NetApp SolidFire Active IQ User Guide

April 2022

NetApp

Copyright Information

Trademark Information

Table of Contents

Introduction **6**

Getting Started **7**

Enabling Active IQ Reporting 7

Using the Active IQ User Interface **8**

Using Filters 8

Sorting Lists 8

Viewing Graphs and Selecting Date Ranges 8

Exporting List Views and Reporting Data 9

Selecting a Cluster 9

Icon Reference 10

Providing Feedback 10

All Clusters View **11**

All Clusters View Dashboard 11

Alerts 11

Viewing Alerts History 11

Alerts History Details 11

Viewing Alert Policies 12

Creating an Alert Policy 12

Alert Policy Types 13

Editing an Alert Policy 14

Deleting an Alert Policy 14

Suppressing Cluster Notifications 15

Viewing Suppressed Clusters 15

Remove Cluster Suppression from a Cluster 16

Alert Notification Email 16

Capacity Licensing 17

Viewing Capacity Licensing 17
Capacity Licensing Details 18
Select a Cluster View **19**
Dashboard in Single Cluster View 19
Storage-Only System 19
NetApp HCI System Overview 20
Capacity 22
Efficiency 22
Performance 23
Error Log 24
Events 24
Alerts 25
iSCSI Sessions 25
Virtual Networks 26
API Collection 27
Nodes **28**
Viewing SolidFire Storage Node Details 28
Viewing NetApp HCI Storage and Compute Node Details 29
Drives **31**
Volumes **32**
Active Volumes Details 32
Viewing Individual Volume Details 33
Viewing Individual Volume Performance Graphs 34
Viewing Snapshots 34
Snapshots Details 34
Viewing Snapshot Schedules 35
Snapshot Schedules Details 35

Replication **37**
Cluster Pairs 37
Volume Pairs 37
Virtual Volumes **38**
Virtual Volumes Details 38
Storage Containers 39
Protocol Endpoints 39
Hosts 39
Bindings 40
QoS Recommendations **40**
Virtual Machines **40**
Viewing Virtual Machine Details 41
Where to Find Additional Information **42**
Contacting NetApp Support **43**

Introduction

This guide provides information about how to use the SolidFire Active IQ (AIQ) user interface (UI). The SolidFire Active IQ UI includes a full set of features that enables the following functionality:

Cluster Access	Access to one or more clusters can be established by connecting with the management node (mNode).
System Monitoring	Information about the health, performance, and capacity of your clusters are provided in list formats and graphical formats that allow you to visualize the state of the clusters you are connected to.
Error Logging	Immediately see errors as they occur in the system. The Error Log format is the same format used in the NetApp Element UI.
Events	Identify the key events that are occurring on the cluster. The Events list format is the same format used in the NetApp Element UI.
Alerts	Define and manage alerts to send an email when certain events occur in the system.
Virtual Networks	View configured virtual networks.
Capacity Forecasting	Access information about current block and metadata storage capacities and forecasts.
Capacity Licensing	Capacity license model customers can view and monitor capacity usage.
VVols	If enabled, view and export data for virtual volumes (VVols).

Getting Started

Welcome to Active IQ from NetApp, a web-based tool that provides continually updated historical views of cluster-wide statistics. Data is collected at defined intervals and might be archived for up to five years, depending on the type of data. Notifications can be set up to alert you about specified events, thresholds, or metrics on a cluster so that they can be addressed quickly when they arise. The Active IQ tool makes monitoring capacity and performance, as well as being informed about cluster health, easy and accessible from anywhere.

Enabling Active IQ Reporting

You must enable Active IQ reporting capability on the management node before the Active IQ server can connect to a cluster and receive cluster information. When the connection has been successfully set up, the cluster sends information to the Active IQ server. The cluster can then be viewed in the Active IQ UI, which displays cluster information.

NOTE: For additional details about the management node and enabling Active IQ, see the latest version of the *management node user guide for NetApp Element software* in the documentation library for your product.

NOTE: Google Chrome and Firefox browsers are supported to run with Active IQ.

Using the Active IQ User Interface

See the following topics to learn about the user interface features and functionality in Active IQ.

- *Using Filters*
- *Sorting Lists*
- *Viewing Graphs and Selecting Date Ranges*
- *Exporting List Views and Reporting Data*
- *Selecting a Cluster*
- *Icon Reference*
- *Providing Feedback*

Using Filters

You can sort and filter list information on pages in Active IQ. When viewing lists (such as nodes, drives, volumes, and so on), you can use filter functionality to focus the information and make it more easily fit on the screen.

Procedure

1. When viewing list information, click **Filter**.
2. Choose a column name to filter by from the drop-down menu.
3. Select a constraint for the column.
4. Enter text to filter by.
5. Click **Add Filter**.

