



# Event and performance monitoring

## ONTAP 9

NetApp  
May 07, 2023

This PDF was generated from [https://docs.netapp.com/us-en/ontap/task\\_cp\\_monitor\\_cluster\\_performance\\_sm.html](https://docs.netapp.com/us-en/ontap/task_cp_monitor_cluster_performance_sm.html) on May 07, 2023. Always check docs.netapp.com for the latest.

# Table of Contents

- Event and performance monitoring . . . . . 1
  - Monitor cluster performance with System Manager . . . . . 1
  - Monitor and manage cluster performance using the CLI . . . . . 2
  - Monitor cluster performance with Unified Manager . . . . . 38
  - Monitor cluster performance with Cloud Insights . . . . . 38
- File System Analytics . . . . . 39
- EMS configuration . . . . . 53

# Event and performance monitoring

## Monitor cluster performance with System Manager

### Monitor cluster performance using System Manager

The topics in this section show you how to manage cluster health and performance with System Manager in ONTAP 9.7 and later releases.

You can monitor cluster performance by viewing information about your system on the System Manager Dashboard. The Dashboard displays information about important alerts and notifications, the efficiency and capacity of storage tiers and volumes, the nodes that are available in a cluster, the status of the nodes in an HA pair, the most active applications and objects, and the performance metrics of a cluster or a node.

The Dashboard lets you determine the following information:

- **Health:** How healthy is the cluster?
- **Capacity:** What capacity is available on the cluster?
- **Performance:** How well is the cluster performing, based on latency, IOPS, and throughput?
- **Network:** How is the network configured with hosts and storage objects, such as ports, interfaces, and storage VMs?

In the Health and Capacity overviews, you can click [→](#) to view additional information and perform tasks.

In the Performance overview, you can view metrics based on the hour, the day, the week, the month, or the year.

In the Network overview, the number of each object in the network is displayed (for example, "8 NVMe/FC ports"). You can click on the numbers to view details about each network object.

### View performance on cluster dashboard

Use the dashboard to make informed decisions about workloads you might want to add or move. You can also look at peak usage times to plan for potential changes.

The performance values refresh every 3 seconds and the performance graph refreshes every 15 seconds.

#### Steps

1. Click **Dashboard**.
2. Under **Performance**, select the interval.

### Identify hot volumes and other objects

Accelerate your cluster performance by identifying the frequently accessed volumes (hot volumes) and data (hot objects).



Beginning in ONTAP 9.10.1, you can use the Activity Tracking feature in File System Analytics to monitor hot objects in a volume.

### Steps

1. Click **Storage > Volumes**.
2. Filter the IOPS, latency, and throughput columns to view the frequently accessed volumes and data.

## Modify QoS

Beginning with ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process. You can also modify QoS after your storage has been provisioned.

### Steps

1. In System Manager, click **Storage** and select **Volumes**.
2. Next to the volume for which you want to modify QoS, click  and select **Edit**.

## Monitor and manage cluster performance using the CLI

### Performance monitoring and management overview

You can set up basic performance monitoring and management tasks and identify and resolve common performance issues.

You can use these procedures to monitor and manage cluster performance if the following assumptions apply to your situation:

- You want to use best practices, not explore every available option.
- 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.

### Related information

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

- [Active IQ Unified Manager 9.8 Installation](#)
- [System administration](#)

## Monitor performance

## Performance monitoring and maintenance workflow overview

Monitoring and maintaining cluster performance involves installing Active IQ Unified Manager software, setting up basic monitoring tasks, identifying performance issues, and making adjustments as needed.



### Verify that your VMware environment is supported

To successfully install 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



The [Interoperability Matrix](#) lists the supported configurations for Unified 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.

### 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

| 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) |
| Email from which alert notifications are sent |                    |
| LDAP bind distinguished name                  |                    |
| LDAP bind password                            |                    |
| Active Directory administrator name           |                    |
| Active Directory password                     |                    |
| Authentication server base distinguished name |                    |
| Authentication server host name or IP address |                    |

#### Cluster information

Capture the following information for each cluster on Unified Manager.

| Cluster 1 of N  | Your value |
|---|------------|
| Host name or cluster-management IP address  |            |
| <div>  <p>The administrator must have been assigned the "admin" role.</p> </div> ONTAP administrator user name |            |
| ONTAP administrator password  |            |
| Protocol (HTTP or HTTPS)  |            |

#### Related information

[Administrator authentication and RBAC](#)

## Install Active IQ Unified Manager

### Download and deploy 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.

<https://mysupport.netapp.com/products/index.html>

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.

### Configure 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.

### Specify 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.

#### What you'll need

- 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 Application 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 **Cluster Setup** page.

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

## Set up basic monitoring tasks

### Perform 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.

### Use 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.

### Use 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.

### Set 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.

|                           |   |  |       |    |       |
|---------------------------|---|--|-------|----|-------|
|                           |  Warning |  Critical |       |    |       |
| Object Counter Condition* | Average Latency ms/op   | 12   | ms/op | 15 | ms/op |

### Add 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.

### What you'll need

- 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 Scripts page.
- You must have the Application 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 Alert Setup page, as described here.

## Steps

1. In the left navigation pane, click **Storage Management > Alert Setup**.
2. In the **Alert Setup** 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.



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.



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 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](mailto: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**.

### Configure alert settings

You can specify which events from Active IQ Unified Manager trigger alerts, the email recipients for those alerts, and the frequency for the alerts.

### What you'll need

You must have the Application 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 Unified Manager admin users for all new events. You can have email alerts sent to other users by adding those users' email addresses.



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

### Steps

1. In the left navigation pane, select **Storage Management > Alert Setup**.

The Alert Setup page is displayed.

2. Click **Add** and 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**.

### Identify 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.

| If you...   | Then...  |
|---|--|
| Receive an email notification of an event                 | Click the link to go directly to the event details page.   |
| Notice the event while analyzing the Event Inventory page | Select the event to go directly to the event details page. |

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.

## Use Active IQ Digital Advisor to view system performance

For any ONTAP system that sends AutoSupport telemetry to NetApp, you can view extensive performance and capacity data. Active IQ shows system performance over a longer period than you can see in System Manager.

You can view graphs of CPU utilization, latency, IOPS, IOPS by protocol, and network throughput. You can also download this data in .csv format for analysis in other tools.

In addition to this performance data, Active IQ can show you storage efficiency by workload and compare that efficiency to the expected efficiency for that type of workload. You can view capacity trends and see an estimate of how much additional storage you might need to add in a given time frame.



- Storage Efficiency is available at the customer, cluster, and node level on the left-hand-side of the main dashboard.
- Performance is available at the cluster and node level on the left-hand-side of the main dashboard.

## Related information

- [Active IQ Digital Advisor documentation](#)
- [Active IQ Digital Advisor video playlist](#)
- [Active IQ Web Portal](#)

## Manage performance issues

### 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.



## Perform basic infrastructure checks

### Check protocol settings on the storage system

#### Check 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.

#### What you'll need

- 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:

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

#### Check 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.

#### What you'll need

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 -vserv,er 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
```

### Check 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
```

### Check 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.

#### What you'll need

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
```

### Check the network settings on the data switches

Although you must maintain the same MTU settings on your clients, servers and storage systems (that is, network endpoints), intermediate network devices such as NICs and switches should be set to their maximum MTU values to ensure that performance is not impacted.

For best performance, all components in the network must be able to forward jumbo frames (9000 bytes IP, 9022 bytes including Ethernet). Data switches should be set to at least 9022 bytes, but a typical value of 9216 is possible with most switches.

### Procedure

For data switches, check that the MTU size is set to 9022 or higher.

For more information, see the switch vendor documentation.

### Check 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 other network endpoints. Whereas the management network MTU setting is set to 1500, the data network MTU size should be 9000.

## About this task

All ports within a broadcast-domain have the same MTU size, with the exception of the e0M port handling management traffic. If the port is part of a broadcast-domain, use the `broadcast-domain modify` command to change the MTU for all ports within the modified broadcast-domain.

Note that intermediate network devices such as NICs and data switches can be set to higher MTU sizes than network endpoints. For more information, see [Check the network settings on the data switches](#).

## Steps

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

```
network port show -instance
```

2. Change the MTU on the broadcast domain used by the ports:

```
network port broadcast-domain modify -ipspace ipspace -broadcast-domain  
broadcast_domain -mtu new_mtu
```

## Example

The following example changes the MTU port setting to 9000:

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain  
Cluster -mtu 9000
```

## Check 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

```

| Disk    | Node  | Busy (%) | Total Ops | Read Ops | Write Ops | Read (Bps) | Write (Bps) | *Latency (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         |

### Check throughput and latency 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.

#### What you'll need

- 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 throughput and latency between nodes. You can run the command between intercluster nodes or intracluster nodes.



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   |
|------------------|---|
| AsyncMirrorLocal | Settings used by SnapMirror between nodes in the same cluster |

|                    |   |
|--------------------|---|
| AsyncMirrorRemote  | Settings used by SnapMirror between nodes in different clusters (default type)  |
| RemoteDataTransfer | Settings used by ONTAP for remote data access 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 throughput and latency 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.

The following command measures throughput and latency 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:

```
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.

## Manage workloads

## Identify 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.

### What you'll need

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 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.

```
sti2520-2131454963690::*> 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.

### Identify 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.

## What you'll need

You must be a cluster administrator to perform this task.

## Steps

1. View the top clients accessing the cluster:

```
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.

