



# **Manage SolidFire Active IQ**

## **SolidFire Active IQ**

NetApp  
October 02, 2025

# Table of Contents

Manage SolidFire Active IQ .....	1
Manage SolidFire Active IQ .....	1
Find more information .....	1
All Clusters View .....	1
All Clusters View .....	1
All Clusters View Dashboard .....	1
Alerts .....	4
Capacity Licensing .....	13
Term Capacity .....	13
Select a cluster .....	14
Single cluster view dashboard .....	14
Reporting options for a selected cluster .....	17
Nodes head .....	22
View SolidFire storage node details .....	22
View NetApp HCI storage and compute node details .....	24
Find more information .....	26
Volumes .....	26
Active Volumes .....	26
Snapshots and Snapshot Schedules .....	27
Volume Performance .....	29
Virtual Volumes .....	31
Virtual Volumes .....	31
Storage Containers .....	32
Protocol Endpoints .....	32
Hosts .....	33
Bindings .....	33
Find more information .....	34
QoS Management .....	34
QoS Management .....	34
Recommendations .....	34
Node Throttling .....	34
Busiest Volumes .....	36
Virtual Machines .....	38
View Virtual Machine details .....	38
Find more information .....	39
VMware Alarms .....	39
Find more information .....	39
All Nodes View .....	39
View information about all nodes .....	40
View information about throttled nodes .....	40
Find more information .....	42

# Manage SolidFire Active IQ

## Manage SolidFire Active IQ

Learn about using [SolidFire Active IQ \(login required\)](#) to monitor cluster capacity and performance:

- [All Clusters View](#)
- [Select a Cluster](#)
- [Nodes](#)
- [Drives](#)
- [Volumes](#)
- [Replication](#)
- [Virtual Volumes](#)
- [QoS Management](#)
- [Virtual Machines \(NetApp HCI clusters only\)](#)
- [VMware alarms \(NetApp HCI clusters only\)](#)
- [All Nodes View](#)

### Find more information

[NetApp Product Documentation](#)

## All Clusters View

### All Clusters View

The **All Clusters View** is the landing page for SolidFire Active IQ.

Learn about what you can access from the **All Clusters View**:

- [All Clusters View dashboard](#)
- [Alerts](#)
- [Capacity Licensing](#)
- [Term Capacity](#)

### Find more information

[NetApp Product Documentation](#)

### All Clusters View Dashboard

## All Clusters View dashboard

On the **Dashboard** page of the **All Clusters View**, you can view performance, capacity, and cluster statistic details about the clusters associated with your account.

Heading	Description
Company	Company name assigned to the cluster.
Cluster	Name assigned to the cluster.
Cluster ID	Assigned cluster number when the cluster is created.
Version	Version of the cluster master running on each node.
Nodes	Number of nodes in the cluster.
Volumes	Number of volumes in the cluster.
Efficiency	The amount of efficiency the system is seeing due to compression, deduplication, and thin provisioning.
Used Block Capacity	Current used capacity of the cluster block.
Faults	Number of currently unresolved faults detected on the cluster.
SVIP	Storage virtual IP address assigned to the cluster.
MVIP	Management Virtual IP address assigned to the cluster.
Last Update	Time and date that the most recent cluster update.
Actions	Options to request upgrade support for a cluster, archive a cluster, and suppress a cluster



If the cluster you are looking for is unavailable, be aware that clusters that have been inactive for 180 days or more are automatically archived. Contact support for further assistance.


### Find more information

[NetApp Product Documentation](#)

## Cluster Actions

On the **Dashboard** page of the **All Clusters View**, you can view the cluster support options about the clusters associated with your account.

### Steps

1. Select **All Clusters View > Overview**.
2. In the **Actions** column, select the  icon for the cluster you want.
3. Select one of the following options:
  - a. **Request Upgrade Support** sends a request for an upgrade of the cluster software. You can select element software, storage firmware, compute firmware, or the management node management services. You enter your contact information, any comments, and a callback time.

Request Support Upgrade Assistance for Cluster

Current Cluster Version: **12.7.0.380**

Element Software
☐

Storage Firmware
☐

Compute Firmware
☐

mNode Management Services
☐

Contact Name \*

Contact Email \*

Contact Phone

Comments

Requested Callback Time \*

2025-09-18 14:18:00
▼

Submit
Cancel

- b. **Archive Cluster** archives the cluster. A window opens providing warnings about the issues around archiving a cluster that might need to be unarchived at a later date.

Archive Cluster

Are you sure you want to archive cluster **SF\_Cluster1** ?

**Notice:**

- Cluster Archival is *not* to be used to temporarily silence a noisy cluster.
- Restoring an archived cluster will have undefined ramifications.
- Future payloads from **SF\_Cluster1** will be ignored. Data will stop being ingested into Active IQ.
- Access to pages for **SF\_Cluster1** will be denied, and it will be removed from the All Cluster Dashboard View.
- Every effort will be made to stop and clear alerts for **SF\_Cluster1** . However, alerts may trigger while archival is being processed.
- The Active IQ development team reserves the right to delete data associated with archived clusters, at any time, and with no notice.

Are you sure you want to continue?

Archive Cluster
Cancel

- c. **Suppress Cluster** stops repeated alerts. You choose alert type, start time, and duration. You can also see currently running alert suppression rules on this window.

**Suppress Alerts for Cluster**

Type: Full

Start Time: 2025-09-15 13:57:00

Duration: 6 hours

☐ Overlap Existing Suppressions

Existing Suppressions

ID	Type	Start Time	End Time
No results found.			

Filter

Suppress Cancel

See [Suppress Cluster Notifications](#) for more information.



If the cluster you are looking for is unavailable, be aware that clusters that have been inactive for 180 days or more are automatically archived. Contact support for further assistance.

Find more information

[NetApp Product Documentation](#)

## Alerts

From the **Alerts** drop-down menu within **All Clusters View**, you can view the alert history, create and manage alert policies, and view and suppress cluster notifications.


Learn about or perform alerts-related tasks:

- [View alerts history](#)
- [Alerts history details](#)
- [View alert policies](#)
- [Create an alert policy](#)
- [Alert policy types](#)
- [Edit an alert policy](#)
- [Delete an alert policy](#)
- [View suppressed clusters](#)
- [Suppress cluster notifications](#)
- [End cluster suppression from a cluster](#)
- [Alert notification email](#)

## View alerts history

You can view the history for either unresolved or resolved alerts.

### Steps

1. Select **Alerts > History**.
2. Select either the **Unresolved** or **Resolved** tab to view the history of alerts for the cluster.
3. (Optional) Select the  icon to export the data to a CSV file.

## Alerts history details

The **History** page in the Alerts drop-down menu within All Clusters View shows up to 10000 entries of alert history, including all unresolved alerts and alerts resolved in the last 30 days.

The following list describes the details that are available to you:

Heading	Description
Alert ID	Unique ID for each alert.
Triggered	The time the alert was triggered in SolidFire Active IQ, not on the cluster itself.
Last Notified	The time the most recent alert email was sent.
Resolved	Shows if the cause of the alert has been resolved.
Resolution Time	The time an issue was resolved.
Policy	This is the user-defined alert policy name.
Severity	Severity assigned at the time the alert policy was created.
Destination	The email address or addresses selected to receive the alert email.
Company	Name of customer associated with the alert.
Cluster	Displays the cluster name for which the alert policy was added.

Heading	Description
Trigger	The user-defined setting that triggered the alert.

## View alert policies

The **Policies** page in the Alerts drop-down menu within All Clusters View shows the following policy information for all clusters.

The following list describes the details that are available to you:

Heading	Description
Policy Name	User-defined alert policy name.
Destination	Email address defined in the alert policy.
Severity	Severity assigned in the alert policy.
Clusters	Number and name of each cluster defined in the alert policy. Select the information icon to reveal associated clusters.
Condition	User-defined setting for when an alert should be triggered.
Suppression Types	<p>Determines which alerts and events are suppressed. The following types are possible:</p> <ul style="list-style-type: none"> <li>• <b>Full:</b> All alerts for the cluster are suppressed for the duration specified. No support cases or email alerts are generated.</li> <li>• <b>Upgrades:</b> Non-critical cluster alerts are suppressed for the duration specified. Critical alerts still generate support cases and emails.</li> <li>• <b>Compute:</b> Alerts that are triggered by VMware on the compute nodes are suppressed.</li> <li>• <b>NodeHardware:</b> Alerts associated with node maintenance are suppressed. For example, swapping out drives or taking nodes offline.</li> <li>• <b>Drive:</b> Alerts associated with drive health are suppressed.</li> <li>• <b>Network:</b> Alerts associated with network configuration and health are suppressed.</li> <li>• <b>Power:</b> Power redundancy alerts are suppressed. It does not suppress a <i>nodeOffline</i> alert which would occur in the event of a total power loss.</li> </ul>
Actions	Select the vertical drop-down menu for edit and delete options for the selected policy.

## Create an alert policy

You can create an alert policy to monitor information from the **All Clusters View** in SolidFire Active IQ. Alert policies allow you to be notified of a status or performance event with one or more clusters across an installation so that action can be taken in advance of, or in response to, a more serious event.