   The system runs the new filter on the information in the list and temporarily stores the new filter. The selected filter is shown at the bottom of the filter dialog box.
6. (Optional) To add another filter, perform the following steps:
   a. Select another column heading and constraint.
   b. Click **Add Filter**.
7. (Optional) Click (**x**) to remove the filters and display the unfiltered list information.

NOTE: Some tables include the option to exclude columns from view. For best results, click **Columns** to ensure all required columns are showing when setting filters.

Sorting Lists

You can sort list information by one or more columns on certain pages within the Active IQ UI. This helps you arrange the information you need on the screen.

Procedure

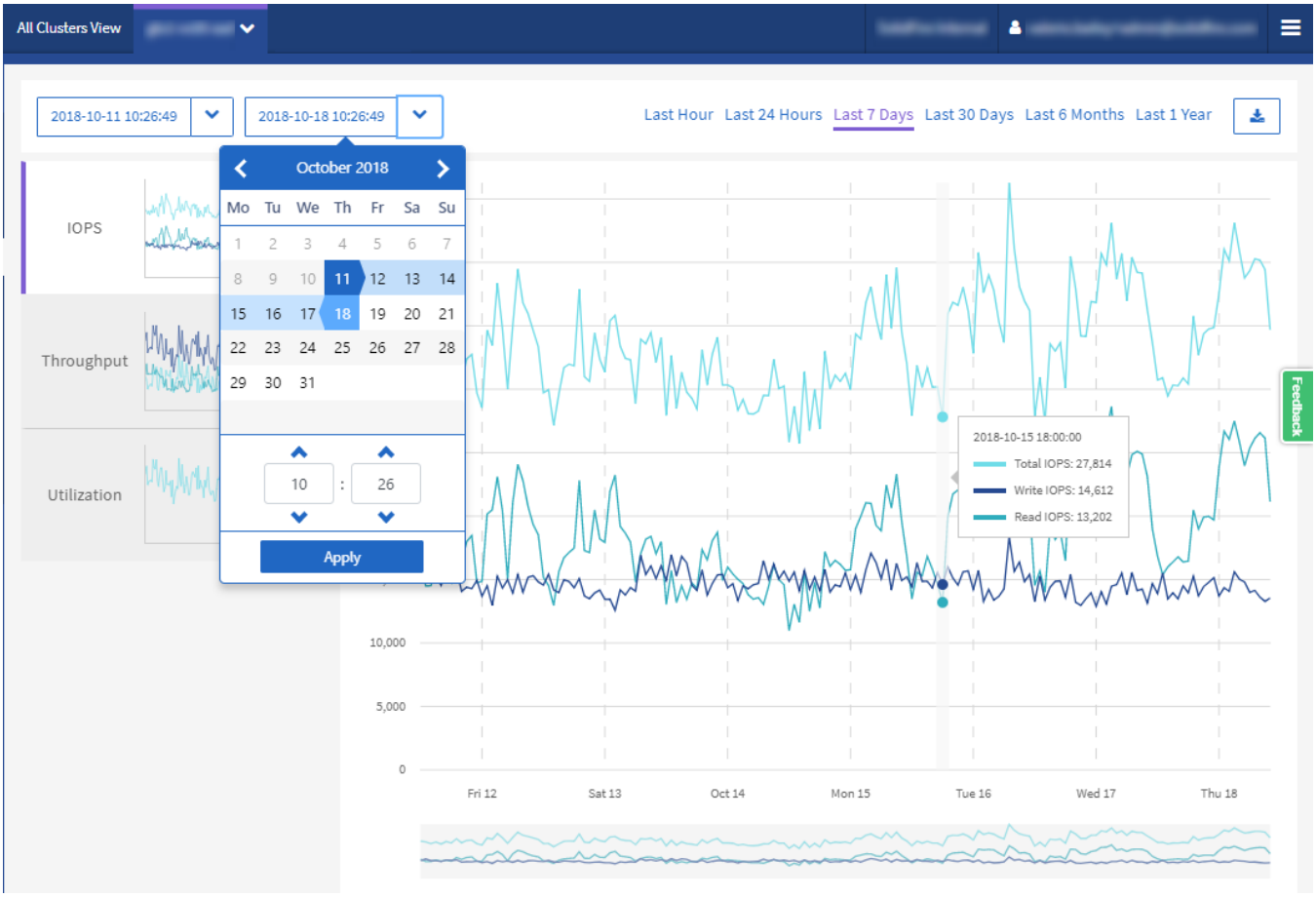
1. To sort on a single column, click the column heading until the information is sorted in the desired order.
2. To sort using multiple columns, click the column heading for each column you wish to sort by until the information in each column is sorted in the desired order. This functionality is not available on all pages.