The following command displays the top clients accessing cluster1:

```
cluster1::> statistics top client show
```

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

| Client         | Vserver | Node         | Protocol | *Total<br>Ops |
|----------------|---------|--------------|----------|---------------|
| -----          | -----   | -----        | -----    | -----         |
| 172.17.180.170 | vs4     | siderop1-vs4 | nfs      | 668           |
| 172.17.180.169 | vs3     | siderop1-vs3 | nfs      | 337           |
| 172.17.180.171 | vs3     | siderop1-vs3 | nfs      | 142           |
| 172.17.180.170 | vs3     | siderop1-vs3 | nfs      | 137           |
| 172.17.180.123 | vs3     | siderop1-vs3 | nfs      | 137           |
| 172.17.180.171 | vs4     | siderop1-vs4 | nfs      | 95            |
| 172.17.180.169 | vs4     | siderop1-vs4 | nfs      | 92            |
| 172.17.180.123 | vs4     | siderop1-vs4 | nfs      | 92            |
| 172.17.180.153 | vs3     | siderop1-vs3 | nfs      | 0             |

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.

The following command displays the top files accessed on cluster1:



```
cluster1::> statistics top file show
```

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

|                          |       |        | *Total       |       |       |
|--------------------------|-------|--------|--------------|-------|-------|
|                          | File  | Volume | Vserver      | Node  | Ops   |
| -----                    | ----- | -----  | -----        | ----- | ----- |
| /vol/vol1/vm170-read.dat | vol1  | vs4    | siderop1-vs4 | 22    |       |
| /vol/vol1/vm69-write.dat | vol1  | vs3    | siderop1-vs3 | 6     |       |
| /vol/vol2/vm171.dat      | vol2  | vs3    | siderop1-vs3 | 2     |       |
| /vol/vol2/vm169.dat      | vol2  | vs3    | siderop1-vs3 | 2     |       |
| /vol/vol2/p123.dat       | vol2  | vs4    | siderop1-vs4 | 2     |       |
| /vol/vol2/p123.dat       | vol2  | vs3    | siderop1-vs3 | 2     |       |
| /vol/vol1/vm171.dat      | vol1  | vs4    | siderop1-vs4 | 2     |       |
| /vol/vol1/vm169.dat      | vol1  | vs4    | siderop1-vs4 | 2     |       |
| /vol/vol1/vm169.dat      | vol1  | vs4    | siderop1-vs3 | 2     |       |
| /vol/vol1/p123.dat       | vol1  | vs4    | siderop1-vs4 | 2     |       |

## Guarantee throughput with QoS

### Guarantee throughput with QoS overview

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.

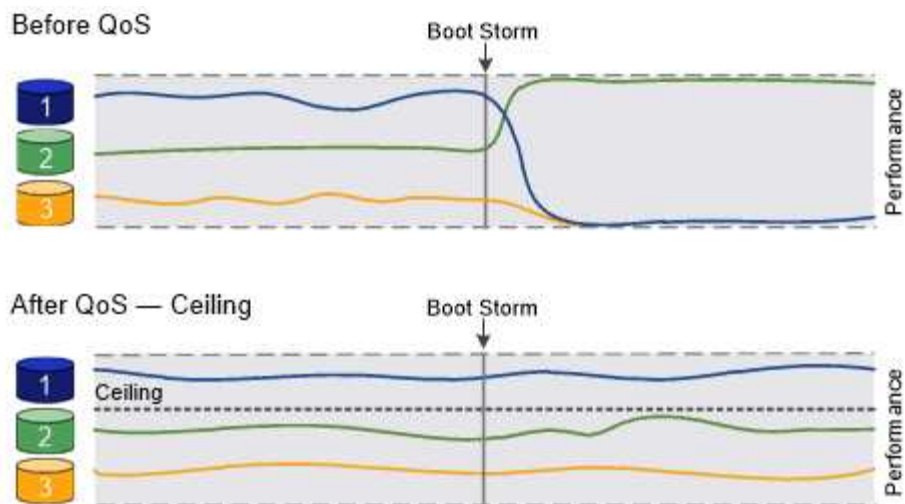
### About throughput ceilings (QoS Max)

A throughput ceiling limits throughput for a workload to a maximum number of IOPS or MBps, or IOPS and MBps. 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, qtree or LUN, or all the volumes, files, qtrees, 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.



Throughput to workloads might exceed the specified ceiling by up to 10%, 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%



### About throughput floors (QoS Min)

A throughput floor guarantees that throughput for a workload does not fall below a minimum number of IOPS or MBps, or IOPS and MBps. 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.



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.

You can specify the floor when you create the policy group, or you can wait until after you monitor workloads to specify it.

Beginning in ONTAP 9.13.1, you can set throughput floors at the SVM scope with [Adaptive policy group templates](#). In releases of ONTAP before 9.13.1, a policy group that defines a throughput floor cannot be applied to an SVM.



In releases before ONTAP 9.7, throughput floors are guaranteed when there is sufficient performance capacity available.

+

In ONTAP 9.7 and later, throughput floors can be guaranteed even when there is insufficient performance capacity available. This new floor behavior is called floors v2. To meet the guarantees, floors v2 can result in higher latency on workloads without a throughput floor or on work that exceeds the floor settings. Floors v2 applies to both QoS and adaptive QoS.

+

The option of enabling/disabling the new behavior of floors v2 is available in ONTAP 9.7P6 and later. A workload might fall below the specified floor 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%. If floors are overprovisioned and there is no performance capacity, some workloads might fall below the specified floor.



### About shared and non-shared QoS policy groups

Beginning 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.

### About 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.



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.

Beginning 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 MBps. The MBps 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 MBps limit of 192MBps.

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.

Beginning with ONTAP 9.6, throughput floors are supported on ONTAP Select premium with SSD.

### Adaptive policy group template

Beginning in ONTAP 9.13.1, you can set an adaptive QoS template on an SVM. Adaptive policy group templates enable you to set throughput floors and ceilings for all volumes in an SVM.

Adaptive policy group templates can only be set after the SVM has been created. Use the `vserver modify` command with the `-qos-adaptive-policy-group-template` parameter to set the policy.

When you set an an adaptive policy group template, volumes created or migrated after setting the policy automatically inherit the policy. Any volumes existing on the SVM are not impacted when you assign the policy template. If you disable the policy on the SVM, any volume subsequently migrated to or created on the SVM will not receive the policy. Disabling the adaptive policy group template does not impact volumes that inherited the policy template as they retain the policy template.

For more information, see [Set an adaptive policy group template](#).

### General support

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

| Resource or feature | Throughput ceiling | Throughput floor   | Throughput floor v2  | Adaptive QoS  |
|---------------------|--------------------|--|--|---------------|
| ONTAP 9 version     | All                | 9.2 and later  | 9.7 and later  | 9.3 and later |
| Platforms           | All                | <ul style="list-style-type: none"><li>• AFF</li><li>• C190 *</li><li>• ONTAP Select premium with SSD *</li></ul> | <ul style="list-style-type: none"><li>• AFF</li><li>• C190</li><li>• ONTAP Select premium with SSD</li></ul> | All           |
| Protocols           | All                | All  | All  | All           |

| Resource or feature    | Throughput ceiling | Throughput floor  | Throughput floor v2   | Adaptive QoS |
|------------------------|--------------------|---|---|--------------|
| FabricPool             | Yes                | Yes, if the tiering policy is set to "none" and no blocks are in the cloud. | Yes, if the tiering policy is set to "none" and no blocks are in the cloud. | Yes          |
| SnapMirror Synchronous | Yes                | No  | No  | Yes          |

\\*C190 and ONTAP Select support started with the ONTAP 9.6 release.

### 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.

| Workload support - ceiling          | ONTAP 9.0 | ONTAP 9.1 | ONTAP 9.2 | ONTAP 9.3 | ONTAP 9.4 - 9.7 | ONTAP 9.8 and later |
|-------------------------------------|-----------|-----------|-----------|-----------|-----------------|---------------------|
| Volume                              | yes       | yes       | yes       | yes       | yes             | yes                 |
| File                                | yes       | yes       | yes       | yes       | yes             | yes                 |
| LUN                                 | yes       | yes       | yes       | yes       | yes             | yes                 |
| SVM                                 | yes       | yes       | yes       | yes       | yes             | yes                 |
| FlexGroup volume                    | no        | no        | no        | yes       | yes             | yes                 |
| qtrees*                             | no        | no        | no        | no        | no              | yes                 |
| Multiple workloads per policy group | yes       | yes       | yes       | yes       | yes             | yes                 |
| Non-shared policy groups            | no        | no        | no        | no        | yes             | yes                 |

\\*Beginning with ONTAP 9.8, NFS access is supported in qtrees in FlexVol and FlexGroup volumes with NFS enabled. Beginning with ONTAP 9.9.1, SMB access is also supported in qtrees in FlexVol and FlexGroup volumes with SMB enabled.

## 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.

| Workload support - floor            | ONTAP 9.2 | ONTAP 9.3 | ONTAP 9.4 - 9.7 | ONTAP 9.8 - 9.13.0 | ONTAP 9.13.1 and later |
|-------------------------------------|-----------|-----------|-----------------|--------------------|------------------------|
| Volume                              | yes       | yes       | yes             | yes                | yes                    |
| File                                | no        | yes       | yes             | yes                | yes                    |
| LUN                                 | yes       | yes       | yes             | yes                | yes                    |
| SVM                                 | no        | no        | no              | no                 | yes                    |
| FlexGroup volume                    | no        | no        | yes             | yes                | yes                    |
| qtrees *                            | no        | no        | no              | yes                | yes                    |
| Multiple workloads per policy group | no        | no        | yes             | yes                | yes                    |
| Non-shared policy groups            | no        | no        | yes             | yes                | yes                    |

\*Beginning with ONTAP 9.8, NFS access is supported in qtrees in FlexVol and FlexGroup volumes with NFS enabled. Beginning with ONTAP 9.9.1, SMB access is also supported in qtrees in FlexVol and FlexGroup volumes with SMB enabled.