### Steps

1. Select **Alerts > Policies**.



2. Select **Create Policy**.
3. Select an alert type from the **Policy Type** list. See [Alert policy types](#).



There are additional policy-specific fields within the **Create Policy** dialog box depending on the policy type selected.

4. Enter a name for the new alert policy.



Alert policy names should describe the condition the alert is being created for. Descriptive titles help identify the alert easily. Alert policy names are displayed as a reference elsewhere in the system.

5. Select a severity level.



Alert policy severity levels are color coded and can be filtered easily from the **Alerts > History** page.

6. Determine the type of suppression for the alert policy by selecting a type from **Suppressible Types**. You can select more than one type.

Confirm that the associations make sense. For example, you have selected **Network Suppression** for a network alert policy.

7. Select one or more clusters to include in the policy.



When you add a new cluster to your installation after you have created the policy, the cluster will not automatically be added to existing alert policies. You must edit an existing alert policy and select the new cluster you want to associate with the policy.

8. Enter one or more email addresses to which alert notifications will be sent. If you are entering multiple addresses, you must use a comma to separate each address.
9. Select **Save Alert Policy**.

## Alert policy types

You can create alert policies based on available policy types listed in the **Create Policy** dialog box from **Alarms > Policies**.

Available policy alerts include the following types:

Policy Type	Description
Cluster Fault	Sends a notification when a specific type or any type of cluster fault occurs.
Event	Sends a notification when a specific event type occurs.
Failed Drive	Sends a notification when a drive failure occurs.
Available Drive	Sends a notification when a drive comes online in <i>Available</i> state.
Cluster Utilization	Sends a notification when the cluster capacity and performance being used is more than the specified percentage.

Policy Type	Description
Usable Space	Sends a notification when usable cluster space is less than a specified percentage.
Provisionable Space	Sends a notification when provisionable cluster space is less than a specified percentage.
Collector Not Reporting	Sends a notification when the collector for SolidFire Active IQ that runs on the management node fails to send data to SolidFire Active IQ for the duration specified.
Drive Wear	Sends a notification when a drive in a cluster has less than a specified percentage of wear or reserve space remaining.
iSCSI Sessions	Sends a notification when the number of active iSCSI sessions is greater than the value specified.
Chassis Resiliency	Sends a notification when the used space of a cluster is greater than a user-specified percentage. You should select a percentage that is sufficient to give early notice before reaching the cluster resiliency threshold. After reaching this threshold, a cluster can no longer automatically heal from a chassis-level failure.
VMware Alarm	Sends a notification when a VMware alarm is triggered and reported to SolidFire Active IQ.
Custom Protection Domain Resiliency	When used space increases beyond the specified percentage of custom protection domain resiliency threshold, the system sends a notification. If this percentage reaches 100, the storage cluster does not have enough free capacity to self-heal after a custom protection domain failure occurs.
Node Core/Crash Dump Files	When a service becomes unresponsive and must be restarted, the system creates a core file or crash dump file and sends a notification. This is not the expected behavior during regular operations.

## Edit an alert policy

You can edit an alert policy to add or remove clusters from a policy or change additional policy settings.

### Steps

1. Select **Alerts > Policies**.
2. Select the menu for more options under **Actions**.
3. Select **Edit Policy**.



The policy type and type-specific monitoring criteria are not editable.

4. (Optional) Enter a revised name for the new alert policy.



Alert policy names should describe the condition the alert is being created for. Descriptive titles help identify the alert easily. Alert policy names are displayed as a reference elsewhere in the system.

5. (Optional) Select a different severity level.



Alert policy severity levels are color coded and can be filtered easily from the Alerts > History page.

6. Determine the type of suppression for the alert policy when it is active by selecting a type from **Suppressible Types**. You can select more than one type.

Confirm that the associations make sense. For example, you have selected **Network Suppression** for a network alert policy.

7. (Optional) Select or remove cluster associations with the policy.



When you add a new cluster to your installation after you have created the policy, the cluster is not automatically be added to existing alert policies. You must select the new cluster you want to associate with the policy.

8. (Optional) Modify one or more email addresses to which alert notifications will be sent. If you are entering multiple addresses, you must use a comma to separate each address.
9. Select **Save Alert Policy**.

## Delete an alert policy

Deleting an alert policy removes it permanently from the system. Email notifications are no longer sent for that policy and cluster associations with the policy are removed.

### Steps

1. Select **Alerts > Policies**.
2. Under **Actions**, select the menu for more options.
3. Select **Delete Policy**.
4. Confirm the action.

The policy is permanently removed from the system.

## View suppressed clusters

On the **Suppressed Clusters** page in the Alerts drop-down menu within the All Clusters View, you can view a list of clusters which have alert notifications suppressed.

NetApp Support or customers can suppress alert notifications for a cluster when performing maintenance. When notifications are suppressed for a cluster using upgrade suppression, common alerts that occur during upgrades are not sent. There is also a full alert suppression option that stops alert notification for a cluster for a specified duration. You can view any email alerts that are not sent when notifications are suppressed on the **History** page of the **Alerts** menu. Suppressed notifications resume automatically after the defined duration elapses. You can end suppression of notifications early by selecting "resume notifications" in the dropdown menu.

On the **Suppressed Clusters** page, you have the option to view the following information for **Past**, **Active**, and **Future** suppressions. The **Past** option shows the suppressions that ended in the last 90 days.

Heading	Description
Company	Company name assigned to the cluster.

Heading	Description
Cluster ID	Assigned cluster number when the cluster is created.
Cluster Name	Name assigned to the cluster.
Created By	The account username that created the suppression.
Created Time	The exact time that the suppression was created.
Updated Time	If the suppression was modified after it was created, this is the exact time that the suppression was last changed.
Start Time	The exact time that the suppression of notifications started or is scheduled to start.
End Time	The exact time that the suppression of notifications is scheduled to end.
Type	<p>Determines which alerts and events are suppressed. The following types are possible:</p> <ul style="list-style-type: none"> <li>• <b>Full:</b> All alerts for the cluster are suppressed for the duration specified. No support cases or email alerts are generated.</li> <li>• <b>Upgrades:</b> Non-critical cluster alerts are suppressed for the duration specified. Critical alerts still generate support cases and emails.</li> <li>• <b>Compute:</b> Alerts that are triggered by VMware on the compute nodes are suppressed.</li> <li>• <b>NodeHardware:</b> Alerts associated with node maintenance are suppressed. For example, swapping out drives or taking nodes offline.</li> <li>• <b>Drive:</b> Alerts associated with drive health are suppressed.</li> <li>• <b>Network:</b> Alerts associated with network configuration and health are suppressed.</li> <li>• <b>Power:</b> Power redundancy alerts are suppressed. It does not suppress a <i>nodeOffline</i> alert which would occur in the event of a total power loss.</li> </ul>
Status	<p>Indicates the status of an alert notification:</p> <ul style="list-style-type: none"> <li>• <b>Active:</b> Suppression of alert notifications is active.</li> <li>• <b>Future:</b> Suppression of alert notifications is scheduled for a future date and time.</li> </ul>
Scheduled	<p>Indicates if the suppression was scheduled when it was created:</p> <ul style="list-style-type: none"> <li>• <b>True:</b> The Created Time and Start Time values are the same.</li> <li>• <b>False:</b> The Created Time and Start Time values are different.</li> </ul>

## Suppress cluster notifications

You can suppress alert notifications at the cluster level for a single cluster or multiple clusters for the current date and time or schedule to start at a future date and time.

## Steps

1. Do one of the following:
  - a. From the **Dashboard** overview, select the Actions menu for the cluster that you want to suppress.
  - b. From **Alerts > Cluster Suppression**, select **Suppress Clusters**.
2. In the **Suppress Alerts for Cluster** dialog box, do the following:
  - a. If you selected the **Suppress Clusters** button from the **Suppressed Clusters** page, select a cluster.
  - b. Select an alert suppression type as either **Full**, **Upgrades**, **Compute**, **NodeHardware**, **Drive**, **Network** or **Power**. [Learn about suppression types](#).



A cluster can have multiple suppression types, which can include multiple selections of the same suppression type. When a suppression type already exists during a scheduled suppression window, it is greyed out. To select this suppression type again, select **Overlap Existing**. Multiple selections of the same suppression type can have overlapping times or, if scheduling future suppressions, be at different times. When two suppressions have overlapping time periods, the functionality is the same as having a single suppression with a start time starting at the earliest of the suppressions and an end time ending at the latest.

- c. Select the start date and time that you want the suppression of notifications to start.
  - d. Select a common duration or enter a custom end date and time during which notifications should be suppressed.
3. Select **Suppress**.



This action also suppresses certain or all notifications to NetApp Support. After cluster suppression is in effect, NetApp Support or any user that is entitled to view the cluster can update the suppression state.

## End cluster suppression from a cluster

You can end cluster alert suppression on clusters that was applied using the Suppress Clusters feature. This enables clusters to resume their normal state of alert reporting.

### Steps

1. From the **Dashboard** overview or **Alerts > Cluster Suppression**, end suppression for the single or multiple clusters that you want to resume normal alert reporting:
  - a. For a single cluster, select the Actions menu for the cluster and select **End Suppression**.
  - b. For multiple clusters, select the clusters and then select **End Selected Suppressions**.