Viewing Graphs and Selecting Date Ranges

The graphs and date ranges in Active IQ are seamlessly integrated with each other. When selecting a date range, all graphs on that page adjust to the range selected. The default date range displayed for each graph is 7 days.

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. Additionally, you can select a desired interval by brushing directly over the bar graph at the bottom. If available, switch between graphs by selecting the thumbnail layouts on the left. These layouts can also be hidden.

Position the mouse pointer over a graph line to see point-in-time details.



Exporting List Views and Reporting Data

You can export an entire list view or graph data to comma-separated values (CSV) format. Only the information displayed in the list view or graph is exported. If there is a certain sort order or if a filter is used to limit the displayed entries, that sort order and filter are preserved in the exported file.

Procedure

- In a list view or graph, click the export button ( ).

Selecting a Cluster

In Active IQ, you can view information about an individual cluster in your environment.

Procedure

1. From the Active IQ dashboard, click **Select a Cluster**.
2. The drop-down menu lists any clusters available to you.

3. Use the search field to locate the desired cluster or recently viewed clusters.
4. Click the name to select the cluster.

Icon Reference

You might see the following icons when viewing the UI for Active IQ.

Icon	Description
	Refresh
	Filter
	Export
	Menu for account settings, documentation, support, and logout.
	Option to provide feedback about user interface.
	Click one time to copy to clipboard.
	Toggle the button to wrap and unwrap text.
	More information. Click for other options.
	Click for more details.

Providing Feedback

You can help improve the Active IQ user interface and address any UI issues by using the feedback form that is accessible throughout the UI.

Procedure

1. From any page in the UI, click the **Feedback** button ().
2. Enter relevant information in the Summary and Description fields.
3. Attach any helpful screenshots.
4. Enter a name and email address.
5. Select the check box to include data about your current environment.
6. For more information, click on the link **What is included in the data about my current environment?**
7. Click **Submit**.

All Clusters View

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

See the following topics to learn about what can be accessed from this view:

- *All Clusters View Dashboard*
- *Alerts*
- *Capacity Licensing*

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.

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.

See the following topics to learn about or perform alerts-related tasks:

- *Viewing Alerts History*
- *Alerts History Details*
- *Viewing Alert Policies*
- *Creating an Alert Policy*
- *Alert Policy Types*
- *Editing an Alert Policy*
- *Deleting an Alert Policy*
- *Viewing Suppressed Clusters*
- *Suppressing Cluster Notifications*
- *Alert Notification Email*

Viewing Alerts History

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

Procedure

1. Click **Alerts > History.**
2. Click either the **Unresolved** or **Resolved** tab to view the history of alerts for the cluster.
3. (Optional) Click the export button ( ) 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.
Alert Triggered	The time the alert was triggered in Active IQ, not on the cluster itself.
Last Notification	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 Name	This is the user-defined alert policy name.
Severity	Severity assigned at the time the alert policy was created.
Value	This value depends the type of alert policy selected. For example, this can be a threshold value, API method, time frame, percentage, or other value.
Destination	The email address(es) selected to receive the alert email.
Customer	Name of customer associated with the alert.
Cluster	Displays the cluster name for which the alert policy was added.
Condition	The user-defined setting that triggered the alert.

Viewing 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.
Cluster	Number and name of each cluster defined in the alert policy. Click the info icon to reveal associated clusters.
Condition	User-defined setting for when an alert should be triggered.
Actions	Select the vertical drop-down menu for edit and delete options for the selected policy.

Creating an Alert Policy

You can create an alert policy to monitor information from the **All Clusters View** in 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.

Procedure

1. Click **Alerts > Policies**.
2. Click **Create Policy**.

3. Select an alert type from the **Policy Type** list. See *Alert Policy Types*.

   NOTE: 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.

   NOTE: 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.

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

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

   Caution: 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.

7. Enter one or more email addresses to which alert notifications will be sent. If you are entering multiple addresses, be sure to use a comma to separate each address.

8. Click **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 *Available* state.
Cluster Utilization	Sends a notification when the cluster capacity and performance being utilized is more than the specified percentage.
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 Active IQ that runs on the management node fails to send data to 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.

Policy Type	Description
Capacity Licensing	Sends a notification when provisioned licensed capacity (PLC) exceeds entitled licensed capacity (ELC) by the percentage 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 Active IQ.

Editing an Alert Policy

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

Procedure

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

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

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

   NOTE: 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.

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

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

   Caution: 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 select the new cluster you want to associate with the policy.

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

Deleting 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.

Procedure

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

4. Confirm the action.

   The policy is permanently removed from the system.

Suppressing Cluster Notifications

You can suppress alert notifications at the cluster level.