## 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.

| Workload support - adaptive QoS     | ONTAP 9.3 | ONTAP 9.4 - 9.13.0 | ONTAP 9.13.1 and later |
|-------------------------------------|-----------|--------------------|------------------------|
| Volume                              | yes       | yes                | yes                    |
| File                                | no        | yes                | yes                    |
| LUN                                 | no        | yes                | yes                    |
| SVM                                 | no        | no                 | yes                    |
| FlexGroup volume                    | no        | yes                | yes                    |
| Multiple workloads per policy group | yes       | yes                | yes                    |
| Non-shared policy groups            | yes       | yes                | yes                    |

## Maximum number of workloads and policy groups

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

| Workload support              | ONTAP 9.3 and earlier | ONTAP 9.4 and later |
|-------------------------------|-----------------------|---------------------|
| Maximum workloads per cluster | 12,000                | 40,000              |
| Maximum workloads per node    | 12,000                | 40,000              |
| Maximum policy groups         | 12,000                | 12,000              |

### Enable or disable throughput floors v2

You can enable or disable throughput floors v2 on AFF. The default is enabled. With floors v2 enabled, throughput floors can be met when controllers are heavily used at the expense of higher latency on other workloads. Floors v2 applies to both QoS and Adaptive QoS.

#### Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Enter one of the following commands:

| If you want to... | Use this command:  |
|-------------------|--|
| Disable floors v2 | <code>qos settings throughput-floors-v2 -enable false</code> |
| Enable floors v2  | <code>qos settings throughput-floors-v2 -enable true</code>  |



To disable throughput floors v2 in an MetroCluster cluster, you must run the

```
qos settings throughput-floors-v2 -enable false
```

command on both the source and destination clusters.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

### 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.

## Set 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.

### What you'll need

- 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

- Beginning 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 `-is-shared=false` for the `qos policy-group create` command to specify a non-shared policygroup.

- 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.



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.

### Steps

1. Create a policy group:

```
qos policy-group create -policy-group policy_group -vserver SVM -max  
-throughput number_of_iops|Mb/S|iops,Mb/S -is-shared true|false
```

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

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

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

The following command creates the non-shared policy group `pg-vs3` with a maximum throughput of 100 IOPS and 400 Kb/S:



```
cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
-max-throughput 100iops,400KB/s -is-shared false
```

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
```

## 2. Apply a policy group to an SVM, file, 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.

The following command applies policy group `pg-vs1` to SVM `vs1`:

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

The following commands apply policy group `pg-app` to the volumes `app1` and `app2`:

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

```
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.



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

The following command shows policy group performance:

```
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.



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

The following command shows workload performance:

```
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       |



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

### Set 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. Beginning with ONTAP 9.8, you can specify the throughput floor in IOPS or MBps, or IOPS and MBps.

#### Before you begin

- You must be running ONTAP 9.2 or later. Throughput floors are available beginning with ONTAP 9.2.
- You must be a cluster administrator to create a policy group.
- Beginning in ONTAP 9.13.1, you can enforce throughput floors at the SVM level using an [adaptive policy group template](#). You cannot set an adaptive policy group template on an SVM with a QoS policy group.

#### About this task

- Beginning 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 [permalink :identify-remaining-performance-capacity-task.html](#)[Identifying remaining performance capacity].
2. Create a policy group:

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

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

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
```

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.

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

```
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.



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

The following command shows policy group performance:

```
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  |
| _System-Best-Effort | 62    | 13.36KB/s  | 4.13ms    |
| _System-Background  | 30    | 0KB/s      | 0ms       |

#### 5. Monitor workload performance:

```
qos statistics workload performance show
```

For complete command syntax, see the man page.



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

The following command shows workload performance:

```
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       |



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

## Use 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 or later. Adaptive QoS policy groups are available beginning 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.



`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`.



`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.

| Default policy group | Expected IOPS/TB | Peak IOPS/TB | Absolute Min IOPS |
|----------------------|------------------|--------------|-------------------|
| extreme              | 6,144            | 12,288       | 1000              |
| performance          | 2,048            | 4,096        | 500               |
| value                | 128              | 512          | 75                |

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...                                       |
|--------------------------|---|
| SVM to a policy group    | Any storage objects contained by the SVM to a policy group      |
| 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            |
| File to a policy group   | The file's containing volume or SVM to a policy group           |

## Steps

1. Create an adaptive QoS policy group:

```
qos adaptive-policy-group create -policy group policy_group -vserver SVM
-expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB -expected
-iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-
space -absolute-min-iops number_of_iops -block-size 8K|16K|32K|64K|ANY
```

For complete command syntax, see the man page.



-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.

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:

```
cluster1::> 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.

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

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

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:

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

## Set an adaptive policy group template

Beginning in ONTAP 9.13.1, you can enforce throughput floors and ceilings at the SVM level using an adaptive policy group template.

### About this task

- The adaptive policy group template is a default policy `apg1`. The policy can be modified at any time. It can only be set with the CLI or ONTAP REST API and can only be applied to existing SVMs.
- The adaptive policy group template only impacts volumes created on or migrated to the SVM after you set the policy. Existing volumes on the SVM retain their existing status.

If you disable the adaptive policy group template, volumes on the SVM retain their existing policies. Only volumes subsequently created on or migrated to the SVM will be impacted by the disablement.

- You cannot set an adaptive policy group template on an SVM with a QoS policy group.
- Adaptive policy group templates are designed for AFF platforms. An adaptive policy group template can be set on other platforms, but the policy may not enforce a minimum throughput. Similarly, you can add an adaptive policy group template to an SVM in a FabricPool aggregate or in an aggregate that does not support a minimum throughput, however the throughput floor will not be enforced.
- If the SVM is in a MetroCluster configuration or an SnapMirror relationship, the adaptive policy group template will be enforced on the mirrored SVM.

### Steps

1. Modify the SVM to apply the adaptive policy group template:

```
vserver modify -qos-adaptive-policy-group-template apg1
```

2. Confirm the policy was set:

```
vserver show -fields qos-adaptive-policy-group
```

## Monitor cluster performance with Unified Manager

With Active IQ Unified Manager, you can maximize availability and maintain control of your NetApp AFF and FAS storage infrastructure for improved scalability, supportability, performance, and security.

Active IQ Unified Manager continuously monitors system health and send alerts, so your organization can free up IT staff resources. You can instantly view storage status from a single dashboard and quickly address issues through recommended actions.

Data management is simplified because you can discover, monitor, and receive notifications to proactively manage storage and quickly resolve issues. Admin efficiency is improved because you can monitor petabytes of data from a single dashboard and manage your data at scale.

With Active IQ Unified Manager, you can keep pace with fluctuating business demands, optimizing performance using performance data and advanced analytics. The reporting capabilities allow you to access standard reports or create custom operational reports to meet the specific needs of your business.

## Monitor cluster performance with Cloud Insights

NetApp Cloud Insights is a monitoring tool that gives you visibility into your complete infrastructure. With Cloud Insights, you can monitor, troubleshoot, and optimize all your resources including your public clouds and your private data centers.

### Cloud Insights comes in two editions

Cloud Insights Basic Edition is designed specifically to monitor and optimize your NetApp Data Fabric assets. It provides advanced analytics for the connections between all NetApp resources including HCI and All Flash FAS (AFF) within the environment free of charge.

Cloud Insights Standard Edition focuses not only on NetApp Data Fabric-enabled infrastructure components, but also on multi-vendor and multi-cloud environments. With its enriched capabilities, you can access support for over 100 services and resources.

In today's world, with resources in play from your on-premises data centers to multiple public clouds, it's crucial to have the complete picture from the application itself to the backend disk of the storage array. The additional support for application monitoring (like Kafka, MongoDB, and Nginx) gives you the information and knowledge you need to operate at the optimal level of utilization as well as with the perfect risk buffer.

Both editions (Basic and Standard) can integrate with NetApp Active IQ Unified Manager. Customers who use Active IQ Unified Manager will be able to see join information inside the Cloud Insights user interface. Notifications posted on Active IQ Unified Manager will not be overlooked and can now be correlated to events in Cloud Insights. In other words, you get the best of both worlds.

### Monitor, troubleshoot, and optimize all your resources

Cloud Insights helps you significantly reduce the time to resolve issues and prevent them from impacting end users. It also helps you reduce cloud infrastructure costs. Your exposure to insider threats is reduced by



protecting your data with actionable intelligence.

Cloud Insights gives you visibility to your entire hybrid infrastructure in one place—from the public cloud to your data center. You can instantly create relevant dashboards that can be customized to your specific needs. You can also create targeted and conditional alerts that are specific and relevant to your organization's needs.

Advanced anomaly detection helps you proactively fix issues before they arise. You can view resource contention and degradation automatically to quickly restore impacted workloads. Troubleshooting goes more quickly with the automatically built hierarchy of relationships between the different components in your stack.

You can identify unused or abandoned resources across your environment, which helps you discover opportunities to right-size the infrastructure and optimize your entire spend.

Cloud Insights visualizes your system topology to gain an understanding of your Kubernetes architecture. You can monitor the health of your Kubernetes clusters, including which nodes are in trouble, and zoom in when you see a problem.

Cloud Insights helps you protect organizational data from being misused by malicious or compromised users through advanced machine learning and anomaly detection that gives you actionable intelligence on insider threats.

Cloud Insights helps you to visualize Kubernetes metrics so you can fully understand the relations between your pods, nodes, and clusters. You're able to assess the health of a cluster or a working pod, as well as the load it is currently processing—enabling you to take command of your K8S cluster and to control both the health and the cost of your deployment.

## File System Analytics

### File System Analytics overview

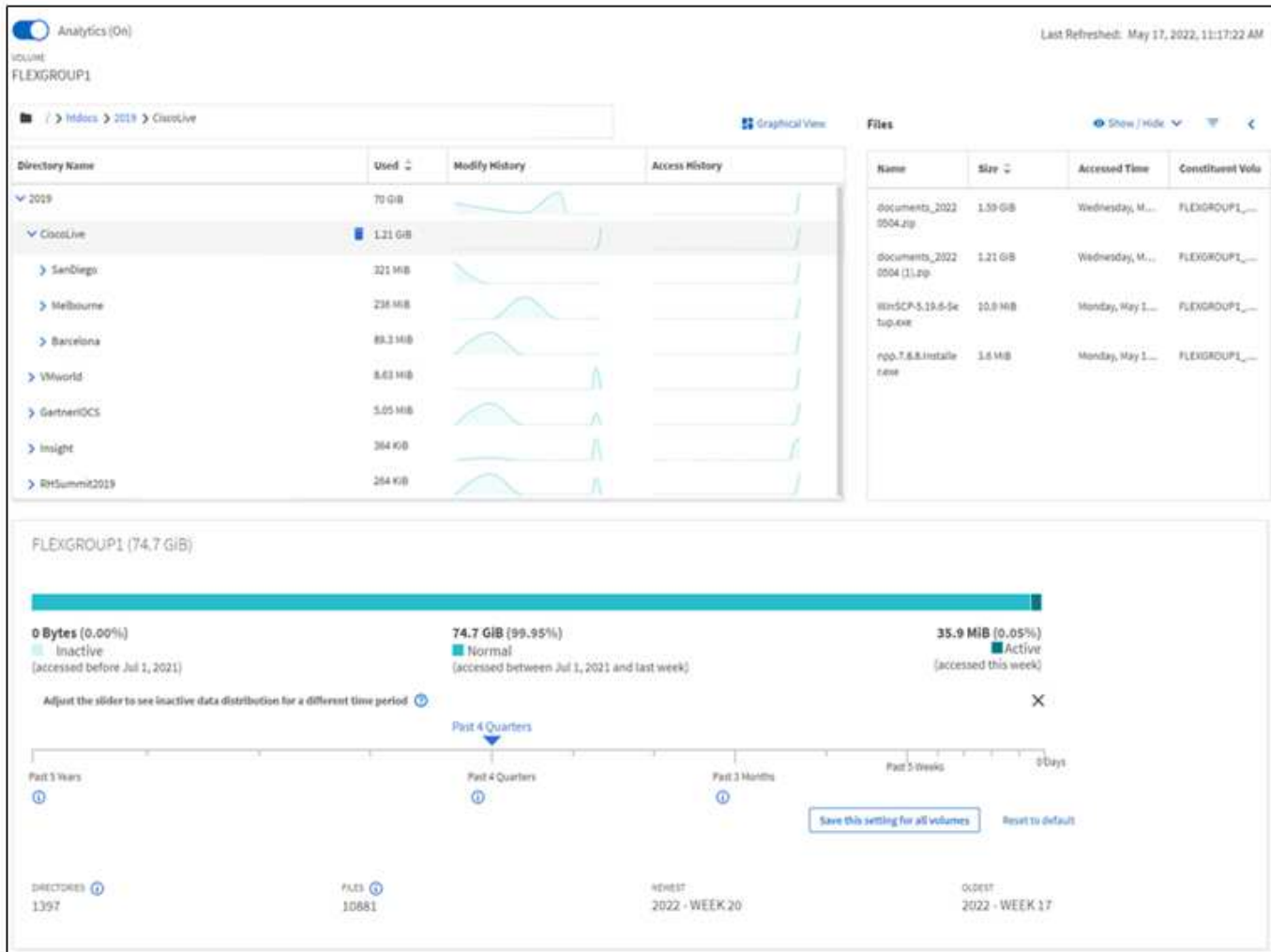
File System Analytics (FSA) was first introduced in ONTAP 9.8 to provide real-time visibility into file usage and storage capacity trends inside ONTAP FlexGroup or FlexVol volumes. This native capability eliminates the need for external tools and provides key insights into how your storage is utilized and whether there are opportunities to optimize the storage for your business needs.

With FSA, you have visibility at all levels of a volume's file system hierarchy in NAS. For example, you can gain usage and capacity insights at the Storage VM (SVM), volume, directory, and file levels. You can use FSA to answer questions like:

- What is filling up my storage, and are there any large files I can move to another storage location?
- Which are my most active volumes, directories, and files? Is my storage performance optimized for the needs of my users?
- How much data was added in the last month?
- Who are my most active or least active storage users?
- How much inactive or dormant data is on my primary storage? Can I move that data to a lower cost cold tier?
- Will my planned quality-of-service changes negatively impact access to critical, frequently accessed files?

File System Analytics is integrated into ONTAP System Manager. Views within System Manager provide:

- Real-time visibility for effective data management and operation
- Real-time data collection and aggregation
- Subdirectory and file sizes and counts, together with associated performance profiles
- File age histograms for modify and access histories



## Supported volume types

File System Analytics is designed to provide visibility on volumes with active NAS data, with the exception of FlexCache caches and SnapMirror destination volumes.

## File System Analytics feature availability

Each ONTAP release expands the scope of File System Analytics.

|                                 | ONTAP 9.13.1 | ONTAP 9.12.1 | ONTAP 9.11.1 | ONTAP 9.10.1 | ONTAP 9.9.1 | ONTAP 9.8 |
|---------------------------------|--------------|--------------|--------------|--------------|-------------|-----------|
| Visualization in System Manager | X            | X            | X            | X            | X           | X         |
| Capacity analytics              | X            | X            | X            | X            | X           | X         |
| Inactive data information       | X            | X            | X            | X            | X           | X         |

|   | ONTAP 9.13.1 | ONTAP 9.12.1 | ONTAP 9.11.1 | ONTAP 9.10.1 | ONTAP 9.9.1 | ONTAP 9.8 |
|---|--------------|--------------|--------------|--------------|-------------|-----------|
| Support for volumes transitioned from Data ONTAP 7-Mode | X            | X            | X            | X            | X           |           |
| Ability to customize inactive period in System Manager  | X            | X            | X            | X            | X           |           |
| Volume-level Activity Tracking                          | X            | X            | X            | X            |             |           |
| Download Activity Tracking data to CSV                  | X            | X            | X            | X            |             |           |
| SVM-level Activity Tracking                             | X            | X            | X            |              |             |           |
| Timeline  | X            | X            | X            |              |             |           |
| Usage Analytics   | X            | X            |              |              |             |           |
| Option to enable File System Analytics by default       | X            |              |              |              |             |           |

### Learn more about File System Analytics

## ONTAP File System Analytics

Daniel Tennant  
 Director of Software Engineering  
 December 13, 2020

© 2020 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL —






### Further Reading

- [TR 4687: Best-practice guidelines for ONTAP File System Analytics](#)
- [Knowledge Base: High or fluctuating latency after turning on NetApp ONTAP File System Analytics](#)

### Enable File System Analytics

To collect and display usage data such as capacity analytics, you need to enable File

# System Analytics on a volume.

## About this task

- Beginning with ONTAP 9.8, you can enable File System Analytics on a new or existing volume. If you upgrade a system to ONTAP 9.8 or later, ensure that all upgrade processes have completed before you enable File System Analytics.
- Depending on the size and contents of the volume, enabling analytics may take time while ONTAP processes existing data in the volume. System Manager displays progress and presents analytics data when complete. If you need more precise information about initialization progress, you can use the ONTAP CLI command `volume analytics show`.

## About this task

Depending on the size and contents of the volume, enabling analytics may take time while ONTAP processes existing data in the volume. System Manager displays progress and presents analytics data when complete. If you need more precise information about initialization progress, you can use the ONTAP CLI command `volume analytics show`.

For additional considerations related to the initialization scan, see [Scan considerations](#).

## Steps

You can enable File System Analytics with ONTAP System Manager or the CLI.

### System Manager

| In ONTAP 9.8 and 9.9.1   | Beginning in ONTAP 9.10.1   |
|--|---|
| <ol style="list-style-type: none"><li>1. Select <b>Storage &gt; Volumes</b>.</li><li>2. Select the desired volume, then select <b>Explorer</b>.</li><li>3. Select <b>Enable Analytics</b> or <b>Disable Analytics</b>.</li></ol> | <ol style="list-style-type: none"><li>1. Select <b>Storage &gt; Volumes</b>.</li><li>2. Select the desired volume. From the individual volume menu, select <b>File System &gt; Explorer</b>.</li><li>3. Select <b>Enable Analytics</b> or <b>Disable Analytics</b>.</li></ol> |

### CLI

#### Enable File System Analytics with the CLI

1. Run the following command:  