## Alert notification email

Subscribers to SolidFire Active IQ alerts receive status emails for any alert that triggers on the system. There are three types of status emails associated with alerts:

New Alert Email	This type of email is sent when an alert is triggered.
Reminder Alert Email	This type of email is sent once every 24 hours for as long as the alert remains active.
Alert Resolved Email	This type of email is sent when the issue is resolved.

After an alert policy is created, and if a new alert is generated for this policy, an email is sent to the designated email address (see [Create an Alert Policy](#)).

The alert email subject line uses one of the following formats depending on error type reported:

- Unresolved cluster fault: [cluster fault code] fault on [cluster name] ([severity])
- Resolved cluster fault: Resolved: [cluster fault code] fault on [cluster name] ([severity])
- Unresolved alert: [policy name] alert on [cluster name] ([severity])
- Resolved alert fault: Resolved: [policy name] alert on [cluster name] ([severity])

Multiple notifications are grouped into a single email with the most severe faults at the top of the email similar to the following example:

Cluster Method Not Reporting detected 2 alert(s) on [SF\_Cluster1, SF\_Cluster2]

(1) SF\_Cluster1

(1) SF\_Cluster2

Alert: 1 of 2

**Status: Alert Reminder Notification**

Alert ID: 1a5a49b7-f0a1-4ca5-9aad-8047e40e6331

Alert Policy: Cluster Method Not Reporting

Severity: Error

Cluster: SF\_Cluster1

Occurrence Time: 2025-05-10 01:13:28 UTC

Notification Time: 2025-05-10 01:13:28 UTC

- lastUpdate: 2025-05-10T00:17:18.362Z
- methodName: ListSnapshots
- expectedInterval: 300

Additional Detail:

- lastUpdate: 2025-05-10T00:17:18.362Z
- methodName: ListSnapshots
- expectedInterval: 300

Historical Detail: This alert has occurred 34 times in the last 30 days.

[Alerts for this Cluster](#)

Alert: 2 of 2

**Status: Alert Reminder Notification**

Alert ID: ec463269-922c-4bcd-9622-12167f0950ae

Alert Policy: Cluster Method Not Reporting

Severity: Error

Cluster: SF\_Cluster2

Occurrence Time: 2025-05-10 01:08:02 UTC

Notification Time: 2025-05-10 01:08:02 UTC

- lastUpdate: 2025-05-10T00:11:53.946Z
- methodName: ListSnapshots
- expectedInterval: 300

Additional Detail:

- lastUpdate: 2025-05-10T00:11:53.946Z
- methodName: ListSnapshots
- expectedInterval: 300

Historical Detail: This alert has occurred 33 times in the last 30 days.

[Alerts for this Cluster](#)



**Find more information**

[NetApp Product Documentation](#)

## Capacity Licensing

On the **Capacity Licensing** page within the **All Clusters View**, you can view information about the NetApp Capacity Licensing model. Customers using standard SolidFire appliances should disregard this page.

To view a given capacity licensing pool, you must have permissions to view all clusters included in that pool. If there are parent and child company relationships involved, work with your account manager to confirm that this is correctly recorded. Failure to do so might cause the capacity licensing pool to become unavailable.

Capacity Licensing is an alternative licensing option available from NetApp. Learn about or perform capacity licensing related tasks:

Heading	Description
Pool Name	Name of the customer associated with the license.
Entitled Capacity	Sum of software capacity licenses purchased.
Provisioned Capacity	Amount of allocated provisioned capacity on all capacity licensed nodes in a customer environment.
Used Capacity	Current used capacity by all clusters in a cluster pool.
Clusters	Number of clusters and their IDs, which comprise a cluster pool for a license.

### Find more information

[NetApp Product Documentation](#)

## Term Capacity

On the **Term Capacity** page within the **All Clusters View**, you can view information about the NetApp term-capacity model.

Heading	Description
Company ID	Company ID associated with the license.
Company Name	Name of the company associated with the license.
Licenses	Number of licenses in a customer environment.
Clusters	Number of clusters and their IDs belonging to a customer.
Licensed Capacity	Amount of allocated capacity on the capacity licensed nodes in a customer environment.
Consumed Capacity	Current consumed capacity by all clusters belonging to a customer.


### Find more information

[NetApp Product Documentation](#)

# Select a cluster

## Single cluster view dashboard

On the **Dashboard** page for a selected cluster, you can view high-level cluster details, including performance, capacity, and compute utilization.

Select the **Show Details** drop-down menu to view more information about the cluster or select the  icon next to a heading for more granular reporting information. You can also move the mouse pointer over graph lines and reporting data to display additional details.

Available details will vary based on your system:

- [Storage-only system](#)
- [NetApp HCI system overview](#)

### Storage-only system

For a SolidFire storage-based solution, you can view details and performance information specific to your cluster when you select **Show Details** from the **Dashboard** page.

Heading	Description
Information bar	This top bar provides a quick overview of the current status of the selected cluster. The bar shows the number of nodes, number of volumes, fault details, real-time statistics about efficiency, and status about the block and metadata capacity. Links from this bar open to the corresponding data in the UI.
Cluster Details	Expand the information bar by selecting <b>Show Details</b> to show these values: <ul style="list-style-type: none"><li>• Element Version</li><li>• iSCSI Sessions</li><li>• Fibre Channel Sessions</li><li>• Total Max Configured IOPS</li><li>• Total Max IOPS</li><li>• Node Types</li><li>• Encryption at Rest</li><li>• Vvols</li><li>• Total Min Configured IOPS</li></ul>
Performance	This graph shows the IOPS and throughput usage.




Heading	Description
Capacity	<p>This shows the health and fullness of the installation's cluster:</p> <ul style="list-style-type: none"> <li>• Provisioned: The total capacity of all volumes created on the system.</li> <li>• Physical: The total amount of physical capacity (total block data capacity) on the system for data to be stored (after all efficiencies are applied).</li> <li>• Block Capacity: The amount of block data capacity currently in use.</li> <li>• Metadata Capacity: The amount of metadata capacity currently in use.</li> <li>• Efficiencies: The amount of efficiencies the system is seeing due to compression, deduplication, and thin provisioning.</li> </ul>

## NetApp HCI system overview

For a NetApp HCI-based solution, you can view details and performance information specific to your cluster when you select **Show Details** from the **Dashboard** page.

Heading	Description
Information bar	<p>This top bar provides a quick overview of the current status of the selected cluster. The bar shows the number of compute and storage nodes, compute status, storage status, number of virtual machines, and number of volumes associated with your NetApp HCI system. Links from this bar open to the corresponding data in the UI.</p>

Heading	Description
Installation Details	<p>Expand the information bar by selecting <b>Show Details</b> to show these values:</p> <ul style="list-style-type: none"> <li>• Element Version</li> <li>• Hypervisor</li> <li>• Associated vCenter Instance</li> <li>• Associated Datacenter</li> <li>• Total Max Configured IOPS</li> <li>• Total Max IOPS</li> <li>• Compute Node Types</li> <li>• Storage Node Types</li> <li>• Encryption at Rest</li> <li>• Vvols</li> <li>• iSCSI Sessions</li> <li>• Total Min Configured IOPS</li> <li>• IOPS Rebalancing</li> </ul> <div>  <p>Beginning with Element 12.8 clusters, an additional field <b>IOPS Rebalancing</b> is provided. If the cluster-wide option is enabled, then each volume shows this parameter. This field's value is either true or false. This field is used to balance slices according to the true load rather than the minimum IOPS settings.</p> </div>
Compute Utilization	CPU and memory usage are represented in this graph.
Storage Capacity	<p>This shows the health and fullness of the installation's cluster:</p> <ul style="list-style-type: none"> <li>• Provisioned: The total capacity of all volumes created on the system.</li> <li>• Physical: The total amount of physical capacity (total block data capacity) on the system for data to be stored (after all efficiencies are applied).</li> <li>• Block Capacity: The amount of block data capacity currently in use.</li> <li>• Metadata Capacity: The amount of metadata capacity currently in use.</li> <li>• Efficiencies: The amount of efficiencies the system is seeing due to compression, deduplication, and thin provisioning.</li> </ul>
Storage Performance	IOPS and throughput are represented in this graph.

## Find more information

[NetApp Product Documentation](#)

## Reporting options for a selected cluster

Learn about the **Reporting** drop-down menu in the side panel:

- [Capacity](#)
- [Efficiency](#)
- [Performance](#)
- [Node Utilization](#)
- [Error Log](#)
- [Events](#)
- [Alerts](#)
- [iSCSI Sessions](#)
- [Virtual Networks](#)
- [API Collection](#)

### Capacity

On the **Capacity** page of the **Reporting** drop-down menu for a selected cluster, you can view details about the overall cluster space that is provisioned into volumes. Capacity information bars provide the current state and forecasts of block and metadata storage capacity for the cluster. The corresponding graphs provide additional methods for analyzing the cluster data.



For details about severity levels and cluster fullness, see the [Element Software documentation](#).

The following descriptions give details about the block capacity, metadata capacity, and provisioned space on the selected cluster.

