Contents

Deciding whether to use this guide ............................................................. 4

Performance monitoring workflow .......................................................... 5
  Verifying that your VMware environment is supported ............................. 6
  Active IQ Unified Manager worksheet ...................................................... 6
  Installing Active IQ Unified Manager ....................................................... 8
    Downloading and deploying Active IQ Unified Manager ...................... 8
    Configuring initial Active IQ Unified Manager settings ...................... 8
  Specifying the clusters to be monitored ............................................... 9
  Setting up basic monitoring tasks ......................................................... 10
    Performing daily monitoring ............................................................. 10
    Using weekly and monthly performance trends to identify performance
      issues ............................................................................................... 10
    Using performance thresholds to generate event notifications .......... 11
  Identifying performance issues in Active IQ Unified Manager .............. 13

Performance management workflow ...................................................... 15
  Performing basic infrastructure checks ................................................. 15
    Checking protocol settings on the storage system ............................... 16
    Checking the network settings on the data switches ............................. 18
    Checking the MTU network setting on the storage system ................. 18
    Checking disk throughput and latency ............................................ 19
    Checking throughput and latency between nodes ............................. 19
  Managing workloads ............................................................................. 21
    Identifying remaining performance capacity ..................................... 21
    Identifying high-traffic clients or files ......................................... 22
    Guaranteeing throughput with QoS ................................................... 23

Where to find additional information ...................................................... 35

Copyright .................................................................................................. 36

Trademark ............................................................................................. 37

How to send comments about documentation and receive update
  notifications ........................................................................................... 38
Deciding whether to use the Performance Management Power Guide

This guide describes 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, monitor cluster performance, and perform root-cause analysis by using Active IQ Unified Manager (formerly OnCommand Unified Manager), in addition to the ONTAP command-line interface.
• You are using the ONTAP command-line interface to configure storage quality of service (QoS). QoS is also available in System Manager, NSLM, WFA, VSC (VMware Plug-in), and APIs.
• You want to install Unified Manager by using a virtual appliance, instead of a Linux or Windows-based installation.
• You're willing to use a static configuration rather than DHCP to install the software.
• You can access ONTAP commands at the advanced privilege level.
• You are a cluster administrator with the “admin” role.

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

• Active IQ Unified Manager 9.6 Installation Guide
• System administration
• Performance monitoring express setup
Monitoring cluster performance involves installing Active IQ Unified Manager software, setting up basic monitoring tasks, and identifying performance issues.

**Steps**

1. **Verifying that your VMware environment is supported** on page 6
   For successful installation of Active IQ Unified Manager, you must verify that your VMware environment meets the necessary requirements.

2. **Active IQ Unified Manager worksheet** on page 6
   Before you install, configure, and connect Active IQ Unified Manager, you should have specific information about your environment readily available. You can record the information in the worksheet.

3. **Installing Active IQ Unified Manager** on page 8
   To install Active IQ Unified Manager to monitor cluster performance, follow these procedures.

4. **Specifying the clusters to be monitored** on page 9
   You must add a cluster to an Active IQ Unified Manager server to monitor the cluster, view the cluster discovery status, and monitor its performance.

5. **Setting up basic monitoring tasks** on page 10
You can monitor your systems for performance issues by checking the systems daily, by establishing weekly and monthly performance trends, and by specifying thresholds for receipt of notifications about potential performance issues.

6. Identifying performance issues in Active IQ Unified Manager on page 13
   If a performance event occurs, you can locate the source of the issue within Active IQ Unified Manager and use other tools to fix it. You might receive an email notification of an event or notice the event during daily monitoring.

Verifying that your VMware environment is supported

For successful installation of Active IQ Unified 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 Unified 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 Unified Manager.

   mysupport.netapp.com/matrix

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.

Active IQ Unified Manager worksheet

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

Unified Manager installation information

<table>
<thead>
<tr>
<th>Virtual machine on which software is deployed</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi server IP address</td>
<td></td>
</tr>
</tbody>
</table>
## Virtual machine on which software is deployed

<table>
<thead>
<tr>
<th>Setting</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host fully qualified domain name</td>
<td></td>
</tr>
<tr>
<td>Host IP address</td>
<td></td>
</tr>
<tr>
<td>Network mask</td>
<td></td>
</tr>
<tr>
<td>Gateway IP address</td>
<td></td>
</tr>
<tr>
<td>Primary DNS address</td>
<td></td>
</tr>
<tr>
<td>Secondary DNS address</td>
<td></td>
</tr>
<tr>
<td>Search domains</td>
<td></td>
</tr>
<tr>
<td>Maintenance user name</td>
<td></td>
</tr>
<tr>
<td>Maintenance user password</td>
<td></td>
</tr>
</tbody>
</table>

## Unified Manager configuration information

<table>
<thead>
<tr>
<th>Setting</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance user email address</td>
<td></td>
</tr>
<tr>
<td>NTP server</td>
<td></td>
</tr>
<tr>
<td>SMTP server host name or IP address</td>
<td></td>
</tr>
<tr>
<td>SMTP user name</td>
<td></td>
</tr>
<tr>
<td>SMTP password</td>
<td></td>
</tr>
<tr>
<td>SMTP default port</td>
<td>25 (Default value)</td>
</tr>
<tr>
<td>Email from which alert notifications are sent</td>
<td></td>
</tr>
<tr>
<td>LDAP bind distinguished name</td>
<td></td>
</tr>
<tr>
<td>LDAP bind password</td>
<td></td>
</tr>
<tr>
<td>Active Directory administrator name</td>
<td></td>
</tr>
<tr>
<td>Active Directory password</td>
<td></td>
</tr>
<tr>
<td>Authentication server base distinguished name</td>
<td></td>
</tr>
<tr>
<td>Authentication server host name or IP address</td>
<td></td>
</tr>
</tbody>
</table>

## Cluster information

Capture the following information for each cluster on Unified Manager.