Procedure

1. Do one of the following:
   - From the **Dashboard** overview, click the Actions menu for the cluster that you want to suppress.
   - From **Alerts > Suppressed Clusters**, click **Suppress Cluster**.
2. In the **Suppress Alerts for Cluster** dialog box, do the following:
   a. If you clicked the **Suppress Cluster** button from the **Suppressed Clusters** page, select a cluster.
   b. Select an alert suppression type as either **Full** or **Upgrades**:
      - Full: All alerts for the cluster are suppressed for the duration specified. No support cases or email alerts are generated.
      - Upgrades: This is the default. Non-critical cluster alerts are suppressed for the duration specified. Critical alerts still generated support cases and emails. Although Element upgrades automatically suppress non-critical alerts and cases to Active IQ as part of the upgrade process, this manual upgrade suppression can be selected by users outside of the Element upgrade process for correlating maintenance activities.
   c. Select a common duration or enter a custom end date and time during which notifications should be suppressed.
3. Click **Suppress**.

NOTE: This action also suppress 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 may update the suppression state.

Viewing Suppressed Clusters

On the **Suppressed Clusters** page in the **Alerts** drop-down menu within **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.

The following information is available on this page.

Company	Company name assigned to the cluster.
Cluster ID	Assigned cluster number when the cluster is created.
Cluster Name	Name assigned to the cluster.
Start Time	Exact time that the suppression of notifications started.
End Time	Exact time that the suppression of notifications is scheduled to end.
Type	The following types are possible:

	• Full: All alerts for the cluster are suppressed for the duration specified. No support cases or email alerts are generated. • Upgrades: Non-critical cluster alerts are suppressed for the duration specified. Critical alerts still generated support cases and emails.
Actions	Select the option to suppress or resume notifications for a cluster.

Remove Cluster Suppression from a Cluster

As a customer, you can remove cluster alert suppression on a cluster that was applied using the Suppress Cluster feature. This enables a cluster to resume its normal state of alert reporting.

Procedure

1. From the **Dashboard** overview or **Alerts > Suppressed Clusters**, click the Actions menu for the cluster you want to resume normal alert reporting.
2. Click **Resume**.

Alert Notification Email

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

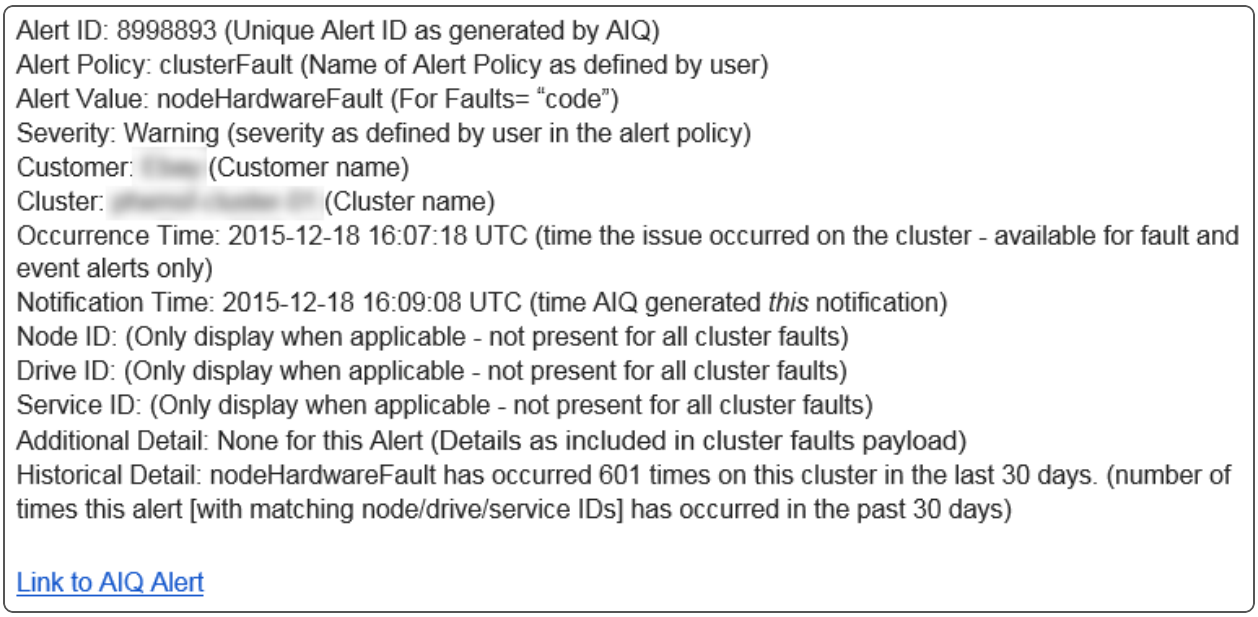
New Alert Email	This type of email is sent when an alert is triggered.
Reminder Alert Email	This type of email is sent once every 24 hours for as long as the alert remains active.
Alert Resolved Email	This type of email is sent when the issue is resolved.