Block capacity		
Heading	Description	Forecast
Used Capacity	Current used capacity of the cluster block.	Not applicable
Warning Threshold	The current warning threshold.	Forecast for when the warning threshold will be reached.
Error Threshold	The current error threshold.	Forecast for when the error threshold will be reached.
Total Capacity	The total capacity for the block.	Forecast for when the critical threshold will be reached.
Current State	Current state of the block.	For details about severity levels, see the <a href="#">Element Software documentation</a> .
Metadata capacity		
Heading	Description	
Used Capacity	The metadata cluster capacity used for this cluster.	

Block capacity	
Total Capacity	The total available metadata capacity for this cluster and the critical threshold forecast.
Current State	The current state of the metadata capacity for this cluster.
Provisioned space	
Heading	Description
Provisioned Space	The amount of space that is currently provisioned on the cluster.
Max Provisioned Space	The maximum space that can be provisioned on the cluster.

## Efficiency

On the **Efficiency** page of the cluster **Reporting** drop-down menu for a selected cluster, you can view details about thin provisioning, deduplication, and compression on the cluster when you move your mouse pointer over data points on the graph.



All combined efficiencies are calculated by simple multiplication of the reported factor values.

The following descriptions give details about calculated efficiencies on the selected cluster.

Heading	Description
Overall efficiency	The global efficiency of thin provisioning, deduplication, and compression multiplied together. These calculations do not take into account the double helix feature built into the system.
Deduplication and Compression	The combined effect of space saved by using deduplication and compression.
Thin Provisioning	The amount of space saved by using this feature. This number reflects the delta between the capacity allocated for the cluster and the amount of data actually stored.
Deduplication	The ratio multiplier of the amount of space that was saved by not storing duplicate data in the cluster.
Compression	The effect of data compression on stored data in the cluster. Different data types compress at different rates. For example, text data and most documents easily compress to a smaller space, but video and graphical images typically do not.

## Performance

On the **Performance** page of the **Reporting** drop-down menu for a selected cluster, you can view details about IOPS usage, throughput, and cluster utilization by selecting the category and filtering based on time period.

## Node Utilization

On the **Node Utilization** page of the **Reporting** drop-down menu for a selected cluster, you can select and view each node.

Beginning with Element 12.8, node utilization information is available as `nodeHeat` using the `getNodeStats` and `listNodeStats` API methods. The `nodeHeat` object is a member of the `nodeStats` object and displays node utilization information based on the ratio of primary total IOPS or total IOPS to the configured IOPS averaged over time. The node utilization graph shows this as a percentage derived from the metric `recentPrimaryTotalHeat`.

## Error Log

On the **Error Log** page of the **Reporting** drop-down menu for a selected cluster, you can view information about unresolved or resolved errors that have been reported by the cluster. This information can be filtered and exported to a comma-separated values (CSV) file. For details about severity levels, see the [Element Software documentation](#).

The following information is reported for the selected cluster.

Heading	Description
ID	ID for a cluster fault.
Date	The date and time the fault was logged.
Severity	This can be warning, error, critical, or best practice.
Type	This can be node, drive, cluster, service, or volume.
Node ID	Node ID for the node that this fault refers to. Included for node and drive faults; otherwise set to - (dash).
Node Name	The system-generated node name.
Drive ID	Drive ID for the drive that this fault refers to. Included for drive faults; otherwise set to - (dash).
Resolved	Displays if the cause of the error has been resolved.
Resolution Time	Displays the time an issue was resolved.
Error Code	A descriptive code that indicates what caused the fault.
Details	Description of the fault with additional details.

## Events

On the **Events** page of the **Reporting** drop-down menu for a selected cluster, you can select between the **Events** and **gcEvents** tabs to view information about key events that have occurred on the cluster. By default, selecting **Events** shows all of the events except for `gcEvents` to improve readability. In order to see all events, including `gcEvents`, select the tab labeled **gcEvents**. This information can be filtered and exported to a CSV file.

The following information is reported for the selected cluster.

Heading	Description
Event ID	Unique ID associated with each event.
Event Time	The time the event occurred.
Type	The type of event being logged, for example, API events, clone events, or gc events. See the <a href="#">Element Software documentation</a> for more information.
Message	Message associated with the event.
Service ID	The service that reported the event (if applicable).
Node ID	The node that reported the event (if applicable).
Drive ID	The drive that reported the event (if applicable).
Details	Information that helps identify why the event occurred.

## Alerts

On the **Alerts** page of the **Reporting** drop-down menu for a selected cluster, you can view unresolved or resolved cluster alerts. This information can be filtered and exported to a CSV file. For details about severity levels, see the [Element Software documentation](#).

The following information is reported for the selected cluster.

Heading	Description
Triggered	The time the alert was triggered in SolidFire Active IQ, not on the cluster itself.
Last Notified	The time the most recent alert email was sent.
Resolved	Shows if the cause of the alert has been resolved.
Policy	This is the user-defined alert policy name.
Severity	Severity assigned at the time the alert policy was created.
Destination	The email address or addresses selected to receive the alert email.
Trigger	The user-defined setting that triggered the alert.

## iSCSI Sessions

On the **iSCSI Sessions** page of the **Reporting** drop-down menu for a selected cluster, you can view details about the number of active sessions on the cluster and the number of iSCSI sessions that have occurred on the cluster.

Expand the iSCSI Sessions example



You can move your mouse pointer over a data point on the graph to find the number of sessions for a defined time period:

- Active Sessions: The number of iSCSI sessions that are attached and active on the cluster.
- Peak Active Sessions: The maximum number of iSCSI sessions that have occurred on the cluster in the last 24 hours.

 This data includes iSCSI sessions generated by FC nodes.

Virtual Networks

On the **Virtual Networks** page of the **Reporting** drop-down menu for a selected cluster, you can view the following information about virtual networks configured on the cluster.

Heading	Description
ID	Unique ID of the VLAN network. This is assigned by the system.
Name	Unique user-assigned name for the VLAN network.
VLAN ID	VLAN tag assigned when the virtual network was created.
SVIP	Storage virtual IP address assigned to the virtual network.
Netmask	Netmask for this virtual network.
Gateway	Unique IP address of a virtual network gateway. VRF must be enabled.

Heading	Description
VRF Enabled	Shows if virtual routing and forwarding is enabled or not.
IPs Used	The range of virtual network IP addresses used for the virtual network.

## API Collection

On the **API Collection** page of the **Reporting** drop-down menu for a selected cluster, you can view the API methods used by the NetApp SolidFire Active IQ. For detailed descriptions of these methods, see the [Element Software API documentation](#).



In addition to these methods, SolidFire Active IQ makes some internal API calls used by NetApp Support and engineering to monitor cluster health. These calls are not documented as they can be disruptive to cluster functionality if used incorrectly. If you require a complete list of SolidFire Active IQ API collections, you must contact NetApp Support.

## Find more information

[NetApp Product Documentation](#)

# Nodes head

From the **Nodes** page, available from the side panel for a selected cluster, you can view information for the nodes in your cluster.

The available details vary based on your system:

- [View SolidFire storage node details](#)
- [View NetApp HCI storage and compute node details](#)

## View SolidFire storage node details

Each node is a collection of SSDs. Each storage node comes with CPU, networking, cache, and storage resources. The storage node resources are pooled into a cluster of nodes.

On the **Nodes** page, the information bar provides a quick overview of the following data:

- MVIP: Management virtual IP address
- MVIP VLAN ID: Virtual LAN ID for the MVIP
- SVIP: Storage virtual IP address
- SVIP VLAN ID: Virtual LAN ID for the SVIP

## View information about storage nodes

The following information is available for each storage node in the cluster:

Heading	Description
ID	System-generated ID for the node.



Heading	Description
Status	<p>The status of the node:</p> <ul style="list-style-type: none"> <li>• Healthy: The node has no critical errors associated with it.</li> <li>• Offline: The node cannot be accessed. Select the link to view the Error Log.</li> <li>• Fault: There are errors associated with this node. Select the link to view the Error Log.</li> </ul>
Name	The system-generated node name.
Type	Displays the model type of the node.
Platform Config Version	The config version of the chassis you are running on.
BIOS Version	The BIOS version for your node's hardware.
BMC Firmware Revision	The revision of the firmware currently running on the Baseboard Management Controller (BMC).
Version	Version of Element software running on the node.
Serial Number	Unique serial number assigned to the node.
Management IP	Management IP address assigned to node for 1GbE or 10GbE network admin tasks.
Cluster IP	Cluster IP address assigned to the node used for the communication between nodes in the same cluster.
Storage IP	Storage IP address assigned to the node used for iSCSI network discovery and all data network traffic.
Average Throughput Last 30 mins	Sum of average throughputs executed in the last 30 minutes against all volumes that have this node as their primary.
Average IOPS Last 30 mins	Sum of the average number of IOPS executed in the last 30 minutes against all volumes that have this node as their primary.
Average Latency (µs) Last 30 mins	The average time in microseconds, as measured over the last 30 minutes, to complete read and write operations to all volumes that have this node as their primary. To report this metric based on active volumes, only non-zero latency values are used.
Role	<p>Identifies what role the node has in the cluster:</p> <ul style="list-style-type: none"> <li>• Cluster Master: The node that performs cluster-wide administrative tasks and contains the MVIP and SVIP.</li> <li>• Ensemble Node: A node that participates in the cluster. There are either three or five ensemble nodes depending on cluster size.</li> <li>• Fibre Channel: An FC node in the cluster.</li> <li>• If a node does not have a role, the value is set to - (dash).</li> </ul>
End of Availability	Date when nodes are no longer available for purchase, but are still supported.
End of Hardware Support	Date when hardware is no longer supported.