<table>
<thead>
<tr>
<th>Cluster 1 of N</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name or cluster-management IP address</td>
<td></td>
</tr>
<tr>
<td>ONTAP administrator user name</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong>: The administrator must have been assigned the “admin” role.</td>
<td></td>
</tr>
<tr>
<td>ONTAP administrator password</td>
<td></td>
</tr>
<tr>
<td>Protocol (HTTP or HTTPS)</td>
<td></td>
</tr>
</tbody>
</table>
Installing Active IQ Unified Manager

To install Active IQ Unified Manager to monitor cluster performance, follow these procedures.

**Downloading and deploying Active IQ 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 Active IQ Unified Manager.
   

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 Active IQ Unified Manager settings**

The Active IQ 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. Accept the default AutoSupport enabled setting.

2. Enter the NTP server details, the maintenance user email address, the SMTP server host name, and additional SMTP options, and then click Save.

**After you finish**

When the initial setup is complete, the Cluster Data Sources page is displayed where you can add the cluster details.
Specifying the clusters to be monitored

You must add a cluster to an Active IQ Unified Manager server to monitor the cluster, view the cluster discovery status, and monitor its performance.

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 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 Configuration > Cluster Data Sources.
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. Review the cluster discovery status from the Configuration/Cluster Data Sources page.

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

Setting up basic monitoring tasks

You can monitor your systems for performance issues by checking the systems daily, by establishing weekly and monthly performance trends, and by specifying thresholds for receipt of notifications about potential 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 Active IQ Unified Manager UI, go to the Event Inventory page to view all current and obsolete events.
2. From the View option, select Active Performance 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 that you suspect is being underused or overused.
2. On the Volume Details tab, click 30 d to display the historical data.
3. In the “Break down data by” drop-down menu, select Latency, and then click Submit.
4. Deselect Aggregate in the cluster components comparison chart, and then compare the cluster latency with the volume latency chart.
5. Select Aggregate and deselect all other components in the cluster components comparison chart, and then compare the aggregate latency with the volume latency chart.
6. Compare the reads/writes latency chart to the volume latency chart.
7. Determine whether client application loads have caused a workload contention and rebalance workloads as needed.
8. Determine whether the aggregate is overused and causing contention and rebalance workloads as needed.
Using performance thresholds to generate event notifications

Events are notifications that the Active IQ Unified Manager generates automatically when a predefined condition occurs, or when a performance counter value crosses a threshold. Events help you identify performance issues in the clusters you are monitoring. You can configure alerts to send email notification automatically when events of certain severity types occur.

Setting performance thresholds

You can set performance thresholds to monitor critical performance issues. User-defined thresholds trigger a warning or a critical event notification when the system approaches or exceeds the defined threshold.

Steps

1. Create the Warning and Critical event thresholds:
   a. Select Configuration > Performance Thresholds.
   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 then 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 and choose the Performance from the View option.
   b. Select the object to which you want to assign the threshold policy, and then click Assign Threshold Policy.
   c. Select the policy you previously created, and then click Assign Policy.

Example

You can set user-defined thresholds to learn about critical performance issues. For example, if you have a Microsoft Exchange Server and you know that it crashes if volume latency exceeds 20 milliseconds, you can set a warning threshold at 12 milliseconds and a critical threshold at 15 milliseconds. With this threshold setting, you can receive notifications when the volume latency exceeds the limit.
Adding alerts

You can configure alerts to notify you when a particular event is generated. You can configure alerts for a single resource, for a group of resources, or for events of a particular severity type. You can specify the frequency with which you want to be notified and associate a script to the alert.

Before you begin

- You must have configured notification settings such as the user email address, SMTP server, and SNMP trap host to enable the Active IQ Unified Manager server to use these settings to send notifications to users when an event is generated.
- You must know the resources and events for which you want to trigger the alert, and the user names or email addresses of the users that you want to notify.
- If you want to have a script execute based on the event, you must have added the script to Unified Manager by using the Management/Scripts page.
- You must have the Administrator or Storage Administrator role.

About this task

You can create an alert directly from the Event details page after receiving an event in addition to creating an alert from the Configuration/Alerting page, as described here.

Steps

1. In the left navigation pane, click Configuration > Alerting.
2. In the Configuration/Alerting page, click Add.
3. In the Add Alert dialog box, click Name, and enter a name and description for the alert.
4. Click Resources, and select the resources to be included in or excluded from the alert.
   You can set a filter by specifying a text string in the Name contains field to select a group of resources. Based on the text string that you specify, the list of available resources displays only those resources that match the filter rule. The text string that you specify is case-sensitive.
   If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule, and the alert is not generated for events related to the excluded resource.
5. Click Events, and select the events based on the event name or event severity type for which you want to trigger an alert.
   Tip: To select more than one event, press the Ctrl key while you make your selections.
6. Click Actions, and select the users that you want to notify, choose the notification frequency, choose whether an SNMP trap will be sent to the trap receiver, and assign a script to be executed when an alert is generated.
   Note: If you modify the email address that is specified for the user and reopen the alert for editing, the Name field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you modified the email address of the selected user from the Management/Users page, the modified email address is not updated for the selected user.
   You can also choose to notify users through SNMP traps.
7. Click Save.
Example of adding an alert

This example shows how to create an alert that meets the following requirements:

• Alert name: HealthTest
• Resources: includes all volumes whose name contains “abc” and excludes all volumes whose name contains “xyz”
• Events: includes all critical health events
• Actions: includes “sample@domain.com”, a “Test” script, and the user has to be notified every 15 minutes

Perform the following steps in the Add Alert dialog box:

1. Click **Name**, and enter **HealthTest** in the **Alert Name** field.
2. Click **Resources**, and in the Include tab, select **Volumes** from the drop-down list.
   a. Enter **abc** in the **Name contains** field to display the volumes whose name contains “abc”.
   b. Select **<<All Volumes whose name contains 'abc'>>** from the Available Resources area, and move it to the Selected Resources area.
   c. Click **Exclude**, and enter **xyz** in the **Name contains** field, and then click **Add**.
3. Click **Events**, and select **Critical** from the Event Severity field.
4. Select **All Critical Events** from the Matching Events area, and move it to the Selected Events area.
5. Click **Actions**, and enter **sample@domain.com** in the Alert these users field.
6. Select **Remind every 15 minutes** to notify the user every 15 minutes.
   You can configure an alert to repeatedly send notifications to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.
7. In the Select Script to Execute menu, select **Test** script.
8. Click **Save**.

Identifying performance issues in Active IQ Unified Manager

If a performance event occurs, you can locate the source of the issue within Active IQ Unified Manager and use other tools to fix it. You might receive an email notification of an event or notice the event during daily monitoring.

Steps

1. Click the link in the email notification, which takes you directly to the storage object having a performance event.

<table>
<thead>
<tr>
<th>If you...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive an email notification of an event</td>
<td>Click the link to go directly to the event details page.</td>
</tr>
<tr>
<td>If you...</td>
<td>Then...</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>Notice the event while analyzing the Event Inventory page</td>
<td>Select the event to go directly to the event details page.</td>
</tr>
</tbody>
</table>

2. If the event has crossed a system-defined threshold, follow the suggested actions in the UI to troubleshoot the issue.

3. If the event has crossed a user-defined threshold, analyze the event to determine if you need to take action.

4. If the issue persists, check the following settings:
   - Protocol settings on the storage system
   - Network settings on any Ethernet or fabric switches
   - Network settings on the storage system
   - Disk layout and aggregate metrics on the storage system

5. If the issue persists, contact technical support for assistance.
Performance management workflow

Once you have identified a performance issue, you can conduct some basic diagnostic checks of your infrastructure to rule out obvious configuration errors. If those don’t pinpoint the problem, you can start looking at workload management issues.

Performing basic infrastructure checks

Some basic diagnostic checks of your infrastructure will help you rule out obvious sources of performance problems. You should review protocol and network settings and check disc throughput and latency. If you are replicating data, you will want to monitor throughput and latency between nodes.
**Choices**

- Checking protocol settings on the storage system on page 16
- Checking the network settings on the data switches on page 18
- Checking the MTU network setting on the storage system on page 18
- Checking disk throughput and latency on page 19
- Checking throughput and latency between nodes on page 19

**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 maximum transfer size**

For NFS, you can check whether the TCP maximum transfer size for reads and writes might be causing a performance issue. If you think the size is slowing performance, you can increase it.

**Before you begin**

- You must have cluster administrator privileges to perform this task.
- You must use advanced privilege level commands for this task.

**Steps**

1. Change to the advanced privilege level:
   ```
   set -privilege advanced
   ```
2. Check the TCP maximum transfer size:
   ```
   vserver nfs show -vserver vserver_name -instance
   ```
3. If the TCP maximum transfer size is too small, increase the size:
   ```
   vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
   ```
4. Return to the administrative privilege level:
   ```
   set -privilege admin
   ```

**Example**

The following example changes the TCP maximum transfer size of SVM1 to 1048576:

```bash
cluster1:*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

**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.

**Before you begin**

Advanced privilege level commands are required for this task.

**Steps**

1. Change to advanced privilege level:
set -privilege advanced

2. Check the TCP window size setting:
   
   vserver iscsi show -vserver vserver_name -instance

3. Modify the TCP window size setting:
   
   vserver iscsi modify -vserver vserver_name -tcp-window-size integer

4. Return to administrative privilege:
   
   set -privilege admin

Example

The following example changes the TCP window size of **SVM1** to 131,400 bytes:

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

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 setting on the storage system:
   `network port show -instance`

2. Change the MTU port setting to 9000:
   `network port modify -node nodename -port port -mtu 9000`

Example

The following example changes the MTU port setting for e0a to 9000:
```
cluster1::*> network port modify -node node0 -port e0a -mtu 9000
```
Checking disk throughput and latency

You can check the disk throughput and latency metrics for cluster nodes to assist you in troubleshooting.

About this task
Advanced privilege level commands are required for this task.

Steps
1. Change to advanced privilege level:
   `set -privilege advanced`
2. 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 *Latency
Disk       Node  (%)  Ops  Ops  Read Write  (Bps)    (Bps)   (us)
------------ ----   ---- ----- ----- ------   -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----    -----   -----
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:

<table>
<thead>
<tr>
<th>Session Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>SnapMirror replication between nodes in different clusters</td>
</tr>
<tr>
<td>AsyncMirrorLocal</td>
<td>SnapMirror replication between nodes in the same cluster</td>
</tr>
<tr>
<td>AsyncMirrorRemote</td>
<td>SnapMirror replication between nodes in different clusters</td>
</tr>
<tr>
<td>SyncMirrorRemote</td>
<td>SyncMirror replication between nodes in different clusters</td>
</tr>
<tr>
<td>RemoteDataTransfer</td>
<td>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)</td>
</tr>
</tbody>
</table>

Steps
1. Change to advanced privilege level:
   ```bash
   set -privilege advanced
   ```
2. Measure throughput and latency between nodes:
   ```bash
   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 throughput and latency for SnapMirror-type replication operations between node1 on the local cluster and node3 on cluster2:

```bash
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:
   ```bash
   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.
Managing workloads

ONTAP offers a powerful set of tools for managing workloads. In addition to the numerous ways you can shift workloads to other resources (adding controllers, moving volumes or LUNs, scaling up to flash media, and so on), you can use storage quality of service (QoS) to guarantee that performance of critical workloads is not compromised by competing workloads.