```
volume analytics on -vserver svm_name -volume volume_name [-foreground {true|false}]
```

By default, the command runs in the foreground; ONTAP displays progress and presents analytics data when complete. If you need more precise information, you can run the command in the background by using the `-foreground false` option and then use the `volume analytics show` command to display initialization progress in the CLI.
2. After successfully enabling File System Analytics, use System Manager or the ONTAP REST API to display the analytic data.

## Modify default File System Analytics settings

Beginning in ONTAP 9.13.1, you can modify SVM or clusters settings to enable File System Analytics by default on new volumes.

## System Manager

If you are using System Manager, you can modify the storage VM or cluster settings to enable capacity analytics and Activity Tracking at volume creation by default. Default enablement only applies to volumes created after you modify the settings, not existing volumes.

### Modify File System Analytics settings on a cluster

1. In System Manager, navigate to **Cluster settings**.
2. In **Cluster settings**, review the File System Settings tab. To modify the settings, select the  icon.
3. In the **Activity Tracking** field, enter the names of the SVMs to enable Activity Tracking for by default. Leaving the field blank will leave Activity Tracking disabled on all SVMs.

Uncheck the **Enable on new storage VMs** box to disable Activity Tracking by default on new storage VMs.

4. In the **Analytics** field, enter the names of the storage VMs you want capacity analytics enabled for by default. Leaving the field blank will leave capacity analytics disabled on all SVMs.

Uncheck the **Enable on new storage VMs** box to disable capacity analytics by default on new storage VMs.

5. Select **Save**.

### Modify File System Analytics settings on an SVM

1. Select the SVM you want to modify then **Storage VM settings**.
2. In the **File System Analytics** card, use the toggles to enable or disable Activity Tracking and capacity analytics for all new volumes on the storage VM.

## CLI

You can configure the storage VM to enable File System Analytics by default on new volumes using the ONTAP CLI.

### Enable File System Analytics by default on an SVM

1. Modify the SVM to enable capacity analytics and Activity Tracking by default on all newly created volumes:  

```
vserver modify -vserver svm_name -auto-enable-activity-tracking true -auto-enable-analytics true
```

## View file system activity

After File System Analytics (FSA) is enabled, you can view the root directory contents of a selected volume sorted by the space used in each subtree.

Select any file system object to browse the file system and to display detailed information about each object in a directory. Information about directories can also be displayed graphically. Over time, historical data is displayed for each subtree. Space used is not sorted if there are more than 3000 directories.

## Explorer

The File System Analytics **Explorer** screen consists of three areas:

- Tree view of directories and subdirectories; expandable list showing name, size, modify history, and access history.
- Files; showing name, size, and accessed time for the object selected in the directory list.
- Active and inactive data comparison for the object selected in the directory list.

Beginning with ONTAP 9.9.1, you can customize the range to be reported. The default value is one year. Based on these customizations, you can take corrective actions, such as moving volumes and modifying the tiering policy.

Accessed time is shown by default. However, if the volume default has been altered from the CLI (by setting the `-atime-update` option to `false` with the `volume modify` command), then only last modified time is shown. For example:

- The tree view will not display the **access history**.
- The files view will be altered.
- The active/inactive data view will be based on modified time (`mtime`).

Using these displays, you can examine the following:

- File system locations consuming the most space
- Detailed information about a directory tree, including file and subdirectory count within directories and subdirectories
- File system locations that contain old data (for example, scratch, temp, or log trees)

Keep the following points in mind when interpreting FSA output:

- FSA show where and when your data is in use, not how much data is being processed. For example, large space consumption by recently accessed or modified files does not necessarily indicate high system processing loads.
- The way that the **Volume Explorer** tab calculates space consumption for FSA might differ from other tools. In particular, there could be significant differences compared to the consumption reported in the **Volume Overview** if the volume has storage efficiency features enabled. This is because the **Volume Explorer** tab does not include efficiency savings.
- Due to space limitations in the directory display, it is not possible to view a directory depth greater than 8 levels in the *List View*. To view directories more than 8 levels deep, you must switch to *Graphical View*, locate the desired directory, then switch back to *List View*. This will allow additional screen space in the display.

## Steps

1. View the root directory contents of a selected volume:

| In ONTAP 9.8 and 9.9.1  | Beginning in ONTAP 9.10.1  |
|---|--|
| Click <b>Storage &gt; Volumes</b> , select the desired volume, then click <b>Explorer</b> . | Select <b>Storage &gt; Volumes</b> , select the desired volume. From the individual volume menu, select <b>File System &gt; Explorer</b> . |

## Enable Activity Tracking

Beginning with ONTAP 9.10.1, File System Analytics includes an Activity Tracking feature that allows you to identify hot objects and download the data as a CSV file. Beginning with ONTAP 9.11.1, Activity Tracking is expanded to the SVM scope. Also beginning in ONTAP 9.11.1, System Manager features a timeline for Activity Tracking, allowing you to look through up to five minutes of Activity Tracking data.

Activity Tracking enables monitoring in four categories:

- Directories
- Files
- Clients
- Users

For each category monitored, Activity Tracking will display read IOPs, write IOPs, read throughputs, and write throughputs. Queries on Activity Tracking refresh every 10 to 15 seconds pertaining to hot spots seen in the system over the previous five-second interval.

Activity tracking information is approximate, and the accuracy of the data depends on the distribution of the incoming I/O traffic.

When viewing Activity Tracking in System Manager at the volume level, only the menu of the expanded volume will actively refresh. If the view of any volumes are collapsed, they will not refresh until the volume display is expanded. You can stop the refreshes with the **Pause Refresh** button. Activity data can be downloaded in a CSV format that will display all the point-in-time data captured for the selected volume.

With the timeline feature available beginning in ONTAP 9.11.1, you can keep a record of hotspot activity on a volume or SVM, continuously updating approximately every five seconds and retaining the previous five minutes of data. Timeline data is only retained for fields that are visible area of the page. If you collapse a tracking category or scroll so the timeline is out of view, the timeline will stop collecting data. By default, timelines are disabled and will automatically be disabled when you navigate away from the Activity tab.

### Enable Activity Tracking for a single volume

You can enable Activity Tracking with ONTAP System Manager or the CLI.

#### About this task

If you use RBAC with the ONTAP REST API or System Manager, you will need to create custom roles to manage access to Activity Tracking. See [Role-based access control](#) for this process.

## System Manager

### Steps

1. Select **Storage > Volumes**. Select the desired volume. From the individual volume menu, select File System and then select the Activity tab.
2. Ensure **Activity Tracking** is turned on to view individual reports on top directories, files, clients, and users.
3. To analyze data in greater depth without refreshes, select **Pause Refresh**. You can download the data to have a CSV record of the report as well.

## CLI

### Steps

1. Enable Activity Tracking:

```
volume activity-tracking on -vsserver svm_name -volume volume_name
```

2. Check if the Activity Tracking state for a volume is on or off with the command:

```
volume activity-tracking show -vsserver svm_name -volume volume_name -state
```

3. Once enabled, use ONTAP System Manager or the ONTAP REST API to display Activity Tracking data.

## Enable Activity Tracking for multiple volumes

You can enable Activity Tracking for multiple volumes at once with System Manager.

### About this task

If you use RBAC with the ONTAP REST API or System Manager, you will need to create custom roles to manage access to Activity Tracking. See [Role-based access control](#) for this process.



## System Manager

### Enable for specific volumes

1. Select **Storage > Volumes**. Select the desired volume. From the individual volume menu, select File System and then select the Activity tab.
2. Select the volumes that you want to enable Activity Tracking on. At the top of the volume list, select the **More Options** button. Select **Enable Activity Tracking**.
3. To view Activity Tracking at the SVM level, select the specific SVM you would like to view from **Storage > Volumes**. Navigate to the File System tab then Activity and you will see data for the volumes that have Activity Tracking enabled.

### Enable for all volumes

1. Select **Storage > Volumes**. Select an SVM from the menu.
2. Navigate to the **File System** tab, choose the **More** tab to enable Activity Tracking on all volumes in the SVM.

## CLI

Beginning in ONTAP 9.13.1, you can enable Activity Tracking for multiple volumes using the ONTAP CLI.

### Steps

1. Enable Activity Tracking:

```
volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
```

Use **\*** to enable Activity Tracking for all volumes on the specified storage VM.

Use **!** followed by volume names to enable Activity Tracking for all volumes on the SVM except the named volumes.

2. Confirm the operation succeeded:

```
volume show -fields activity-tracking-state
```

3. Once enabled, use ONTAP System Manager or the ONTAP REST API to display Activity Tracking data.

## Enable usage analytics

Tracking directories by size enables you to capture important data about the directories in a volume using the most space. Tracking directories by size is available beginning in ONTAP 9.12.1 and provides:

- The total number of directories in the volume
- The total number of files in the volume
- A bar chart identifying the largest directories in the volume by size in descending order

Tracking for large directories will refresh every 15 minutes. File System Analytics limits reporting of large directories to the 25 directories consuming the most space.

You can monitor the most recent refresh by checking the **Last Refreshed** timestamp at the top of the page. You can additionally download tracking data to an Excel workbook with the **Download** button. The download operation will run in the background and present the most recently reported information for the selected volume.

If the scan returns without any results, ensure the volume is online. Events such as SnapRestore will cause File System Analytics to rebuild its list of large directories.

**Steps**

- 1. Select **Storage > Volumes**. Select the desired volume.
- 2. From the individual volume menu, select **File System**. Then select the **Usage** tab.
- 3. Toggle the **Analytics** switch to enable usage analytics.
- 4. System Manager will display a bar graph identifying the directories with the largest size in descending order.



ONTAP might display partial data or no data at all while the list of top directories is being collected. The progress of the scan can be in the **Usage** tab that displays during the scan.

Gain more insights about any directory by selecting the directory to go to the the Explorer tab. For more information about the **Explorer** tab, refer to [View activity on a file system](#).

**Take corrective action based on analytics**

Beginning with ONTAP 9.9.1, you can take corrective actions based on current data and desired outcomes directly from the File System Analytics displays.

When analytics are enabled, you can take the following actions:

- Delete directories and files  
  
In the Explorer display, you can select directories or individual files to delete. Directories are deleted with low-latency fast directory delete functionality. (Fast directory delete is also available beginning in ONTAP 9.9.1 without analytics enabled.)
- Assign media cost in storage tiers to compare costs of inactive data storage locations  
  
Media cost is a value that you assign based on your evaluation of storage costs, represented as your choice of currency per GB. When set, System Manager uses the assigned media cost to project estimated savings when you move volumes.  
  
The media cost you set is not persistent; it can only be set for a single browser session.
- Move volumes to reduce storage costs  
Based on analytics displays and media cost comparisons, you can move volumes to less expensive storage in local tiers.  
  
Only one volume at a time can be compared and moved.

|                           |                     |
|---------------------------|---------------------|
| To perform this action... | Take these steps... |
|---------------------------|---------------------|

|                                       |  |
|---------------------------------------|--|
| Delete directories or files           | <ol style="list-style-type: none"> <li>1. Click <b>Storage &gt; Volumes</b>, then click <b>Explorer</b>.<br/><br/>When you hover over a file or folder, the option to delete appears. You can only delete one object at a time.</li> </ol> <div>  <p>When directories and files are deleted, the new storage capacity values are not displayed immediately.</p> </div>  |
| Enable media cost comparison          | <ol style="list-style-type: none"> <li>1. Click <b>Storage &gt; Tiers</b>, then click <b>Set Media Cost</b> in the desired local tier (aggregate) tiles.<br/><br/>Be sure to select active and inactive tiers to enable comparison.</li> <li>2. Enter a currency type and amount.<br/><br/>When you enter or change the media cost, the change is made in all media types.</li> </ol>  |
| Move volumes to a less expensive tier | <ol style="list-style-type: none"> <li>1. After enabling media cost display, click <b>Storage &gt; Tiers</b>, then click <b>Volumes</b>.</li> <li>2. To compare destination options for a volume, click  for the volume, then click <b>Move</b>.</li> <li>3. In the <b>Select Destination Local Tier</b> display, select destination tiers to display the estimated cost difference.</li> <li>4. After comparing options, select the desired tier and click <b>Move</b>.</li> </ol> |

## Role-based access control with File System Analytics

Beginning in ONTAP 9.12.1, ONTAP includes a predefined role-based access control (RBAC) role called `admin-no-fsa`. The `admin-no-fsa` role grants administrator-level privileges but prevents the user from performing operations related to the `files` endpoint (i.e. File System Analytics) in the ONTAP CLI, REST API, and in System Manager.

For more information on the `admin-no-fsa` role, refer to [Predefined roles for cluster administrators](#).

If you are using a version of ONTAP released prior to ONTAP 9.12.1, you will need to create a dedicated role to control access to File System Analytics. In versions of ONTAP prior to ONTAP 9.12.1, you must configure RBAC permissions through the ONTAP CLI or ONTAP REST API.

## System Manager

Beginning in ONTAP 9.12.1, you can configure RBAC permissions for File System Analytics using System Manager.

### Steps

1. Select **Cluster > Settings**. Under **Security**, navigate to **Users and Roles** and select [➔](#).
2. Under **Roles**, select [+ Add](#).
3. Provide a name for the role. Under Role Attributes, configure the access or restrictions for the user role by providing the appropriate [API endpoints](#). See the table below for primary paths and secondary paths to configure File System Analytics access or restrictions.

| Restriction                          | Primary Path         | Secondary Path  |
|--------------------------------------|----------------------|---|
| Activity Tracking on volumes         | /api/storage/volumes | <ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul> |
| Activity Tracking on SVMs            | /api/svm/svms        | <ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul> |
| All File System Analytics operations | /api/storage/volumes | /:uuid/files  |

You can use `/*` instead of an UUID to set the policy for all volumes or SVMs at the endpoint.

Choose the access privileges for each endpoint.

4. Select **Save**.
5. To assign the role to a user or users, see [Control administrator access](#).

### CLI

If you are using a version of ONTAP released prior to ONTAP 9.12.1, use the ONTAP CLI to create a custom-role.

### Steps

### 1. Create a default role to have access to all features.

This needs to be done before creating the restrictive role to ensure the role is only restrictive on the Activity Tracking:

```
security login role create -cmddirname DEFAULT -access all -role
storageAdmin
```

### 2. Create the restrictive role:

```
security login role create -cmddirname "volume file show-disk-usage"
-access none -role storageAdmin
```

### 3. Authorize roles to access the SVM's web services:

- `rest` for REST API calls
- `security` for password protection
- `sysmgr` for System Manager access

```
vserver services web access create -vserver svm-name -name _ -name rest
-role storageAdmin
```

```
vserver services web access create -vserver svm-name -name security
-role storageAdmin
```

```
vserver services web access create -vserver svm-name -name sysmgr -role
storageAdmin
```

### 4. Create a user.

You must issue a distinct create command for each application you would like to apply to the user. Calling create multiple times on the same user simply applies all the applications to that one user and does not create a new user each time. The `http` parameter for application type applies for the ONTAP REST API and System Manager.