Heading	Description
End of Software Support	Date when software is no longer supported.

## View NetApp HCI storage and compute node details

For NetApp H-series nodes, which comprise a NetApp HCI system, there are two types: compute and storage nodes.

On the **Nodes** page, the information bar provides a quick overview of the following data:

- MVIP: Management virtual IP address
- SVIP: Storage virtual IP address

Learn about viewing information about storage nodes and compute nodes in a NetApp HCI cluster:

- [View information about storage nodes](#)
- [View information about compute nodes](#)

### View information about storage nodes

Select **Storage** to view the following information about the storage nodes in the cluster.

Heading	Description
ID	System-generated ID for the node.
Status	The status of the node: <ul style="list-style-type: none"> <li>• Healthy: The node has no critical errors associated with it.</li> <li>• Offline: The node cannot be accessed. Select the link to view the Error Log.</li> <li>• Fault: There are errors associated with this node. Select the link to view the Error Log.</li> </ul>
Name	The system-generated node name.
Type	Shows the model type of the node.
Chassis / Slot	Unique serial number assigned to the chassis and the slot location of the node.
Serial Number	Unique serial number assigned to the node.
Platform Config Version	The config version of the chassis you are running on.
BIOS Version	The BIOS version for your node's hardware.
BMC Firmware Revision	The revision of the firmware currently running on the Baseboard Management Controller (BMC).
Version	Version of Element software running on the node.
Management IP	Management IP address assigned to node for 1GbE or 10GbE network admin tasks.
Storage IP	Storage IP address assigned to the node used for iSCSI network discovery and all data network traffic.

Heading	Description
Average IOPS Last 30 mins	Sum of the average number of IOPS executed in the last 30 minutes against all volumes that have this node as their primary.
Average Throughput Last 30 mins	Sum of average throughputs executed in the last 30 minutes against all volumes that have this node as their primary.
Average Latency (µs) Last 30 mins	The average time in microseconds, as measured over the last 30 minutes, to complete read and write operations to all volumes that have this node as their primary. To report this metric based on active volumes, only non-zero latency values are used.
Role	Identifies what role the node has in the cluster: <ul style="list-style-type: none"> <li>• Cluster Master: The node that performs cluster-wide administrative tasks and contains the MVIP and SVIP.</li> <li>• Ensemble Node: A node that participates in the cluster. There are either three or five ensemble nodes depending on cluster size.</li> <li>• If a node does not have a role, the value is set to - (dash).</li> </ul>
End of Availability	Date when nodes are no longer available for purchase, but are still supported.
End of Hardware Support	Date when hardware is no longer supported.
End of Software Support	Date when software is no longer supported.

### View information about compute nodes

Select **Compute** to view the following information about the compute nodes in the cluster.

Heading	Description
Host	IP address of the compute node.
Status	The value that comes back from VMware. Hover over this for the VMware description.
Type	Shows the model type of the node.
Chassis/Slot	Unique serial number assigned to the chassis and the slot location of the node.
Serial Number	Unique serial number assigned to the node.
vCenter IP	IP address of the vCenter Server.
BIOS Version	The BIOS version for your node's hardware.
BMC Firmware Revision	The revision of the firmware currently running on the Baseboard Management Controller (BMC).
vMotion IP	VMware vMotion network IP address of the compute node.
End of Availability	Date when nodes are no longer available for purchase, but are still supported.
End of Hardware Support	Date when hardware is no longer supported.
End of Software Support	Date when software is no longer supported.

## Find more information

[NetApp Product Documentation](#)

# Volumes

## Active Volumes

From the **Volumes** page, you can view details about active volumes.

### View active volume details

On the **Volumes > Active Volumes** page for a selected cluster, you can view the following information in the list of active volumes.

Heading	Description
ID	ID given when the volume was created.
Account ID	ID of the account assigned to the volume.
Volume Size	Size of the volume from which the snapshot was created.
Used Capacity	Current used capacity of the volume: <ul style="list-style-type: none"><li>• Green = up to 80%</li><li>• Yellow = above 80%</li><li>• Red = above 95%</li></ul>
Primary Node ID	Primary node for this volume.
Secondary Node ID	List of secondary nodes for this volume. Can be multiple values during transitory states, like change of secondary nodes, but will usually have a single value.
QoS Throttle	Represents the current throttling for the volume. <ul style="list-style-type: none"><li>• Green = up to 20%</li><li>• Yellow = above 20%</li><li>• Red = above 80%</li></ul> The value does not include historical throttling on the volume.
Min IOPS	The minimum number of IOPS guaranteed for the volume.
Max IOPS	The maximum number of IOPS allowed for the volume.
Burst IOPS	The maximum number of IOPS allowed over a short period of time.

Heading	Description
Average IOPS Last 30 mins	<p>The average number of IOPS executed for all volumes that have this node as their primary.</p> <p>IOPS are collected over 500 millisecond intervals on the cluster side. SolidFire Active IQ collects these values at 60 second intervals. For each volume, the average IOPS is calculated from the SolidFire Active IQ values collected in the last 30 minutes.</p>
Average Throughput Last 30 mins	<p>The average throughput executed for all volumes that have this node as their primary.</p> <p>Throughput is collected over 500 millisecond intervals on the cluster side. SolidFire Active IQ collects these values at 60 second intervals. For each volume, the average throughput is calculated from the SolidFire Active IQ values collected in the last 30 minutes.</p>
Average Latency (µs) Last 30 min	<p>The average time in microseconds to complete read and write operations to all volumes that have this node as their primary.</p> <p>Latency is measured over 500 millisecond intervals on the cluster side. SolidFire Active IQ collects these values at 60 second intervals. For each volume, the average latency is calculated from the SolidFire Active IQ values collected in the last 30 minutes. For more information, see this <a href="#">KB article</a>.</p>
Snapshots	The number of snapshots created for the volume.
Actions	Select the vertical drop-down menu for more details on an individual volume.
IOPS Rebalancing	Beginning with Element 12.8 clusters, an additional field <b>IOPS Rebalancing</b> is provided. If the cluster-wide option is enabled, then each volume shows this parameter. This field's value is either true or false. This field is used to balance slices according to the true load rather than the minimum IOPS settings.

## Find more information

[NetApp Product Documentation](#)

## Snapshots and Snapshot Schedules


Learn about viewing information about snapshots and snapshot schedules:


- [Snapshots](#)
- [Snapshot Schedules](#)

### Snapshots

From the **Volumes** page that is available from the side panel for a selected cluster, you can view information about volume snapshots.

#### Steps

1. Select **Volumes > Snapshots**.
2. Alternatively, select **Volumes > Active Volumes** and in the Actions column, select the  icon for the volume you want and select **View Snapshots**.


3. (Optional) You can export the snapshot list as a CSV file by selecting the  icon.

The following list describes the available details:

Heading	Description
ID	Displays the snapshot ID assigned to the snapshot.
Volume ID	ID given when the volume was created.
Account ID	ID of the account assigned to the volume.
UUID	Universally unique identifier.
Size	User-defined size of the snapshot.
Volume Size	Size of the volume from which the snapshot was created.
Create Time	The time at which the snapshot was created.
Retain Until	The day and time the snapshot will be deleted.
Group Snapshot ID	The group ID the snapshot belongs to if grouped together with other volume snapshots.
Replicated	Displays the status of the snapshot on the remote cluster: <ul style="list-style-type: none"><li>• Present: The snapshot exists on a remote cluster.</li><li>• Not Present: The snapshot does not exist on a remote cluster.</li><li>• Syncing: The target cluster is currently replicating the snapshot.</li><li>• Deleted: The target replicated the snapshot and then deleted it.</li></ul>

## Snapshot Schedules

From the **Volumes > Snapshot Schedules** page that is available from the side panel for a selected cluster, you can view snapshot schedule details.

You can export the snapshot schedule list as a CSV file by selecting the  icon.

The following list describes the available details:

Heading	Description
ID	The schedule ID assigned to the schedule.
Name	User-assigned name of the schedule.
Frequency	The frequency at which the schedule is run. The frequency can be set in hours and minutes, weeks, or months.
Recurring	Indicates whether or not the schedule is recurring.
Volume IDs	The volume IDs included in the scheduled snapshot.
Last Run	The last time the schedule executed.
Last Run Status	The outcome of the last schedule execution. Possible values: Success or Error

Heading	Description
Manually Paused	Identifies whether or not the schedule has been manually paused.

### Find more information

[NetApp Product Documentation](#)

## Volume Performance


From the **Volumes** page, you can view details about each volume and see its performance graphs:

- [View individual volume details](#)
- [View individual volume performance graphs](#)

### View individual volume details

From the **Volumes** page, you can view more information for an individual volume.

#### Steps

1. Select **Volumes > Active Volumes**.
2. In the Actions column, select the  icon for the volume you want and select **View Details**.

After the page opens for the active volume, you can view recent volume data from the information bar.