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 *Creating 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])`

The content of the notification email will be similar to the example here:


Alert ID: 8998893 (Unique Alert ID as generated by AIQ)
Alert Policy: clusterFault (Name of Alert Policy as defined by user)
Alert Value: nodeHardwareFault (For Faults= "code")
Severity: Warning (severity as defined by user in the alert policy)
Customer: (Customer name)
Cluster: (Cluster name)
Occurrence Time: 2015-12-18 16:07:18 UTC (time the issue occurred on the cluster - available for fault and event alerts only)
Notification Time: 2015-12-18 16:09:08 UTC (time AIQ generated *this* notification)
Node ID: (Only display when applicable - not present for all cluster faults)
Drive ID: (Only display when applicable - not present for all cluster faults)
Service ID: (Only display when applicable - not present for all cluster faults)
Additional Detail: None for this Alert (Details as included in cluster faults payload)
Historical Detail: nodeHardwareFault has occurred 601 times on this cluster in the last 30 days. (number of times this alert [with matching node/drive/service IDs] has occurred in the past 30 days)

Link to AIQ Alert

Figure 1: Example of New Alert Notification Email

Capacity Licensing

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

Capacity Licensing is an alternative licensing option available from NetApp. For more information, see Capacity Licensing.

See the following topics to learn about or perform capacity licensing related tasks:

- *Viewing Capacity Licensing*
- *Capacity Licensing Details*

Viewing Capacity Licensing

On the **Capacity Licensing** page, you can view the following information:

Heading	Description
Customer ID	Customer ID associated with the license.
Customer Name	Name of the customer associated with the license.
Number of Capacity Licensed Nodes	Number of capacity licensed nodes in a customer environment.
Entitled Licensed Capacity	Sum of software capacity licenses purchased.
Provisioned Licensed Capacity	Amount of allocated provisioned capacity on all capacity licensed nodes in a customer environment.
Actions	Select the vertical drop-down menu for more details on capacity licensing for an individual customer.

Capacity Licensing Details

From the **Capacity Licensing** page within **All Clusters View**, click the  icon in the **Actions** column and click **Details**.

You can view the following on the capacity licensing details page:

Heading	Description
Customer Name	Name of the customer associated with the license.
Entitled Licensed Capacity	Sum of software capacity licenses purchased.
Provisioned Licensed Capacity	Amount of allocated provisioned capacity on all capacity licensed nodes.
Provisioned Licensed Capacity by Cluster	
Cluster ID	Cluster ID associated with the license.
Cluster Name	Name of the cluster associated with the license.
Provisioned Licensed Capacity	Amount of allocated provisioned capacity on all capacity licensed nodes in the cluster.
% of Total Provisioned Licensed Capacity	Percentage of the specific cluster relative to the Provisioned Licensed Capacity.
Capacity Licensed Nodes	
Cluster Name	Name of the cluster associated with the node.
Service Tag	Unique service tag number assigned to the node.
Model	Model name of the node.
Raw Capacity	Raw capacity of the node.

Select a Cluster View

You can view cluster information for a specific cluster when you select a cluster from the **Select a Cluster** drop-down list. Each category of cluster information is presented in either a table format or a graphical format.

See the following topics for more information on various lists and filters available from the **Dashboard** cluster overview or **Reporting** drop-down menu in the side panel:

- *Dashboard in Single Cluster View*
- *Capacity*
- *Efficiency*
- *Performance*
- *Error Log*
- *Events*
- *Alerts*
- *iSCSI Sessions*
- *Virtual Networks*
- *API Collection*

Dashboard in Single Cluster View

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

Click the **Show Details** drop-down menu to view more information about the cluster or click the arrow 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 click **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 user interface.
Cluster Details	Expand the information bar by selecting **Show Details** to show these values: • Element Version • iSCSI Sessions • Fibre Channel Sessions

Heading	Description
	• Nodes Types • Encryption at Rest
Performance	This graph shows the IOPS and throughput usage.
Utilization	This graph shows the percentage of cluster IOPS being consumed.
Capacity	This shows the health and fullness of the installation's cluster. • Provisioned: The total capacity of all volumes created on the system. • Physical: The total amount of physical capacity (total block data capacity) on the system for data to be stored (after all efficiencies are applied). • Block Data Capacity: The amount of block data capacity currently in use. • Metadata Capacity: The amount of metadata capacity currently in use. • Efficiencies: The amount of efficiencies the system is seeing due to compression, deduplication, and thin provisioning.