Choices

• Identifying remaining performance capacity on page 21
• Identifying high-traffic clients or files on page 22
• Guaranteeing throughput with QoS on page 23

Identifying remaining performance capacity

Performance capacity, or headroom, measures how much work you can place on a node or an aggregate before performance of workloads on the resource begins to be affected by latency. Knowing the available performance capacity on the cluster helps you provision and balance workloads.

Before you begin

Advanced privilege level commands are required for this task.

About this task

You can use the following values for the -object option to collect and display headroom statistics:

• For CPUs, resource_headroom_cpu.
• For aggregates, resource_headroom_aggr.

You can also complete this task using ONTAP System Manager and Active IQ Unified Manager.

Steps

1. Change to advanced privilege level:
   ```
   set -privilege advanced
   ```
2. Start real-time headroom statistics collection:
   ```
   statistics start -object resource_headroom_cpu|aggr
   ```
   For complete command syntax, see the man page.
3. Display real-time headroom statistics information:
   ```
   statistics show -object resource_headroom_cpu|aggr
   ```
   For complete command syntax, see the man page.
4. Return to administrative privilege:
   ```
   set -privilege admin
   ```

Example

The following example displays the average hourly headroom statistics for cluster nodes.

You can compute the available performance capacity for a node by subtracting the current_utilization counter from the optimal_point_utilization counter. In this
example, the utilization capacity for CPU_sti2520-213 is -14% (72%-86%), which suggests that the CPU has been overutilized on average for the past hour.

You could have specified ewma_daily, ewma_weekly, or ewma_monthly to get the same information averaged over longer periods of time.

```bash
sti2520-213::> statistics show -object 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                                                     -
current_ops                             4376
current_latency                            37719
current_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                                                     -
current_ops                                0
current_latency                                0
current_utilization                                0
optimal_point_ops                                0
optimal_point_latency                                0
optimal_point_utilization                               71
optimal_point_confidence_factor                                1

2 entries were displayed.
```

### Identifying high-traffic clients or files

You can use ONTAP Active Objects technology to identify clients or files that are responsible for a disproportionately large amount of cluster traffic. Once you have identified these “top” clients or files, you can rebalance cluster workloads or take other steps to resolve the issue.

**Before you begin**

You must be a cluster administrator to perform this task.