Heading	Description
Account ID	System-generated ID for the volume.
Volume Size	Total size of the volume.
Used Capacity	Shows how full the volume is.
Average IOPS	Average number of IOPS executed against the volume in the last 30 minutes.
Average Throughput	Average throughput executed against the volume in the last 30 minutes.
Average Latency	The average time, in microseconds, to complete read and write operations to the volume in the last 30 minutes. For more information, see this <a href="#">KB article</a> .
<b>You can view additional details from the Show Volume Details drop-down menu.</b>	
Access	The read/write permissions assigned to the volume.
Access Groups	Associated volume access groups.
Non-Zero Blocks	Total number of 4KiB blocks with data after the last round of garbage collection operation has completed.
Zero Blocks	Total number of 4KiB blocks without data after the last round of garbage collection operation has completed.
Snapshot Count	The number of associated snapshots.
Min IOPS	The minimum number of IOPS guaranteed for the volume.

Heading	Description
Max IOPS	The maximum number of IOPS allowed for the volume.
Burst IOPS	The maximum number of IOPS allowed over a short period of time.
512e Enabled	Identifies if 512e is enabled on a volume.
QoS Throttle	Represents the current throttling for the volume. The value does not include historical throttling on the volume.
Primary Node ID	Primary node for this volume.
Secondary Node ID	List of secondary nodes for this volume. Can be multiple values during transitory states, like change of secondary nodes, but will usually have a single value.
Volumes Paired	Indicates if a volume has been paired or not.
Create Time	The time the volume creation task was completed.
Block Size	Size of the blocks on the volume.
IQN	The iSCSI Qualified Name (IQN) of the volume.
scsiEUIDeviceID	Globally unique SCSI device identifier for the volume in EUI-64 based 16-byte format.
scsiNAADeviceID	Globally unique SCSI device identifier for the volume in NAA IEEE Registered Extended format.
Attributes	List of Name/Value pairs in JSON object format.


## View individual volume performance graphs

From the **Volumes** page, you can view performance activity for each volume in a graphical format. This information provides real-time statistics for throughput, IOPS, latency, queue depth, average IO size, and capacity for each volume.


### Steps

1. Select **Volumes > Volume Performance**.
2. From the **Volume** drop-down list, select a Volume ID to view details for that volume. Note that the Volume drop-down list is searchable by Volume ID.
3. On the left, select a thumbnail graph to view performance graphs in detail. You can view the following graphs:
  - Throughput
  - IOPS
  - Latency
  - Queue Depth
  - Average IO Size
  - Capacity

You can also view the **Average**, **Min**, or **Max** for each graph too. Note that Average is the default view.

4. (Optional) You can export each graph as a CSV file by selecting the  icon.



- Alternatively, you can select **Volumes > Active Volumes**.
- In the **Actions** column, select the  icon for the volume you want and select **View Details**.

A separate page opens to display an adjustable timeline, which is synced with the performance graphs.

### Find more information

[NetApp Product Documentation](#)

## Virtual Volumes

From the **VVols** page, available from the side panel for a selected cluster, you can view information about virtual volumes and their associated storage containers, protocol endpoints, bindings, and hosts.

Learn about VVols-related tasks:

- [Virtual Volumes](#)
- [Storage Containers](#)
- [Protocol Endpoints](#)
- [Hosts](#)
- [Bindings](#)

### Virtual Volumes

The **VVols > Virtual Volumes** page for a selected cluster provides information about each active virtual volume on the cluster.

Heading	Description
Volume ID	The ID of the underlying volume.
Snapshot ID	The ID of the underlying volume snapshot. The value is zero if the virtual volume does not represent a snapshot.
Parent Virtual Volume ID	The virtual volume ID of the parent virtual volume. If the ID is all zeros, the virtual volume is independent with no link to a parent.
Virtual Volume ID	The universal unique identifier of the virtual volume.
Name	The name assigned to the virtual volume.
Guest OS Type	Operating system associated with the virtual volume.
Type	The virtual volume type: Config, Data, Memory, Swap, or Other.
Access	The read/write permissions assigned to the virtual volume.
Size	The size of the virtual volume in gigabytes (GB) or gibibytes (GiB).

Heading	Description
Used Capacity	Current used capacity of the volume: <ul style="list-style-type: none"> <li>• Green = up to 80%</li> <li>• Yellow = above 80%</li> <li>• Red = above 95%</li> </ul>
Snapshot	The number of associated snapshots. Select the number to link to the snapshot copy details.
Min IOPS	The minimum IOPS QoS setting of the virtual volume.
Max IOPS	The maximum IOPS QoS setting of the virtual volume.
Burst IOPS	The maximum burst QoS setting of the virtual volume.
VMW_VmID	Information in fields prefaced with "VMW_" are defined by VMware. See VMware documentation for descriptions.
Create Time	The time the virtual volume creation task was completed.
Actions	Select the vertical drop-down menu for more details on an individual virtual volume.

## Storage Containers

On the **VVols > Storage Containers** page for a selected cluster, you can view the following information for all active storage containers on the cluster.

Heading	Description
Account ID	The ID of the account associated with the storage container.
Name	The name of the storage container.
Status	The status of the storage container: <ul style="list-style-type: none"> <li>• Active: The storage container is in use.</li> <li>• Locked: The storage container is locked.</li> </ul>
PE Type	Indicates the protocol endpoint type (SCSI is the only available protocol for Element software).
Storage Container ID	The universal unique identifier (UUID) of the virtual volume storage container.
Active Virtual Volumes	The number of active virtual volumes associated with the storage container.

## Protocol Endpoints

The **VVols > Protocol Endpoints** page of the selected cluster provides protocol endpoint information such as primary provider ID, secondary provider ID, and protocol endpoint ID.

Heading	Description
Primary Provider ID	The ID of the primary protocol endpoint provider.
Secondary Provider ID	The ID of the secondary protocol endpoint provider.
Protocol Endpoint ID	The UUID of the protocol endpoint.
Protocol Endpoint State	The status of the protocol endpoint: <ul style="list-style-type: none"> <li>• Active: The protocol endpoint is in use.</li> <li>• Start: The protocol endpoint is starting.</li> <li>• Failover: The protocol endpoint has failed over.</li> <li>• Reserved: The protocol endpoint is reserved.</li> </ul>
Provider Type	The type of the protocol endpoint's provider: Primary or Secondary.
SCSI NAA Device ID	The globally unique SCSI device identifier for the protocol endpoint in NAA IEEE Registered Extended Format.

## Hosts

The **VVols > Hosts** page for a selected cluster provides information about VMware ESXi hosts that host virtual volumes.

Heading	Description
Host ID	The UUID for the ESXi host that hosts virtual volumes and is known to the cluster.
Bindings	Binding IDs for all virtual volumes bound by the ESXi host.
ESX Cluster ID	The vSphere host cluster ID or vCenter GUID.
Initiator IQNs	Initiator IQNs for the virtual volume host.
SolidFire Protocol Endpoint IDs	The protocol endpoints that are currently visible to the ESXi host.

## Bindings

The **VVols > Bindings** page for a selected cluster provides binding information about each virtual volume.

Heading	Description
Host ID	The UUID for the ESXi host that hosts virtual volumes and is known to the cluster.
Protocol Endpoint ID	The UUID of the protocol endpoint.
Protocol Endpoint In Band ID	The SCSI NAA device ID of the protocol endpoint.
Protocol Endpoint Type	Indicates the protocol endpoint type (SCSI is the only available protocol for Element software).
VVol Binding ID	The binding UUID of the virtual volume.
VVol ID	The UUID of the virtual volume.

Heading	Description
VVol Secondary ID	The secondary ID of the virtual volume that is a SCSI second level LUN ID.

## Find more information

[NetApp Product Documentation](#)

# QoS Management

## QoS Management

From the **QoS Management** page, available from the side panel for a selected cluster, you can view information on QoS recommendations, throttling, and volumes for the nodes in a cluster.

Learn about viewing information on QoS recommendations, throttling, and volumes for a selected node:

- [Recommendations](#)
- [Node Throttling](#)
- [Busiest Volumes](#)

## Find more information

[NetApp Product Documentation](#)

## Recommendations

The **QoS Management > Recommendations** page, available from the side panel for a selected cluster, provides daily quality of service (QoS) recommendations for a cluster based on recent performance data. QoS recommendations are only supported for clusters on Element software 11.x or later.

SolidFire Active IQ makes performance recommendations based on volume statistics data for recent activity. Recommendations focus on QoS maximum and minimum guaranteed IOPS for a volume and are only visible in the UI when cluster improvements might be needed.

## Find more information

- [Performance and QoS for a SolidFire storage cluster](#)
- [Create and manage volume QoS policies](#)
- [NetApp Product Documentation](#)

## Node Throttling

From the **QoS Management > Node Throttling** page, available from the side panel for a selected cluster, you can view the percent throttling for the nodes in the cluster. The nodes are listed as thumbnail layouts on the left side of the display and are ordered

depending on the degree of throttling for a selected time range.