NetApp HCI System Overview

For an NetApp HCI-based solution, you can view details and performance information specific to your cluster when you click **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 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 user interface.
Installation Details	Expand the information bar by selecting **Installation Details** to show these values: • Element Version • Hypervisor • Associated vCenter Instance • Associated Datacenter • Compute Node Types • Storage Node Types • Encryption at Rest • iSCSI Sessions
Compute Utilization	CPU and memory usage are represented in this graph.
Storage Capacity	This shows the health and fullness of the installation's cluster. • Provisioned: The total capacity of all volumes created on the system. • Physical: The total amount of physical capacity (total block data capacity) on the system for data to be stored (after all efficiencies are applied).

Heading	Description
	• Block Capacity: The amount of block data capacity currently in use. • Metadata Capacity: The amount of metadata capacity currently in use. • Efficiencies: The amount of efficiencies the system is seeing due to compression, deduplication, and thin provisioning.
Storage Performance	IOPS and throughput are represented in this graph.

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.

NOTE: For details about severity levels and cluster fullness, see *Element Software documentation*.

Block Capacity

Heading	Description	Forecast
Used Capacity	Current used capacity of the cluster block.	N/A
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 *Element Software User Guide.*

Metadata Capacity

Heading	Description
Used Capacity	The metadata cluster capacity used for this cluster.
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

Max Provisioned Space	The maximum space that can be provisioned on the cluster.
Provisioned Space	The amount of space that is currently 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.

NOTE: 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:

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.
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 + Compression Efficiency	The combined effect of space saved by using deduplication and compression.
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.
Deduplication	The ratio multiplier of the amount of space that was saved by not storing duplicate data in the cluster.

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.

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 CSV file. For details about severity levels, refer to *Element Software documentation*.

The following information is reported.

Heading	Description
ID	Unique 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).
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 view information about key events that have occurred on the cluster. This information can be filtered and exported to a CSV file.

The following information is reported:

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 event or clone events. See the *Element Software User Guide* 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 *Element Software documentation*.

The following information is reported:

Heading	Description
Alert ID	Unique ID associated with each alert.
Alert Triggered	The time the alert was triggered in 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.
Severity	Severity assigned at the time the alert policy was created.
Policy Name	This is the user-defined alert policy name.
Alert Value	This value depends the type of alert policy selected. For example, this can be a threshold value, API method, time frame, percentage, or other value.
Destination	The email address(es) selected to receive the alert email
Alert Condition	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.

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.

NOTE: This data includes iSCSI sessions generated by Fibre Channel 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.

Heading	Description
Gateway	Unique IP address of a virtual network gateway. VRF must be enabled.
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, refer to the *Element Software API Reference Guide*.

NOTE: In addition to these methods, 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 improperly. Customers requiring a complete list of Active IQ API collections should contact NetApp Support.

Nodes

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

Available details will vary based on your system:

Viewing SolidFire Storage Node Details

Viewing NetApp HCI Storage and Compute Node Details

Viewing SolidFire Storage Node Details

Each node is a collection of solid state drives (SSD). 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

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

Heading	Description
ID	System-generated ID for the node.
Status	The status of the node. Possible values: Healthy: The node has no critical errors associated with it. Offline: The node cannot be accessed. Click link to see Error Log. Fault: There are errors associated with this node. Click link to see Error Log.
Name	The system-generated node name.
Type	Displays the model type of the node.
Version	Version of Element software running on each node.
Service Tag	Unique service tag number assigned to the node.
Serial Number	Unique serial number assigned to the node.
Management IP	Management IP (MIP) address assigned to node for 1GbE or 10GbE network admin tasks.
Cluster IP	Cluster IP (CIP) address assigned to the node used for the communication between nodes in the same cluster.
Storage IP	Storage IP (SIP) address assigned to the node used for iSCSI network discovery and all data network traffic.
Replication Port	The port used on nodes for remote replication.
Role	Identifies what role the node has in the cluster. Possible values: • Cluster Master: The node that performs cluster-wide administrative tasks and contains the MVIP

Heading	Description
	and SVIP. • Ensemble Node: A node that participates in the cluster. There are either 3 or 5 ensemble nodes depending on cluster size. • Fibre Channel: A Fibre Channel node in the cluster.
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.

Viewing 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:

vCenter IP	IP Address of the vCenter Server
MVIP	Management Virtual IP Address
SVIP	Storage Virtual IP Address

Click **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. Possible values: Healthy: The node has no critical errors associated with it. Offline: The node cannot be accessed. Click link to see Error Log. Fault: There are errors associated with this node. Click link to see Error Log.
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.
Version	Version of Element software running on each node.
Management IP	Management IP (MIP) address assigned to node for 1GbE or 10GbE network admin tasks.
Storage IP	Storage IP (SIP) address assigned to the node used for iSCSI network discovery and all data network traffic.
Role	Identifies what role the node has in the cluster. Possible values: • Cluster Master: The node that performs cluster-wide administrative tasks and contains the MVIP and SVIP.