**Steps**

1. View the top clients accessing the cluster:

   ```bash
   statistics top client show -node node_name -sort-key sort_column -interval seconds_between_updates -iterations iterations -max number_of_instances
   
   For complete command syntax, see the man page.
   
   **Example**
   
   The following command displays the top clients accessing cluster1:
   ```
   ```
2. View the top files accessed on the cluster:

   statistics top file show -node node_name -sort-key sort_column -interval seconds_between_updates -iterations iterations -max number_of_instances

   For complete command syntax, see the man page.

   Example

   The following command displays the top files accessed on cluster1:

   cluster1::> statistics top file show

   cluster1 : 3/23/2016 17:59:10

<table>
<thead>
<tr>
<th>File</th>
<th>Volume</th>
<th>Vserver</th>
<th>Node</th>
<th>Ops</th>
</tr>
</thead>
<tbody>
<tr>
<td>/vol/vol1/vm170-read.dat</td>
<td>vol1</td>
<td>vs4</td>
<td>siderop1-vsim4</td>
<td>22</td>
</tr>
<tr>
<td>/vol/vol1/vm69-write.dat</td>
<td>vol1</td>
<td>vs3</td>
<td>siderop1-vsim3</td>
<td>6</td>
</tr>
<tr>
<td>/vol/vol2/vm171.dat</td>
<td>vol2</td>
<td>vs3</td>
<td>siderop1-vsim3</td>
<td>2</td>
</tr>
<tr>
<td>/vol/vol2/vm169.dat</td>
<td>vol2</td>
<td>vs3</td>
<td>siderop1-vsim3</td>
<td>2</td>
</tr>
<tr>
<td>/vol/vol2/pl23.dat</td>
<td>vol2</td>
<td>vs4</td>
<td>siderop1-vsim4</td>
<td>2</td>
</tr>
<tr>
<td>/vol/vol2/pl23.dat</td>
<td>vol2</td>
<td>vs3</td>
<td>siderop1-vsim3</td>
<td>2</td>
</tr>
<tr>
<td>/vol/vol1/vm171.dat</td>
<td>vol1</td>
<td>vs4</td>
<td>siderop1-vsim4</td>
<td>2</td>
</tr>
<tr>
<td>/vol/vol1/vm169.dat</td>
<td>vol1</td>
<td>vs4</td>
<td>siderop1-vsim4</td>
<td>2</td>
</tr>
<tr>
<td>/vol/vol1/vm169.dat</td>
<td>vol1</td>
<td>vs4</td>
<td>siderop1-vsim3</td>
<td>2</td>
</tr>
<tr>
<td>/vol/vol1/pl23.dat</td>
<td>vol1</td>
<td>vs4</td>
<td>siderop1-vsim4</td>
<td>2</td>
</tr>
</tbody>
</table>

Guaranteeing throughput with QoS

You can use storage quality of service (QoS) to guarantee that performance of critical workloads is not degraded by competing workloads. You can set a throughput ceiling on a competing workload to limit its impact on system resources, or set a throughput floor for a critical workload, ensuring that it meets minimum throughput targets, regardless of demand by competing workloads. You can even set a ceiling and floor for the same workload.

Understanding throughput ceilings (QoS Max)

A throughput ceiling limits throughput for a workload to a maximum number of IOPS, MB/s, or IOPS, MB/s. In the figure below, the throughput ceiling for workload 2 ensures that it does not “bully” workloads 1 and 3.

A policy group defines the throughput ceiling for one or more workloads. A workload represents the I/O operations for a storage object: a volume, file, or LUN, or all the volumes, files, or LUNs in an SVM. You can specify the ceiling when you create the policy group, or you can wait until after you monitor workloads to specify it.

Note: Throughput to workloads might exceed the specified ceiling by up to 10 percent, especially if a workload experiences rapid changes in throughput. The ceiling might be exceeded by up to 50% to handle bursts. Bursts occur on single nodes when tokens accumulate up to 150%
Understanding throughput floors (QoS Min)

A throughput floor guarantees that throughput for a workload does not fall below a minimum number of IOPS. In the figure below, the throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

**Tip:** As the examples suggest, a throughput ceiling throttles throughput directly. A throughput floor throttles throughput indirectly, by giving priority to the workloads for which the floor has been set.

A workload represents the I/O operations for a volume, LUN, or, starting with ONTAP 9.3, file. A policy group that defines a throughput floor cannot be applied to an SVM. You can specify the floor when you create the policy group, or you can wait until after you monitor workloads to specify it.

**Note:** Throughput to a workload might fall below the specified floor if there is insufficient performance capacity (headroom) on the node or aggregate, or during critical operations like volume move trigger-cutover. Even when sufficient capacity is available and critical operations are not taking place, throughput to a workload might fall below the specified floor by up to 5 percent.

**Understanding shared and non-shared QoS policy groups**

Starting with ONTAP 9.4, you can use a non-shared QoS policy group to specify that the defined throughput ceiling or floor applies to each member workload individually. Behavior of shared policy groups depends on the policy type:

- For throughput ceilings, the total throughput for the workloads assigned to the shared policy group cannot exceed the specified ceiling.
- For throughput floors, the shared policy group can be applied to a single workload only.
Understanding adaptive QoS

Ordinarily, the value of the policy group you assign to a storage object is fixed. You need to change the value manually when the size of the storage object changes. An increase in the amount of space used on a volume, for example, usually requires a corresponding increase in the throughput ceiling specified for the volume.

*Adaptive QoS* automatically scales the policy group value to workload size, maintaining the ratio of IOPS to TBs|GBs as the size of the workload changes. That is a significant advantage when you are managing hundreds or thousands of workloads in a large deployment.

You typically use adaptive QoS to adjust throughput ceilings, but you can also use it to manage throughput floors (when workload size increases). Workload size is expressed as either the allocated space for the storage object or the space used by the storage object.

**Note:** Used space is available for throughput floors in ONTAP 9.5 and later. It is not supported for throughput floors in ONTAP 9.4 and earlier.

- An *allocated space* policy maintains the IOPS/TB|GB ratio according to the nominal size of the storage object. If the ratio is 100 IOPS/GB, a 150 GB volume will have a throughput ceiling of 15,000 IOPS for as long as the volume remains that size. If the volume is resized to 300 GB, adaptive QoS adjusts the throughput ceiling to 30,000 IOPS.

- A *used space* policy (the default) maintains the IOPS/TB|GB ratio according to the amount of actual data stored before storage efficiencies. If the ratio is 100 IOPS/GB, a 150 GB volume that has 100 GB of data stored would have a throughput ceiling of 10,000 IOPS. As the amount of used space changes, adaptive QoS adjusts the throughput ceiling according to the ratio.

Starting with ONTAP 9.5, you can specify an I/O block size for your application that enables a throughput limit to be expressed in both IOPS and MB/s. The MB/s limit is calculated from the block size multiplied by the IOPS limit. For example, an I/O block size of 32K for an IOPS limit of 6144IOPS/TB yields an MB/s limit of 192MB/s.

You can expect the following behavior for both throughput ceilings and floors:

- When a workload is assigned to an adaptive QoS policy group, the ceiling or floor is updated immediately.
- When a workload in an adaptive QoS policy group is resized, the ceiling or floor is updated in approximately five minutes.

Throughput must increase by at least 10 IOPS before updates take place.

Adaptive QoS policy groups are always non-shared: the defined throughput ceiling or floor applies to each member workload individually.

Starting with ONTAP 9.6, throughput floors is supported on ONTAP Select premium with SSD.

**General support**

The following table shows the differences in support for throughput ceilings, throughput floors, and adaptive QoS.

<table>
<thead>
<tr>
<th>Resource or feature</th>
<th>Throughput ceiling</th>