Learn about viewing node throttling information:

- [View graphs and select date ranges](#)
- [Export node throttling data](#)

### View graphs and select date ranges

The graphs and date ranges in SolidFire Active IQ are seamlessly integrated with each other. When selecting a date range, the **Node Throttling** and **Total Volume Throughput** graphs on that page adjust to the range selected. The default date range displayed for each graph is seven days. When you select a node from the graph selection tabs, these graphs change to the newly selected node.

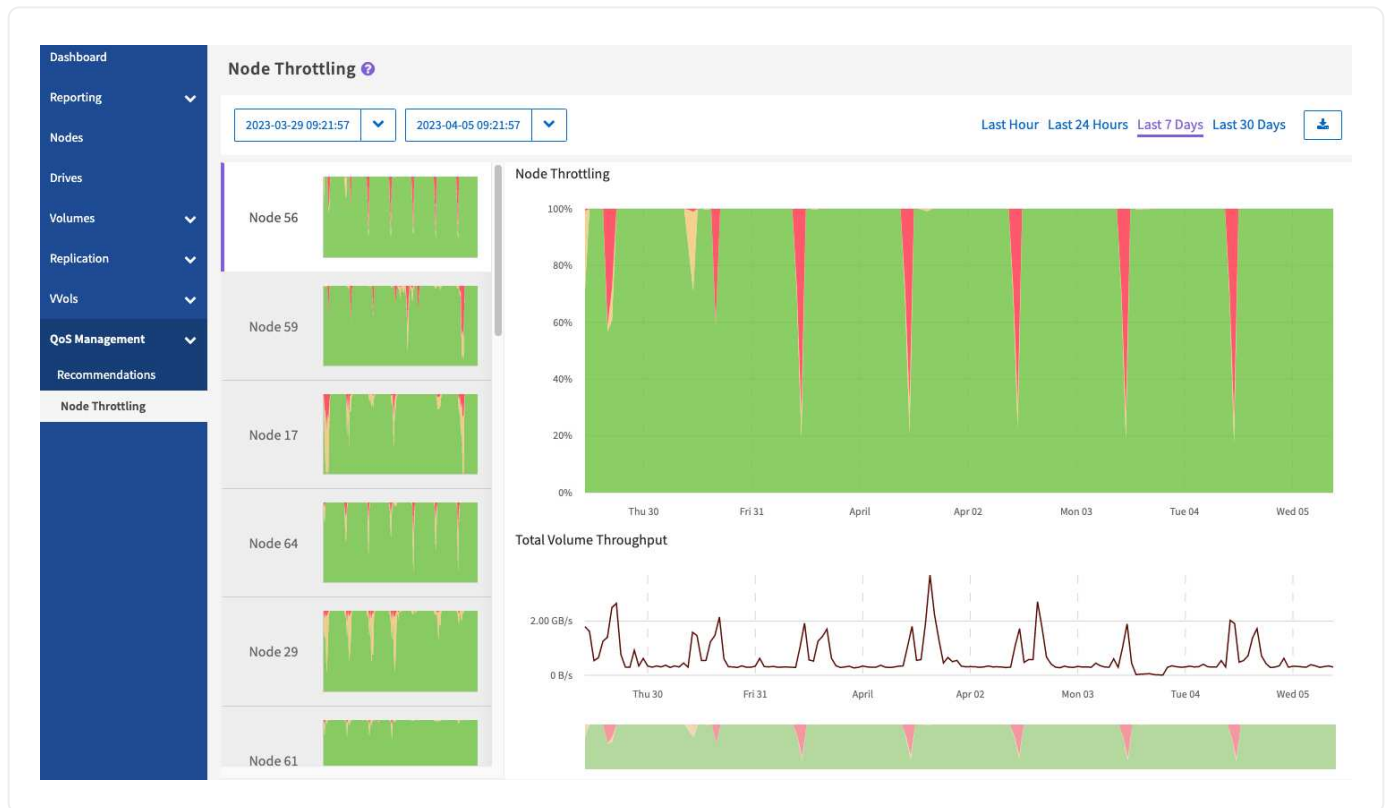
You can select a date range from the calendar drop-down box or from a set of pre-defined ranges. Date ranges are calculated using the current browser time (at the time of selection) and the configured amount of time. You can also select a desired interval by brushing directly over the bar graph at the bottom. To switch between graphs, select the thumbnail layouts on the left.

The **Node Throttling** graph displays node throttling over the selected time period based on the minimum and maximum IOPS settings for the volumes hosted on the selected node. The color represents the amount of throttling:

- Green: The node is not being throttled. Volumes are permitted to perform up to their maximum configured IOPS.
- Yellow: The node is experiencing limited throttling. Volumes are throttled down from their maximum IOPS setting, but still retain performance at or above their minimum IOPS setting.
- Red: The node is experiencing high throttling. When volumes are throttled more severely, performance can fall below the minimum IOPS setting.

The **Total Volume Throughput** graph displays the sum of the throughput for the primary volumes for a selected node. The graph shows the sum of volume read and write throughput. It does not include metadata or other node traffic. It also takes into account when volumes are present on a node, which results in a drop in throughput when volumes are transferred off a node.

## Expand the graph example



Position the mouse pointer at any point in the graph to see point-in-time details.

[Learn about QoS recommendations for a cluster.](#)




From the Node Throttling page, you can determine if there is QoS pushback in a storage cluster, see this [KB article](#) for information.

## Export node throttling data

You can export graph data to a comma-separated values (CSV) format. Only the information displayed in the graph is exported.

### Steps

1. In a list view or graph, select the  icon.

## Find more information

[NetApp Product Documentation](#)

## Busiest Volumes

From the **QoS Management > Busiest Volumes** page, available from the side panel for a selected cluster, you can view the ten volumes with the highest throughput for a selected node and time range in the cluster.

Learn about viewing the busiest volume information:

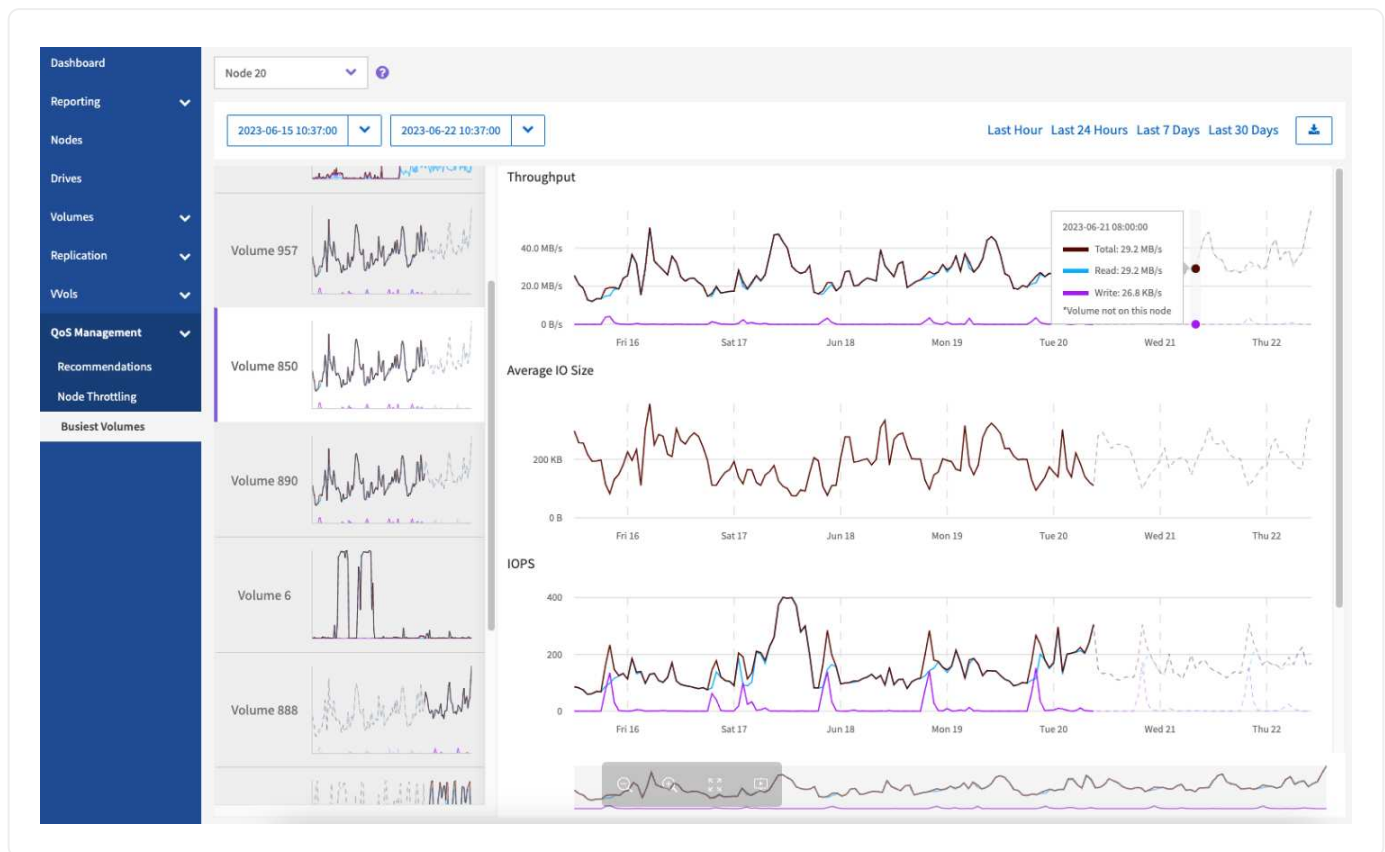
- [View graphs and select date ranges](#)
- [Export busiest node data](#)

## View graphs and select date ranges

After selecting the node from the drop-down list, the ten volumes with the highest throughput on that node are displayed. For each volume, you can view the **Throughput**, **Average IO Size**, **IOPS**, and **Latency** graphs; to see the last graph, you might need to scroll down the page. To switch between volumes, select the thumbnail layouts on the left. When you select a different node, these graphs change to the newly selected node.