Heading	Description
	• Ensemble Node: A node that participates in the cluster. There are either 3 or 5 ensemble nodes depending on cluster size.
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.

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

Heading	Description
IP	IP address of the compute node.
vCenter 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.
vMotion IP	The VMware vMotion network IP address of the compute node.

Drives

Each node contains one or more physical drives, which are used to store a portion of the data for the cluster. The cluster utilizes the capacity and performance of the drive after the drive is successfully added to a cluster.

On the **Drives** page, available from the side panel for a selected cluster, you can filter the page by selecting from the **Active**, **Available**, and **Failed** tabs.

The following information is available for each drive in the cluster depending on the state of drive functionality:

Heading	Description
Drive ID	Sequential number assigned to the drive.
Node ID	Assigned node number when the node is added to the cluster.
Service ID	The current service ID of the block or slice service that is associated with the drive.
Slot	Slot number where the drive is physically located.
Capacity	GB size of the drive.
Firmware Version	Version of the firmware on the drive.
Serial	Serial number of the SSD.
Wear Remaining	Wear level indicator.
Reserve	Drive available reserves.
Type	Drive type can be block or metadata.

Volumes

On the **Volumes** page, available from the side panel for a selected cluster, you can view information about volumes that are provisioned on the cluster. Each category of volume information is presented in either a table format or a graphical format.

See the following topics to learn about what is displayed from the **Volumes** page:

- *Active Volumes Details*
  - *Viewing Individual Volume Details*
  - *Viewing Individual Volume Performance Graphs*
- *Snapshots Details*
- *Viewing Snapshot Schedules*
  - *Snapshot Schedules Details*

Active Volumes 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. Green = up to 80%. Yellow = above 80%. Red = above 95%.
512e	Identifies if 512e is enabled on a 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.
QoS Throttle	Identifies if the volume is being throttled due to high load on the primary storage node. Green = up to 20%. Yellow = above 20%. Red = above 80%.
Access	The type of access assigned to the volume when it was created.
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.
Paired	Indicates whether or not the volume is part of a volume pairing.
Configured Access Protocols	The type of protocol the volume is configured for.
Snapshots	The number of snapshots created for the volume.
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	Sum of average throughputs executed in the last 30 minutes against all volumes that have this

Heading	Description
mins	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.
Actions	Select the vertical drop-down menu for more details on an individual volume.

Viewing Individual Volume Details

From the **Volumes > Active Volumes** page, you can click the icon in the **Actions** column to view more information for an individual volume.

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

Account ID	System-generated ID for the volume.
Volume Size	Total size of the volume.
Used Capacity	Shows how full the volume is. Green = up to 80%. Yellow = above 80%. Red = above 95%.
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.

You can view additional details from the **Show Volume Details** drop-down menu.

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.
512e Enabled	Identifies if 512e is enabled on a volume.
Primary Node	Primary node for this volume.
Secondary Nodes	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.
Throttle	Identifies if the volume is being throttled due to high load on the primary storage node.
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.

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.
Unaligned Writes	For 512e volumes, the number of write operations that were not on a 4k sector boundary. High numbers of unaligned writes may indicate improper partition alignment.
IQN	The 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.

Viewing Individual Volume Performance Graphs

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.

Procedure

1. Select **Volumes > Active Volumes**.
2. In the **Actions** column, click the (⋮) icon for the volume you want and select **View Details**.
   A separate page opens to display an adjustable time line, which is synced with the performance graphs.
3. On the left, click on a thumbnail graph to view performance graphs in detail. The following graphs can be viewed.
   - Throughput
   - IOPS
   - Latency
   - Queue Depth
   - Average IO Size
   - Capacity
4. (Optional) If you want to export each graph as a CSV file, click the export button ( ).

Viewing Snapshots

You can view information about volume snapshots from **Volumes > Snapshots**.

Procedure

1. Select **Volumes > Snapshots**. Alternatively, click **Volumes > Active Volumes** and click on the link in the **Snapshots** column.
2. (Optional) If you want to export the list as a CSV file, click the export button ( ).

Snapshots Details

You can view snapshot details from the **Volumes > Snapshots** page that is available from the side panel for a selected cluster.

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

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. Possible Values: **Present**: The snapshot exists on a remote cluster. **Not Present**: The snapshot does not exist on a remote cluster. **Syncing**: The target cluster is currently replicating the snapshot. **Deleted**: The target replicated the snapshot and then deleted it.

Viewing Snapshot Schedules

You can view a list of snapshot schedules and their active settings from the **Snapshot Schedules** page for a selected cluster.

