slow	`qos statistics workload latency show`
CPU utilization	`qos statistics workload resource cpu show`
Disk utilization, in terms of the percentage of time spent on the disk during read and write operations	`qos statistics workload resource disk show`

Commands for advanced monitoring of volume performance

You use the following commands to view advanced performance data for individual volume.

If you want to view data about...	Use this command...
The load on volume, in terms of request size, read percentage, and concurrency	`qos statistics volume characteristics show`
Latency breakdown for the in volume, which helps to determine why response time is slow	`qos statistics volume latency show`
Total read/write operations, throughput and latency of a volume	`qos statistics volume performance show`
CPU utilization across all the domains	`qos statistics volume resource cpu show`
Number of disks or disk utilization in terms of the percentage of time spent on the disk during read and write operations	`qos statistics volume resource disk show`

Histogram-based predictions in RAVE

Starting in Data ONTAP 8.2.1, the speculative read-ahead engine (RAVE) in WAFL can capture additional temporal data about previous user read requests to a file and use this information to intelligently speculate on future read requests. In prior releases, speculation was based only on information from the current user I/O.

For clustered systems, you can enable histogram-based predictions as part of the QoS read-ahead settings, and then attach them to a QoS workload. The `qos settings read-ahead create | modify` *`read_ahead_setting_name`* `-use-histogram` **`true`** | **`false`** command enables or disables the functionality. The `qos workload modify -read-ahead` *`read_ahead_setting_name`* `-workload` *`workload_name`* command attaches the read-ahead setting to any workload.

Where to find additional information

After you have successfully installed and configured Unified Manager and Performance Manager and set up monitoring tasks, you can perform more advanced tasks.

- *OnCommand Unified Manager 7.0 Installation and Setup Guide for VMware Virtual Appliances*
  Provides instructions for installing the Unified Manager appliance on a VMware ESXi server.
- *OnCommand Unified Manager 7.0 Administration Guide*
  Provides information about performing Unified Manager tasks and troubleshooting.
- *OnCommand Performance Manager 7.1 Installation and Administration Guide for VMware Virtual Appliances*
  Provides instructions for installing the Performance Manager appliance on a VMware ESXi server.
- *OnCommand Performance Manager 7.1 User Guide*
  Explains how to use Performance Manager.
- *System administration*
  Describes general system administration for storage systems running clustered Data ONTAP.
- *NetApp Technical Report 4211: NetApp Storage Performance Primer for Clustered Data ONTAP 8.3*
  Describes the basic performance concepts in clustered Data ONTAP, how different processes can impact performance, and how to observe cluster performance.
- *NetApp Technical Report 4448: OnCommand Performance Manager Best Practices (OnCommand Performance Manager Version 2.0)*
  Describes some best practices when using Performance Manager to manage storage systems running clustered Data ONTAP.

Copyright information

Trademark information

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

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

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

You can also contact us in the following ways:

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

Index

I

L

M

N

O

P

R

S

T

U

V

W