```
security login create -user-or-group-name storageUser -authentication
-method password -application http -role storageAdmin
```

### 5. With the new user credentials, you can now log in to System Manager or use the ONTAP REST API to access File Systems Analytics data.

#### More information

- [Predefined roles for cluster administrators](#)
- [Control administrator access with System Manager](#)
- [Learn more about RBAC roles and the ONTAP REST API](#)

## Considerations for File System Analytics

You should be aware of certain usage limits and potential performance impacts associated with implementing File System Analytics.

## SVM-protected relationships

If you have enabled File System Analytics on volumes whose containing SVM is in a protection relationship, the analytics data is not replicated to the destination SVM. If the source SVM must be resynchronized in a recovery operation, you must manually reenable analytics on desired volumes after recovery.

## Performance considerations

In some cases, enabling File System Analytics could negatively impact performance during the initial metadata collection. This is most typically seen on systems that are at maximum utilization. To avoid enabling analytics on such systems, you can use ONTAP System Manager performance monitoring tools.

If you experience a notable increase in latency, refer to the Knowledge Base article [High or fluctuating latency after turning on NetApp ONTAP File System Analytics](#).

## Scan considerations

When you enable capacity analytics, ONTAP conducts an initialization scan. The scan accesses metadata for all files in volumes for which capacity analytics is enabled. No file data is read during the scan.

After the scan completes, File System Analytics is continuously updated in real time as the filesystem changes without the need to run the scan again.

The time required for the scan is proportional to the number of directories and files on the volume. Because the scan collects metadata, file size does not impact the scan time.

For more information about the initialization scan, see [TR-4867: Best practice guidelines for File System Analytics](#).

## Best practices

You should start the scan on volumes that do not share aggregates. You can see which aggregates are currently hosting which volumes using the command:

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

While the scan runs, volumes continue to serve client traffic. It's recommended you start the scan during periods where you anticipate lower client traffic.

If client traffic increases, it will consume system resources and cause the scan to take longer.

Beginning in ONTAP 9.12.1, you can pause data collection in System Manager and with the ONTAP CLI.

- If you are using the ONTAP CLI:
  - You can pause data collection with the command: `volume analytics initialization pause -vserver svm_name -volume volume_name`
  - Once client traffic has slowed, you can resume data collection with the command: `volume analytics initialization resume -vserver svm_name -volume volume_name`
- If you are using System Manager, in the **Explorer** view of the volume menu, you use the **Pause Data Collection** and **Resume Data Collection** buttons to manage the scan.

# EMS configuration

## EMS configuration overview

You can configure ONTAP 9 to send important EMS (Event Management System) event notifications directly to an email address, syslog server, Simple Management Network Protocol (SNMP) trap host, or webhook application so that you are immediately notified of system issues that require prompt attention.

Because important event notifications are not enabled by default, you need to configure the EMS to send notifications to either an email address, a syslog server, an SNMP trap host, or webhook application.

Review release-specific versions of the [ONTAP 9 EMS Reference](#).

If your EMS event mapping uses deprecated ONTAP command sets (such as event destination, event route), it's recommended that you update your mapping. [Learn how to update your EMS mapping from deprecated ONTAP commands](#).

## Configure EMS event notifications and filters with System Manager

You can use System Manager to configure how the Event Management System (EMS) delivers event notifications so that you can be notified of system issues that require your prompt attention.

| ONTAP version          | With System Manager, you can...  |
|------------------------|--|
| ONTAP 9.12.1 and later | Specify Transport Layer Security (TLS) protocol when sending events to remote syslog servers.  |
| ONTAP 9.10.1 and later | Configure email addresses, syslog servers, and webhook applications, as well as SNMP trap hosts.   |
| ONTAP 9.7 to 9.10.0    | Configure only SNMP trap hosts. You can configure other EMS destination with the ONTAP CLI. See <a href="#">EMS configuration overview</a> . |

You can perform the following procedures:

- [Add an EMS event notification destination](#)
- [Create a new EMS event notification filter](#)
- [Edit an EMS event notification destination](#)
- [Edit an EMS event notification filter](#)
- [Delete an EMS event notification destination](#)
- [Delete an EMS event notification filter](#)

### Related information

- [ONTAP EMS Reference](#)
- [Using the CLI to configure SNMP trap hosts to receive event notifications](#)

## Add an EMS event notification destination

You can use System Manager to specify to where you want EMS messages sent.

Beginning with ONTAP 9.12.1, EMS events can be sent to a designated port on a remote syslog server via the Transport Layer Security (TLS) protocol. For details, see the [event notification destination create man page](#).

### Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click , then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Events Destinations** tab.
4. Click  **Add**.
5. Specify a name, an EMS destination type, and filters.



If needed, you can add a new filter. Click **Add a New Event Filter**.

6. Depending on the EMS destination type you selected, specify the following:

| To configure...                          | Specify or select...   |
|--|--|
| SNMP traphost                            | <ul style="list-style-type: none"><li>• Traphost name</li></ul>  |
| Email<br>(Beginning with 9.10.1)         | <ul style="list-style-type: none"><li>• Destination email address</li><li>• Mail server</li><li>• From email address</li></ul>   |
| Syslog server<br>(Beginning with 9.10.1) | <ul style="list-style-type: none"><li>• Host name or IP address of the server</li><li>• Syslog port (beginning with 9.12.1)</li><li>• Syslog transport (beginning with 9.12.1)</li></ul> <p>Selecting <b>TCP Encrypted</b> enables the Transport Layer Security (TLS) protocol. If no value is entered for <b>Syslog port</b>, a default is used based on the <b>Syslog transport</b> selection.</p> |
| Webhook<br>(Beginning with 9.10.1)       | <ul style="list-style-type: none"><li>• Webhook URL</li><li>• Client authentication (select this option to specify a client certificate)</li></ul>   |

## Create a new EMS event notification filter

Beginning with ONTAP 9.10.1, you can use System Manager to define new customized filters that specify the rules for handling EMS notifications.

### Steps

1. Click **Cluster > Settings**.





2. In the **Notifications Management** section, click , then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Event Filters** tab.
4. Click  **Add**.
5. Specify a name, and select whether you want to copy rules from an existing event filter or add new rules.
6. Depending on your choice, perform the following steps:

| If you choose....                            | Then, perform these steps...   |
|--|--|
| <b>Copy rules from existing event filter</b> | <ol style="list-style-type: none"> <li>1. Select an existing event filter.</li> <li>2. Modify the existing rules.</li> <li>3. Add other rules, if needed, by clicking  <b>Add</b>.</li> </ol> |
| <b>Add new rules</b>                         | Specify the type, name pattern, severities, and SNMP trap type for each new rule.  |

### Edit an EMS event notification destination

Beginning with ONTAP 9.10.1, you can use System Manager to change the event notification destination information.

#### Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click , then click **View Event Destinations**.
3. On the **Notifications Management** page, select the **Events Destinations** tab.
4. Next to the name of the event destination, click , then click **Edit**.
5. Modify the event destination information, then click **Save**.



### Edit an EMS event notification filter

Beginning with ONTAP 9.10.1, you can use System Manager to modify customized filters to change how event notifications are handled.



You cannot modify system-defined filters.

#### Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click , then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Event Filters** tab.
4. Next to the name of the event filter, click , then click **Edit**.
5. Modify the event filter information, then click **Save**.

### Delete an EMS event notification destination

Beginning with ONTAP 9.10.1, you can use System Manager to delete an EMS event notification destination.



You cannot delete SNMP destinations.

### Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click , then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Events Destinations** tab.
4. Next to the name of the event destination, click , then click **Delete**.

### Delete an EMS event notification filter

Beginning with ONTAP 9.10.1, you can use System Manager to delete customized filters.



You cannot delete system-defined filters.

### Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click , then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Event Filters** tab.
4. Next to the name of the event filter, click , then click **Delete**.

## Configure EMS event notifications with the CLI

### EMS configuration workflow

You must configure important EMS event notifications to be sent either as email, forwarded to a syslog server, forwarded to an SNMP traphost, or forwarded to a webhook application. This helps you to avoid system disruptions by taking corrective actions in a timely manner.

#### About this task

If your environment already contains a syslog server for aggregating the logged events from other systems, such as servers and applications, then it is easier to use that syslog server also for important event notifications from storage systems.

If your environment does not already contain a syslog server, then it is easier to use email for important event notifications.

If you already forward event notifications to an SNMP traphost, then you might want to monitor that traphost for important events.



### Choices

- Set EMS to send event notifications.

| If you want...  | Refer to this...   |
|---|--|
| The EMS to send important event notifications to an email address           | <a href="#">Configure important EMS events to send email notifications</a>                       |
| The EMS to forward important event notifications to a syslog server         | <a href="#">Configure important EMS events to forward notifications to a syslog server</a>       |
| If you want the EMS to forward event notifications to an SNMP traphost      | <a href="#">Configure SNMP traphosts to receive event notifications</a>                          |
| If you want the EMS to forward event notifications to a webhook application | <a href="#">Configure important EMS events to forward notifications to a webhook application</a> |

### Configure important EMS events to send email notifications

To receive email notifications of the most important events, you must configure the EMS to send email messages for events that signal important activity.

#### What you'll need

DNS must be configured on the cluster to resolve the email addresses.

### About this task

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

### Steps

1. Configure the event SMTP mail server settings:

```
event config modify -mail-server mailhost.your_domain -mail-from  
cluster_admin@your_domain
```

2. Create an email destination for event notifications:

```
event notification destination create -name storage-admins -email  
your_email@your_domain
```

3. Configure the important events to send email notifications:

```
event notification create -filter-name important-events -destinations storage-  
admins
```

### Configuring important EMS events to forward notifications to a syslog server

To log notifications of the most severe events on a syslog server, you must configure the EMS to forward notifications for events that signal important activity.

### What you'll need

DNS must be configured on the cluster to resolve the syslog server name.

### About this task

If your environment does not already contain a syslog server for event notifications, you must first create one. If your environment already contains a syslog server for logging events from other systems, then you might want to use that one for important event notifications.

You can perform this task any time the cluster is running by entering the commands on the ONTAP CLI.

Beginning with ONTAP 9.12.1, EMS events can be sent to a designated port on a remote syslog server via the Transport Layer Security (TLS) protocol. Two new parameters are available:

#### **tcp-encrypted**

When `tcp-encrypted` is specified for the `syslog-transport`, ONTAP verifies the identity of the destination host by validating its certificate. The default value is `udp-unencrypted`.

#### **syslog-port**

The default value `syslog-port` parameter depends on the setting for the `syslog-transport` parameter. If `syslog-transport` is set to `tcp-encrypted`, `syslog-port` has the default value 6514.

For details, see the `event notification destination create` man page.

### Steps

1. Create a syslog server destination for important events:

```
event notification destination create -name syslog-ems -syslog syslog-server-  
address -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}
```

Beginning with ONTAP 9.12.1, the following values can be specified for `syslog-transport`:

- `udp-unencrypted` - User Datagram Protocol with no security
- `tcp-unencrypted` - Transmission Control Protocol with no security
- `tcp-encrypted` - Transmission Control Protocol with Transport Layer Security (TLS)

The default protocol is `udp-unencrypted`.

2. Configure the important events to forward notifications to the syslog server:

```
event notification create -filter-name important-events -destinations syslog-  
ems
```

## Configure SNMP traphosts to receive event notifications

To receive event notifications on an SNMP traphost, you must configure a traphost.

### What you'll need

- SNMP and SNMP traps must be enabled on the cluster.



SNMP and SNMP traps are enabled by default.

- DNS must be configured on the cluster to resolve the traphost names.

### About this task

If you do not already have an SNMP traphost configured to receive event notifications (SNMP traps), you must add one.

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

### Step

1. If your environment does not already have an SNMP traphost configured to receive event notifications, add one:

```
system snmp traphost add -peer-address snmp_traphost_name
```

All event notifications that are supported by SNMP by default are forwarded to the SNMP traphost.

## Configure important EMS events to forward notifications to a webhook application

You can configure ONTAP to forward important event notifications to a webhook application. The configuration steps needed depend on the level of security you choose.

### Prepare to configure EMS event forwarding

There are several concepts and requirements you should consider before configuring ONTAP to forward event notifications to a webhook application.

## Webhook application

You need a webhook application capable of receiving the ONTAP event notifications. A webhook is a user-defined callback routine that extends the capability of the remote application or server where it runs. Webhooks are called or activated by the client (in this case ONTAP) by sending an HTTP request to the destination URL. Specifically, ONTAP sends an HTTP POST request to the server hosting the webhook application along with the event notification details formatted in XML.

## Security options

There are several security options available depending on how the Transport Layer Security (TLS) protocol is used. The option you choose determines the required ONTAP configuration.



TLS is a cryptographic protocol that is widely used on the internet. It provides privacy as well as data integrity and authentication using one or more public key certificates. The certificates are issued by trusted certificate authorities.

## HTTP

You can use HTTP to transport the event notifications. With this configuration, the connection is not secure. The identities of the ONTAP client and webhook application are not verified. Further, the network traffic is not encrypted or protected. See [Configure a webhook destination to use HTTP](#) for the configuration details.

## HTTPS

For additional security, you can install a certificate at the server hosting the webhook routine. The HTTPS protocol is used by ONTAP to verify the identity of the webhook application server as well as by both parties to ensure the privacy and integrity of the network traffic. See [Configure a webhook destination to use HTTPS](#) for the configuration details.

## HTTPS with mutual authentication

You can further enhance the HTTPS security by installing a client certificate at the ONTAP system issuing the webhook requests. In addition to ONTAP verifying the identity of the webhook application server and protecting the network traffic, the webhook application verifies the identity of the ONTAP client. This two-way peer authentication is known as *Mutual TLS*. See [Configure a webhook destination to use HTTPS with mutual authentication](#) for the configuration details.

## Related information

- [The Transport Layer Security \(TLS\) Protocol Version 1.3](#)

## Configure a webhook destination to use HTTP

You can configure ONTAP to forward event notifications to a webhook application using HTTP. This is the least secure option but the simplest to set up.

## Steps

1. Create a new destination `restapi-ems` to receive the events:

```
event notification destination create -name restapi-ems -rest-api-url  
http://<webhook-application>
```

In the above command, you must use the **HTTP** scheme for the destination.

2. Create a notification linking the `important-events` filter with the `restapi-ems` destination:

```
event notification create -filter-name important-events -destinations restapi-ems
```

### Configure a webhook destination to use HTTPS

You can configure ONTAP to forward event notifications to a webhook application using HTTPS. ONTAP uses the server certificate to confirm the identity of the webhook application as well as secure the network traffic.

#### Before you begin

- Generate a private key and certificate for the webhook application server
- Have the root certificate available to install in ONTAP

#### Steps

1. Install the appropriate server private key and certificates at the server hosting your webhook application. The specific configuration steps are dependent on the server.
2. Install the server root certificate in ONTAP:

```
security certificate install -type server-ca
```

The command will ask for the certificate.

3. Create the `restapi-ems` destination to receive the events:

```
event notification destination create -name restapi-ems -rest-api-url https://<webhook-application>
```

In the above command, you must use the **HTTPS** scheme for the destination.

4. Create the notification that links the `important-events` filter with the new `restapi-ems` destination:

```
event notification create -filter-name important-events -destinations restapi-ems
```

### Configure a webhook destination to use HTTPS with mutual authentication

You can configure ONTAP to forward event notifications to a webhook application using HTTPS with mutual authentication. With this configuration there are two certificates. ONTAP uses the server certificate to confirm the identity of the webhook application and secure the network traffic. In addition, the application hosting the webhook uses the client certificate to confirm the identity of the ONTAP client.

#### Before you begin

You must do the following before configuring ONTAP:

- Generate a private key and certificate for the webhook application server
- Have the root certificate available to install in ONTAP
- Generate a private key and certificate for the ONTAP client

#### Steps

1. Perform the first two steps in the task [Configure a webhook destination to use HTTPS](#) to install the server certificate so that ONTAP can verify the identity of the server.

2. Install the appropriate root and intermediate certificates at the webhook application to validate the client certificate.
3. Install the client certificate in ONTAP:

```
security certificate install -type client
```

The command will ask for the private key and certificate.

4. Create the `restapi-ems` destination to receive the events:

```
event notification destination create -name restapi-ems -rest-api-url  
https://<webhook-application> -certificate-authority <issuer of the client  
certificate> -certificate-serial <serial of the client certificate>
```

In the above command, you must use the **HTTPS** scheme for destination.

5. Create the notification that links the `important-events` filter with the new `restapi-ems` destination:

```
event notification create -filter-name important-events -destinations restapi-  
ems
```

## Update deprecated EMS event mapping

### EMS event mapping models

Prior to ONTAP 9.0, EMS events could only be mapped to event destinations based on event name pattern matching. The ONTAP command sets (`event destination`, `event route`) that use this model continue to be available in the latest versions of ONTAP, but they have been deprecated starting with ONTAP 9.0.

Beginning with ONTAP 9.0, the best practice for ONTAP EMS event destination mapping is to use the more scalable event filter model in which pattern matching is done on multiple fields, using the `event filter`, `event notification`, and `event notification destination` command sets.

If your EMS mapping is configured using the deprecated commands, you should update your mapping to use the `event filter`, `event notification`, and `event notification destination` command sets.

There are two types of event destinations:

1. **System-generated destinations:** There are five system-generated event destinations (created by default)

- `allevents`
- `asup`
- `criticals`
- `pager`
- `traphost`

Some of the system-generated destinations are for special purpose. For example, the `asup` destination routes `callhome.*` events to the AutoSupport module in ONTAP to generate AutoSupport messages.



2. **User-created destinations:** These are manually created using the event destination create command.

```
cluster-1::event*> destination show
```

| Name | Mail Dest. | SNMP Dest. | Syslog Dest. | Hide |
|------|------------|------------|--------------|------|
|------|------------|------------|--------------|------|

Params

|           |       |       |       |       |
|-----------|-------|-------|-------|-------|
| -----     | ----- | ----- | ----- | ----- |
| -----     |       |       |       |       |
| allevents | -     | -     | -     |       |
| false     |       |       |       |       |
| asup      | -     | -     | -     |       |
| false     |       |       |       |       |
| criticals | -     | -     | -     |       |
| false     |       |       |       |       |
| pager     | -     | -     | -     |       |
| false     |       |       |       |       |
| traphost  | -     | -     | -     |       |
| false     |       |       |       |       |

5 entries were displayed.

+

```
cluster-1::event*> destination create -name test -mail test@xyz.com
```

This command is deprecated. Use the "event filter", "event notification destination" and "event notification" commands, instead.

+

```
cluster-1::event*> destination show
```

+

Hide

| Name | Mail Dest. | SNMP Dest. | Syslog Dest. |
|------|------------|------------|--------------|
|------|------------|------------|--------------|

Params

|           |              |       |       |
|-----------|--------------|-------|-------|
| -----     | -----        | ----- | ----- |
| -----     |              |       |       |
| allevents | -            | -     | -     |
| false     |              |       |       |
| asup      | -            | -     | -     |
| false     |              |       |       |
| criticals | -            | -     | -     |
| false     |              |       |       |
| pager     | -            | -     | -     |
| false     |              |       |       |
| test      | test@xyz.com | -     | -     |
| false     |              |       |       |
| traphost  | -            | -     | -     |
| false     |              |       |       |

6 entries were displayed.

In the deprecated model, EMS events are individually mapped to a destination using the `event route add-destinations` command.

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.
```

```
cluster-1::event*> route show -message-name raid.aggr.*
```

| Time                       |               |              | Freq    |       |
|----------------------------|---------------|--------------|---------|-------|
| Message                    | Severity      | Destinations | Threshd |       |
| Threshd                    |               |              |         |       |
| -----                      | -----         | -----        | -----   | ----- |
| raid.aggr.autoGrow.abort   | NOTICE        | test         | 0       | 0     |
| raid.aggr.autoGrow.success | NOTICE        | test         | 0       | 0     |
| raid.aggr.lock.conflict    | INFORMATIONAL | test         | 0       | 0     |
| raid.aggr.log.CP.count     | DEBUG         | test         | 0       | 0     |

4 entries were displayed.

The new, more scalable EMS event notifications mechanism is based on event filters and event notification destinations. Refer to the following KB article for detailed information on the new event notification mechanism:

- [Overview of Event Management System for ONTAP 9](#)

Legacy routing based model



Event notification based model



## Update EMS event mapping from deprecated ONTAP commands

If your EMS event mapping is currently configured using the deprecated ONTAP command sets (event destination, event route), you should follow this procedure to update your mapping to use the event filter, event notification, and event notification destination command sets.

### Steps

1. List all the event destinations in the system using the `event destination show` command.

```
cluster-1::event*> destination show
```

```
Hide
Name          Mail Dest.      SNMP Dest.      Syslog Dest.
Params
-----
-----
allevents      -                -                -
false
asup           -                -                -
false
criticals     -                -                -
false
pager         -                -                -
false
test          test@xyz.com     -                -
false
traphost       -                -                -
false
6 entries were displayed.
```

- For each destination, list the events being mapped to it using the `event route show -destinations <destination name>` command.

```
cluster-1::event*> route show -destinations test
```

```
Time
Message          Severity      Destinations  Freq
Threshd
-----
-----
raid.aggr.autoGrow.abort      NOTICE      test          0          0
raid.aggr.autoGrow.success    NOTICE      test          0          0
raid.aggr.lock.conflict       INFORMATIONAL test          0          0
raid.aggr.log.CP.count        DEBUG        test          0          0
4 entries were displayed.
```

- Create a corresponding event filter which includes all these subsets of events. For example, if you want to include only the `raid.aggr.*` events, use a wildcard for the message-name parameter when creating the filter. You can also create filters for single events.



You can create up to 50 event filters.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule      Rule      Message Name      SNMP Trap Type
Severity
      Position Type
-----
test_events
      1      include  raid.aggr.*      *      *
      2      exclude  *      *      *
2 entries were displayed.
```

4. Create an event notification destination for each of the event destination endpoints (i.e., SMTP/SNMP/syslog)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name      Type      Destination
-----
dest1      email      test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost  snmp      - (from "system snmp traphost")
2 entries were displayed.
```

5. Create an event notification by mapping the event filter to the event notification destination.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID  Filter Name      Destinations
---
1   default-trap-events  snmp-traphost
2   asup_events         dest1
2 entries were displayed.
```

6. Repeat steps 1-5 for each event destination that has an event route mapping.



Events routed to SNMP destinations should be mapped to the `snmp-traphost` event notification destination. The SNMP traphost destination uses the system configured SNMP traphost.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
      scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>   Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

      Destination Name: snmp-traphost
      Type of Destination: snmp
      Destination: 10.234.166.135 (from "system snmp
traphost")
      Server CA Certificates Present?: -
      Client Certificate Issuing CA: -
      Client Certificate Serial Number: -
      Client Certificate Valid?: -
```

## Copyright information

Copyright © 2023 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, 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) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.