Procedure

1. Click **Volumes > Snapshot Schedules**.
2. (Optional) If you want to export the list as a CSV file, click the export button ( ).

Snapshot Schedules Details

On the **Volumes > Snapshot Schedules** page, you can view the following information:

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.

Replication

The **Replication** page, available from the side panel for a selected cluster, provides information about cluster pairs and volumes pairs.

See the following topics for additional information about cluster and volume pairs:

Cluster Pairs

Volume Pairs

Cluster Pairs

On the **Replication > Cluster Pairs** page for a selected cluster, you can view the following information about cluster pairs.

Heading	Description
Cluster Pair ID	ID number given when the cluster pair was created.
Remote Cluster Name	Name of the remote cluster of the pair.
Remote MVIP	Management Virtual IP of the remote cluster.
Replicating Volumes	Represents the number of volumes that are replicated on the paired cluster.
Status	State of the cluster pair.
UUID	Universally unique identifier.

Volume Pairs

On the **Replication > Volume Pairs** page for a selected cluster, you can view the following information about volume pairs.

Heading	Description
Volume ID	ID number given when the volume was created.
Account ID	ID of the account assigned to the volume.
Volume Status	State of the replicating volume.
Replication Mode	Type of mode selected for the volume pair.
Direction	Indicates the direction of the volume data: **Source** indicates data is being written to a target outside the cluster. **Target** indicates data is being written to the local volume from an outside source.
Async Delay	Length of time since the volume was last synced with the remote cluster. If the volume is not paired, this is null. **NOTE:** A target volume in an active replication state always has an Async Delay of 0 (zero). Target volumes are system-aware during replication and assume async delay is accurate at all times.
Remote Cluster	Name of the remote cluster on which the volume resides.
Remote Volume ID	Volume ID of the volume on the remote cluster.

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.

See the following topics to learn about VVols-related tasks:

- *Virtual Volumes Details*
- *Storage Containers*
- *Protocol Endpoints*
- *Hosts*
- *Bindings*

Virtual Volumes Details

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 0 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 UUID 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 GB or GiB.
Used Capacity	Current used capacity of the volume. Green = up to 80%. Yellow = above 80%. Red = above 95%.
Snapshot	The number of associated snapshots. Click the number to link to snapshot 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.

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. Possible values: **Active**: The storage container is in use. **Locked**: The storage container is locked.
PE Type	Indicates the protocol endpoint type (SCSI is the only available protocol for Element software).
Storage Container ID	The 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. Possible values: **Active**: The protocol endpoint is in use. **Start**: The protocol endpoint is starting. **Failover**: The protocol endpoint has failed over. **Reserved**: The protocol endpoint is reserved.
Provider Type	The type of the protocol endpoint's provider. Possible values: **Primary** **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 universally unique identifier (UUID) of the virtual volume.
VVol Secondary ID	The secondary ID of the virtual volume that is a SCSI second level LUN ID.

QoS Recommendations

The **QoS 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. Quality of service recommendations are only supported for clusters on Element 11 or later.

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.

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.

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

See the following topic to learn about filtering and understanding virtual machine data displayed in the UI:

- *Viewing Virtual Machine Details*

Viewing Virtual Machine Details

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

In addition to conventional filtering options that are available on all Active IQ pages, the **Virtual Machines** page has quick filter buttons that you can click 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 virtual machines associated with the storage cluster.
Status	The number of warnings or errors for the virtual machines.
Provisioned Resources	Total storage and memory resources for all virtual machines associated with the storage cluster.

Heading	Description
Name	The friendly name of the virtual machine.
Status	The availability status of the virtual machine. Possible values: Normal: The virtual machine is responding as expected. Warning: A warning has been reported. See vSphere for more details. Critical: A critical error has been reported. See vSphere for more details. Unknown: The virtual machine is inaccessible.
Power State	Indicates whether the virtual machine is powered on, powered off, or suspended.
Number of CPUs	The number of CPUs for each virtual machine.
CPU Usage	The percentage of actively used virtual CPU as a percentage of total available CPU in the VM.
Used Capacity	The percentage of virtual machine storage resources in use.
Peak Disk Latency	The maximum detected disk latency in milliseconds.
Alarms	The number of triggered vSphere alarms on the VM.

Where to Find Additional Information

You can learn about tasks related to the NetApp SolidFire storage system and NetApp HCI in NetApp's extensive documentation library.

NetApp Documentation

Contacting NetApp Support

If you need help or have questions or comments about NetApp products, contact NetApp Support:

- Web: mysupport.netapp.com
- Phone: 888.4.NETAPP (888.463.8277)

Web: netapp.com
Support: mysupport.netapp.com

April 2022