The graphs and date ranges in SolidFire Active IQ are seamlessly integrated with each other. When selecting a date range, the graphs on that page adjust to the range selected. The default date range displayed for each graph is seven days. You can select a date range from the calendar drop-down box or from a set of pre-defined ranges. You can also select a desired interval by brushing directly over the bar graph at the bottom. Date ranges are calculated using the current browser time (at the time of selection) and the configured amount of time. When you change the selected date range for a node, the ten busiest volumes displayed might also change.

## Expand the graph example




Position the mouse pointer at any point in the graph to see point-in-time details for the read, write, and total operations. If a volume is not present on the node for part of the selected time range, it is represented by a dotted line

## Export busiest node data

You can export graph data to a comma-separated values (CSV) format. Only the information displayed in the graph is exported.

Steps

- 1. In a list view or graph, select the  icon.

Find more information

[NetApp Product Documentation](#)

# Virtual Machines

From the **Virtual Machines** page, available from the side panel for a selected NetApp HCI cluster, you can view CPU and storage-related status information about virtual machines (VMs).



The **Virtual Machines** page is available only on a NetApp HCI cluster.

Learn about filtering and understanding VM data displayed in the UI.

## View Virtual Machine details

The **Virtual Machines** page, available from the side panel for a selected cluster, provides information about each active VM associated with the cluster.

In addition to conventional filtering options that are available on all SolidFire Active IQ pages, the **Virtual Machines** page has quick filter buttons that you can select to determine common VM states of availability.

The information bar provides a quick overview of the following data:

- Virtual Machines: The number and various availability states of VMs associated with the storage cluster.
- Status: The number of warnings or errors for the VMs.
- Provisioned Resources: The total storage and memory resources for all VMs associated with the storage cluster.

Heading	Description
Name	The friendly name of the VM.
Status	The availability status of the VM: <ul style="list-style-type: none"><li>• Normal: The VM is responding as expected.</li><li>• Warning: A warning has been reported. See vSphere for more details.</li><li>• Critical: A critical error has been reported. See vSphere for more details.</li><li>• Unknown: The VM is inaccessible.</li></ul>
Power State	Indicates whether the VM is powered on, powered off, or suspended.
vCenter IP	IP address of the vCenter Server.
Number of CPUs	The number of CPUs for each VM.
Host Memory Usage	The amount of ESXi host memory that is being used by a virtual machine.



Heading	Description
CPU Usage	The percentage of actively used virtual CPU as a percentage of total available CPU in the VM.
Used Capacity	The percentage of VM storage resources in use.
Peak Disk Latency	The maximum detected disk latency in milliseconds.
Alarms	The number of triggered vSphere alarms on the VM.

## Find more information

[NetApp Product Documentation](#)

## VMware Alarms

From the **VMware Alarms** page, available from the side panel for a selected NetApp HCI cluster, you can view the VMware alarms related information about a cluster.



The **VMware Alarms** page is available only on a NetApp HCI cluster.

Learn about the VMware alarms data displayed in the UI.

Heading	Description
vCenter IP	IP address of the vCenter Server.
Entity ID	The ID of the object in vSphere where the alarm originated.
Status	Severity of the VMware alarm.
Alarm Name	Name of the VMware alarm.
Description	Description of the VMware alarm.
Trigger Time	The time the alert was triggered in SolidFire Active IQ, not on the cluster itself.

## Find more information

[NetApp Product Documentation](#)

## All Nodes View

You can view information about all nodes for a company, including throttled nodes, when you select the company name from the **All Nodes View** drop-down list. After you select the company name, it replaces **All Nodes View** in the top navigation bar.



If your SolidFire Active IQ account has only one company name associated with it, the **All Nodes** and **Throttled Nodes** pages, available from the side panel, default to that company name.

Learn more about the All Nodes and Throttled Nodes pages:

- [View information about all nodes](#)
- [View information about throttled nodes](#)

## View information about all nodes


On the **All Nodes** page, available from the side panel, you can view information about all nodes for your selected company.

Heading	Description
Cluster ID	Assigned cluster number when the cluster is created.
Cluster	Name assigned to the cluster.
Node ID	System-generated ID for the node.
Status	<p>The status of the node:</p> <ul style="list-style-type: none"><li>• Healthy: The node has no critical errors associated with it.</li><li>• Offline: The node cannot be accessed. Select the link to view the Error Log.</li><li>• Fault: There are errors associated with this node. Select the link to view the Error Log.</li></ul>
Name	The system-generated node name.
Type	Shows the model type of the node.
Serial Number	Unique serial number assigned to the node.
Version	Version of Element software running on the node.
Management IP	Management IP address assigned to node for 1GbE or 10GbE network admin tasks.
Storage IP	Storage IP address assigned to the node used for iSCSI network discovery and all data network traffic.
Role	<p>Identifies what role the node has in the cluster:</p> <ul style="list-style-type: none"><li>• Cluster Master: The node that performs cluster-wide administrative tasks and contains the management virtual IP address and storage virtual IP address.</li><li>• Ensemble Node: A node that participates in the cluster. There are either three or five ensemble nodes depending on cluster size.</li><li>• Fibre Channel: An FC node in the cluster.</li><li>• If a node does not have a role, the value is set to - (dash).</li></ul>

## View information about throttled nodes

On the **Throttled Nodes** page, available from the side panel, you can view information for all nodes with throttling greater than 1% in the last 30 days for your selected company.

You have the option to view nodes with a **High**, **Limited**, or **Combined** (high and limited) throttling time. You

can also view descriptions for the node throttling table and the high, limited, and combined throttling options by selecting the  icon, as shown in the following example:

All Nodes

Throttled Nodes

High

Limited

Combined

Cluster ID	Cluster	Node
		11
		17
		29
		32
		22
		47
		38

This table displays nodes across all clusters which have experienced throttling over the last 30 days. This metric is based on a combination of throughput, observed IO latencies, and system cache fullness. As the load on a given node increases, QoS will progressively throttle volumes hosted on that node, based on the volume's QoS settings. Nodes which have not experienced throttling in the past 30 days will not appear in this table.

The percentage in the throttling columns is the amount of time the node experienced throttling over the specified time period.

High	The amount of time High throttling was in effect. During this time, volumes will be throttled more severely and performance can fall below the minimum IOPS setting.
Limited	The amount of time Limited throttling was in effect. During this time, volumes are throttled down from their maximum IOPS setting, but will retain performance at or above their minimum IOPS setting.
Combined	The amount of time either High or Limited throttling was in effect.

If a node continues to experience persistent high throttling, please contact your Support Engineer to address potential workload rebalancing.

Learn more about the information available for throttled nodes.

Heading	Description
Cluster ID	Assigned cluster number when the cluster is created.
Cluster	Name assigned to the cluster.
Node ID	System-generated ID for the node.
Name	The system-generated node name.
Type	Shows the model type of the node.
Version	Version of Element software running on the node.
High throttling time view	
High Throttle Last 24 hours	The percentage of high node throttling in the last 24 hours.
High Throttle Last 7 days	The percentage of high node throttling in the last 7 days.
High Throttle Last 14 days	The percentage of high node throttling in the last 14 days.
High Throttle Last 30 days	The percentage of high node throttling in the last 30 days.
Limited throttling time view	
Limited Throttle Last 24 hours	The percentage of limited node throttling in the last 24 hours.

Heading	Description
Limited Throttle Last 7 days	The percentage of limited node throttling in the last 7 days.
Limited Throttle Last 14 days	The percentage of limited node throttling in the last 14 days.
Limited Throttle Last 30 days	The percentage of limited node throttling in the last 30 days.
<b>Combined throttling time view</b>	
Combined Throttle Last 24 hours	The percentage of combined node throttling in the last 24 hours.
Combined Throttle Last 7 days	The percentage of combined node throttling in the last 7 days.
Combined Throttle Last 14 days	The percentage of combined node throttling in the last 14 days.
Combined Throttle Last 30 days	The percentage of combined node throttling in the last 30 days.
Average Throughput Last 30 mins	Sum of average throughputs executed in the last 30 minutes against all volumes that have this node as their primary.
Average IOPS Last 30 mins	Sum of the average number of IOPS executed in the last 30 minutes against all volumes that have this node as their primary.
Average Latency (µs) Last 30 mins	The average time in microseconds, as measured over the last 30 minutes, to complete read and write operations to all volumes that have this node as their primary. To report this metric based on active volumes, only non-zero latency values are used.

## Find more information

[NetApp Product Documentation](#)

## Copyright information

Copyright © 2025 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.