<th>Throughput floor</th>
<th>Adaptive QoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONTAP 9 version</td>
<td>All</td>
<td>9.2 and later</td>
<td>9.3 and later</td>
</tr>
<tr>
<td>Platforms</td>
<td>All</td>
<td>AFF, ONTAP Select premium with SSD</td>
<td>All</td>
</tr>
<tr>
<td>Protocols</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Resource or feature</td>
<td>Throughput ceiling</td>
<td>Throughput floor</td>
<td>Adaptive QoS</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>FabricPool</td>
<td>Yes</td>
<td>Yes, if the tiering policy is set to “none” and no blocks are in the cloud.</td>
<td>Yes</td>
</tr>
<tr>
<td>SnapMirror Synchronous</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Supported workloads for throughput ceilings**

The following table shows workload support for throughput ceilings by ONTAP 9 version. Root volumes, load-sharing mirrors, and data protection mirrors are not supported.

<table>
<thead>
<tr>
<th>Workload support - ceiling</th>
<th>9.0</th>
<th>9.1</th>
<th>9.2</th>
<th>9.3</th>
<th>9.4 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>File</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>LUN</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SVM</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>FlexGroup volume</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Multiple workloads per policy group</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Non-shared policy groups</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Supported workloads for throughput floors**

The following table shows workload support for throughput floors by ONTAP 9 version. Root volumes, load-sharing mirrors, and data protection mirrors are not supported.

<table>
<thead>
<tr>
<th>Workload support - floor</th>
<th>9.2</th>
<th>9.3</th>
<th>9.4 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>File</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>LUN</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SVM</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>FlexGroup volume</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Multiple workloads per policy group</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Non-shared policy groups</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Supported workloads for adaptive QoS**

The following table shows workload support for adaptive QoS by ONTAP 9 version. Root volumes, load-sharing mirrors, and data protection mirrors are not supported.

<table>
<thead>
<tr>
<th>Workload support - adaptive QoS</th>
<th>9.3</th>
<th>9.4 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>File</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>LUN</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>
Workload support - adaptive QoS

<table>
<thead>
<tr>
<th></th>
<th>9.3</th>
<th>9.4 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>FlexGroup volume</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Multiple workloads per policy group</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Non-shared policy groups</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

Maximum number of workloads and policy groups

The following table shows the maximum number of workloads and policy groups by ONTAP 9 version.

<table>
<thead>
<tr>
<th>Workload support</th>
<th>9.3 and earlier</th>
<th>9.4 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum workloads per cluster</td>
<td>12,000</td>
<td>40,000</td>
</tr>
<tr>
<td>Maximum workloads per node</td>
<td>12,000</td>
<td>40,000</td>
</tr>
<tr>
<td>Maximum policy groups</td>
<td>12,000</td>
<td>12,000</td>
</tr>
</tbody>
</table>

Storage QoS workflow

If you already know the performance requirements for the workloads you want to manage with QoS, you can specify the throughput limit when you create the policy group. Otherwise, you can wait until after you monitor the workloads to specify the limit.
Do you know the performance requirements for the workloads?

- **Yes**
  - Create policy groups with throughput limits
  - Assign the storage objects to policy groups
  - Monitor performance by viewing statistics
  - Adjust policy group settings, if necessary

- **No**
  - Create policy groups without throughput limits
  - Assign the storage objects to policy groups
  - Monitor performance by viewing statistics
  - Adjust policy group settings, if necessary

**Related tasks**
- Setting a throughput ceiling with QoS on page 28
- Setting a throughput floor with QoS on page 31
- Using adaptive QoS policy groups on page 32

**Setting a throughput ceiling with QoS**

You can use the `max-throughput` field for a policy group to define a throughput ceiling for storage object workloads (QoS Max). You can apply the policy group when you create or modify the storage object.

**Before you begin**
- You must be a cluster administrator to create a policy group.
- You must be a cluster administrator to apply a policy group to an SVM.

**About this task**
- Starting with ONTAP 9.4, you can use a *non-shared* QoS policy group to specify that the defined throughput ceiling applies to each member workload individually. Otherwise, the policy group is *shared*: the total throughput for the workloads assigned to the policy group cannot exceed the specified ceiling.
Set \texttt{-is-shared=false} for the \texttt{qos policy-group create} command to specify a non-shared policy group.

- You can specify the throughput limit for the ceiling in IOPS, MB/s, or IOPS, MB/s. If you specify both IOPS and MB/s, whichever limit is reached first is enforced.
  
  \textbf{Note:} If you set a ceiling and a floor for the same workload, you can specify the throughput limit for the ceiling in IOPS only.

- A storage object that is subject to a QoS limit must be contained by the SVM to which the policy group belongs. Multiple policy groups can belong to the same SVM.
- You cannot assign a storage object to a policy group if its containing object or its child objects belong to the policy group.
- It is a QoS best practice to apply a policy group to the same type of storage objects.

\textbf{Steps}

1. Create a policy group:

\begin{verbatim}
qos policy-group create -policy group policy_group -vserver SVM -max-throughput number_of_iops|Mb/S|iops,Mb/S -is-shared true|false
\end{verbatim}

For complete command syntax, see the man page. You can use the \texttt{qos policy-group modify} command to adjust throughput ceilings.

\textbf{Example}

The following command creates the shared policy group \texttt{pg-vs1} with a maximum throughput of 5,000 IOPS:

\begin{verbatim}
cluster1::> qos policy-group create -policy group pg-vs1 -vserver vs1 -max-throughput 5000iops -is-shared true
\end{verbatim}

\textbf{Example}

The following command creates the non-shared policy group \texttt{pg-vs3} with a maximum throughput of 100 IOPS or 400 Kb/S:

\begin{verbatim}
cluster1::> qos policy-group create -policy group pg-vs3 -vserver vs3 -max-throughput 100iops,400KB/s -is-shared false
\end{verbatim}

\textbf{Example}

The following command creates the non-shared policy group \texttt{pg-vs4} without a throughput limit:

\begin{verbatim}
cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4 -is-shared false
\end{verbatim}

2. Apply a policy group to an SVM, file, volume, or LUN:

\begin{verbatim}
storage_object create -vserver SVM -qos-policy-group policy_group
\end{verbatim}

For complete command syntax, see the man pages. You can use the \texttt{storage_object modify} command to apply a different policy group to the storage object.

\textbf{Example}

The following command applies policy group \texttt{pg-vs1} to SVM \texttt{vs1}:

\begin{verbatim}
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
\end{verbatim}
Example
The following commands apply policy group **pg-app** to the volumes **app1** and **app2**:

```bash
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1 -qos-policy-group pg-app
```

```bash
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1 -qos-policy-group pg-app
```

3. Monitor policy group performance:

**qos statistics performance show**

For complete command syntax, see the man page.

**Note:** Monitor performance from the cluster. Do not use a tool on the host to monitor performance.

Example
The following command shows policy group performance:

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

4. Monitor workload performance:

**qos statistics workload performance show**

For complete command syntax, see the man page.

**Note:** Monitor performance from the cluster. Do not use a tool on the host to monitor performance.

Example
The following command shows workload performance:

```bash
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-Total-              -    12320        47.84MB/s  1215.00us
app1-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
```

**Note:** You can use the **qos statistics workload latency show** command to view detailed latency statistics for QoS workloads.

Related concepts

*Guaranteeing throughput with QoS* on page 23
Setting a throughput floor with QoS

You can use the `min-throughput` field for a policy group to define a throughput floor for storage object workloads (QoS Min). You can apply the policy group when you create or modify the storage object.

Before you begin

- You must be running ONTAP 9.2 or later. Throughput floors are available starting with ONTAP 9.2.
- You must be a cluster administrator to create a policy group.

About this task

- Starting with ONTAP 9.4, you can use a `non-shared` QoS policy group to specify that the defined throughput floor be applied to each member workload individually. This is the only condition in which a policy group for a throughput floor can be applied to multiple workloads.
  
  Set `-is-shared=false` for the `qos policy-group create` command to specify a non-shared policy group.

- Throughput to a workload might fall below the specified floor if there is insufficient performance capacity (headroom) on the node or aggregate.

- A storage object that is subject to a QoS limit must be contained by the SVM to which the policy group belongs. Multiple policy groups can belong to the same SVM.

- It is a QoS best practice to apply a policy group to the same type of storage objects.

- A policy group that defines a throughput floor cannot be applied to an SVM.

Steps

1. Check for adequate performance capacity on the node or aggregate, as described in Identifying remaining performance capacity on page 21.

2. Create a policy group:

   ```
   qos policy-group create -policy group policy_group -vserver SVM -min-throughput number_of_iops -is-shared true|false
   ```

   For complete command syntax, see the man page. You can use the `qos policy-group modify` command to adjust throughput floors.

   **Example**

   The following command creates the shared policy group `pg-vs2` with a minimum throughput of 1,000 IOPS:

   ```
   cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2 -min-throughput 1000iops -is-shared true
   ```

   **Example**

   The following command creates the non-shared policy group `pg-vs4` without a throughput limit:

   ```
   cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4 -is-shared false
   ```

3. Apply a policy group to a volume or LUN:

   ```
   storage_object create -vserver SVM -qos-policy-group policy_group
   ```

   For complete command syntax, see the man pages. You can use the `storage_object modify` command to apply a different policy group to the storage object.
Example

The following command applies policy group `pg-app2` to the volume `app2`:

```bash
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1 -qos-policy-group pg-app2
```

4. Monitor policy group performance:

```
qos statistics performance show
```

For complete command syntax, see the man page.

**Note:** Monitor performance from the cluster. Do not use a tool on the host to monitor performance.

Example

The following command shows policy group performance:

```bash
cluster1::> qos statistics performance show
```

<table>
<thead>
<tr>
<th>Policy Group</th>
<th>IOPS</th>
<th>Throughput</th>
<th>Latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>-total-</td>
<td>12316</td>
<td>47.76MB/s</td>
<td>1264.00us</td>
</tr>
<tr>
<td>pg_app2</td>
<td>7216</td>
<td>28.19MB/s</td>
<td>420.00us</td>
</tr>
<tr>
<td>_System-Best-Effort</td>
<td>62</td>
<td>13.36KB/s</td>
<td>4.13ms</td>
</tr>
<tr>
<td>_System-Background</td>
<td>30</td>
<td>0KB/s</td>
<td>0ms</td>
</tr>
</tbody>
</table>

5. Monitor workload performance:

```
qos statistics workload performance show
```

For complete command syntax, see the man page.

**Note:** Monitor performance from the cluster. Do not use a tool on the host to monitor performance.

Example

The following command shows workload performance:

```bash
cluster1::> qos statistics workload performance show
```

<table>
<thead>
<tr>
<th>Workload</th>
<th>ID</th>
<th>IOPS</th>
<th>Throughput</th>
<th>Latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>-total-</td>
<td>-</td>
<td>12320</td>
<td>47.84MB/s</td>
<td>1215.00us</td>
</tr>
<tr>
<td>app2-wid7967</td>
<td>7967</td>
<td>7219</td>
<td>28.20MB/s</td>
<td>319.00us</td>
</tr>
<tr>
<td>vs1-wid12279</td>
<td>12279</td>
<td>5026</td>
<td>19.63MB/s</td>
<td>2.52ms</td>
</tr>
<tr>
<td>_USERSPACE_APPS</td>
<td>14</td>
<td>55</td>
<td>10.92KB/s</td>
<td>236.00us</td>
</tr>
<tr>
<td>_Scan_Backgro..</td>
<td>5688</td>
<td>20</td>
<td>0KB/s</td>
<td>0ms</td>
</tr>
</tbody>
</table>

**Note:** You can use the `qos statistics workload latency show` command to view detailed latency statistics for QoS workloads.

Related concepts

*Guaranteeing throughput with QoS* on page 23

Using adaptive QoS policy groups

You can use an *adaptive QoS* policy group to automatically scale a throughput ceiling or floor to volume size, maintaining the ratio of IOPS to TBs|GBs as the size of the volume changes. That is a
significant advantage when you are managing hundreds or thousands of workloads in a large
deployment.

**Before you begin**

- You must be running ONTAP 9.3. Adaptive QoS policy groups are available starting with ONTAP 9.3.
- You must be a cluster administrator to create a policy group.

**About this task**

A storage object can be a member of an adaptive policy group or a non-adaptive policy group, but not both. The SVM of the storage object and the policy must be the same. The storage object must be online.

Adaptive QoS policy groups are always non-shared: the defined throughput ceiling or floor applies to each member workload individually.

The ratio of throughput limits to storage object size is determined by the interaction of the following fields:

- **expected-iops** is the minimum expected IOPS per allocated TB|GB.
  
  **Note:** expected-iops is guaranteed on AFF platforms only. expected-iops is guaranteed for FabricPool only if the tiering policy is set to “none” and no blocks are in the cloud.
  
  expected-iops is guaranteed for volumes that are not in a SnapMirror Synchronous relationship.

- **peak-iops** is the maximum possible IOPS per allocated or used TB|GB.

- **expected-iops-allocation** specifies whether allocated space (the default) or used space is used for expected-iops.
  
  **Note:** expected-iops-allocation is available in ONTAP 9.5 and later. It is not supported in ONTAP 9.4 and earlier.

- **peak-iops-allocation** specifies whether allocated space or used space (the default) is used for peak-iops.

- **absolute-min-iops** is the absolute minimum number of IOPS. You can use this field with very small storage objects. It overrides both peak-iops and/or expected-iops when absolute-min-iops is greater than the calculated expected-iops.

  For example, if you set expected-iops to 1,000 IOPS/TB, and the volume size is less than 1 GB, the calculated expected-iops will be a fractional IOP. The calculated peak-iops will be an even smaller fraction. You can avoid this by setting absolute-min-iops to a realistic value.

- **block-size** specifies the application I/O block size. The default is 32K. Valid values are 8K, 16K, 32K, 64K, ANY. ANY means that the block size is not enforced.

Three default adaptive QoS policy groups are available, as shown in the following table. You can apply these policy groups directly to a volume.

<table>
<thead>
<tr>
<th>Default policy group</th>
<th>Expected IOPS/TB</th>
<th>Peak IOPS/TB</th>
<th>Absolute Min IOPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>extreme</td>
<td>6,144</td>
<td>12,288</td>
<td>1000</td>
</tr>
<tr>
<td>performance</td>
<td>2,048</td>
<td>4,096</td>
<td>500</td>
</tr>
<tr>
<td>value</td>
<td>128</td>
<td>512</td>
<td>75</td>
</tr>
</tbody>
</table>

**Steps**

1. Create an adaptive QoS policy group:
qos adaptive-policy-group create -policy group policy_group -vserver SVM

For complete command syntax, see the man page.

**Note:** -expected-iops-allocation and -block-size is available in ONTAP 9.5 and later. These options are not supported in ONTAP 9.4 and earlier.

**Example**

The following command creates adaptive QoS policy group adpg-app1 with -expected-iops set to 300 IOPS/TB, -peak-iops set to 1,000 IOPS/TB, -peak-iops-allocation set to used-space, and -absolute-min-iops set to 50 IOPS:

```
classic1::> qos adaptive-policy-group create -policy group adpg-app1 -vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops-allocation used-space -absolute-min-iops 50iops
```

2. Apply an adaptive QoS policy group to a volume:

```
volume create -vserver SVM -volume volume -aggregate aggregate -size number_of_TB|GB -qos-adaptive-policy-group policy_group
```

For complete command syntax, see the man pages.

**Example**

The following command applies adaptive QoS policy group adpg-app1 to volume app1:

```
classic1::> volume create -vserver vs1 -volume app1 -aggregate aggr1 -size 2TB -qos-adaptive-policy-group adpg-app1
```

**Example**

The following commands apply the default adaptive QoS policy group extreme to the new volume app4 and to the existing volume app5. The throughput ceiling defined for the policy group applies to volumes app4 and app5 individually:

```
classic1::> volume create -vserver vs4 -volume app4 -aggregate aggr4 -size 2TB -qos-adaptive-policy-group extreme
classic1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy-group extreme
```

**Related concepts**

*Guaranteeing throughput with QoS* on page 23
Where to find additional information

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

- **Active IQ Unified Manager 9.6 System Configuration Guide**
  Provides initial setup and configuration instructions for Unified Manager. This includes adding clusters, adding users, configuring alerts, and setting up remote authentication.

- **Active IQ Unified Manager 9.6 Workflow Guide for Managing Cluster Performance**
  Provides information about using Unified Manager to manage and troubleshoot cluster storage performance issues. This includes identifying workloads that are overusing cluster components so that you can take corrective action to bring performance back to normal levels of operation.

- **System administration**
  Describes general system administration for storage systems running ONTAP.

- **NetApp Technical Report 4211: Storage Performance Primer**
  Describes the basic performance concepts in ONTAP, how different processes can impact performance, and how to observe cluster performance.
Copyright

Copyright © 2019 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).
Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

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., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277