Manage events and alerts

Active IQ Unified Manager

NetApp
December 23, 2021

Table of Contents

Manage events and alerts

Managing events

Events help you to identify issues in the clusters that are monitored.

What Active IQ platform events are

Unified Manager can display events that have been discovered by the Active IQ platform. These events are created by running a set of rules against AutoSupport messages generated from all storage systems being monitored by Unified Manager.

For more information, see How Active IQ platform events are generated

Unified Manager checks for a new rules file automatically and only downloads a new file when there are newer rules. In sites with no external network access, you need to upload the rules manually from **Storage Management** > **Event Setup** > **Upload Rules**.

These Active IQ events do not overlap with existing Unified Manager events, and they identify incidents or risks concerning system configuration, cabling, best practice, and availability issues.

For more information about enabling platform events, see Enabling Active IQ portal events For more information about uploading rules file, see Uploading a new Active IQ rules file

NetApp Active IQ is a cloud based service that provides predictive analytics and proactive support to optimize storage system operations across the NetApp hybrid cloud. See NetApp Active IQ for more information.

What Event Management System events are

The Event Management System (EMS) collects event data from different parts of the ONTAP kernel and provides event forwarding mechanisms. These ONTAP events can be reported as EMS events in Unified Manager. Centralized monitoring and management eases configuration of critical EMS events and alert notifications based on these EMS events.

The Unified Manager address is added as a notification destination to the cluster when you add the cluster to Unified Manager. An EMS event is reported as soon as the event occurs in the cluster.

There are two methods for receiving EMS events in Unified Manager:

- A certain number of important EMS events are reported automatically.
- You can subscribe to receive individual EMS events.

The EMS events that are generated by Unified Manager are reported differently depending on the method in which the event was generated:

Functionality	Automatic EMS messages	Subscribed EMS messages
Available EMS events	Subset of EMS events	All EMS events

Functionality	Automatic EMS messages	Subscribed EMS messages
EMS message name when triggered	Unified Manager event name (converted from EMS event name)	Non-specific in the format "Error EMS received". The detailed message provides the dot-notation format of the actual EMS event
Messages received	As soon as the cluster has been discovered	After adding each required EMS event to Unified Manager, and after the next 15 minute polling cycle
Event life cycle	Same as other Unified Manager events: New, Acknowledged, Resolved, and Obsolete states	The EMS event is made obsolete after the cluster is refreshed, after 15 minutes, from when the event was created
Captures events during Unified Manager downtime	Yes, when the system starts up it communicates with each cluster to acquire missing events	No
Event details	Suggested corrective actions are imported directly from ONTAP to provide consistent resolutions	Corrective actions not available in Event Details page

Some of the new automatic EMS events are Informational events that indicate that a previous event has been resolved. For example, the "FlexGroup Constituents Space Status All OK" Informational event indicates that the "FlexGroup Constituents Have Space Issues" Error event has been resolved. Informational events cannot be managed using the same event life cycle as other event severity types, however, the event is obsoleted automatically if the same volume receives another “Space Issues” Error event.

EMS events that are added automatically to Unified Manager

The following ONTAP EMS events are added automatically to Unified Manager. These events will be generated when triggered on any cluster that Unified Manager is monitoring.

The following EMS events are available when monitoring clusters running ONTAP 9.5 or greater software:

Unified Manager Event name	EMS Event name	Affected resource	Unified Manager severity
Cloud Tier Access Denied for Aggregate Relocation	arl.netra.ca.check.failed	Aggregate	Error
Cloud Tier Access Denied for Aggregate Relocation During Storage Failover	gb.netra.ca.check.failed	Aggregate	Error

Unified Manager Event name	EMS Event name	Affected resource	Unified Manager severity
FabricPool Mirror Replication Resync Completed	wafl.ca.resync.complete	Cluster	Error
FabricPool Space Nearly Full	fabricpool.nearly.full	Cluster	Error
NVMe-oF Grace Period Started	nvmf.graceperiod.start	Cluster	Warning
NVMe-oF Grace Period Active	nvmf.graceperiod.active	Cluster	Warning
NVMe-oF Grace Period Expired	nvmf.graceperiod.expired	Cluster	Warning
LUN Destroyed	lun.destroy	LUN	Information
Cloud AWS MetaDataConnFail	cloud.aws.metadataConnFail	Node	Error
Cloud AWS IAMCredsExpired	cloud.aws.iamCredsExpired	Node	Error
Cloud AWS IAMCredsInvalid	cloud.aws.iamCredsInvalid	Node	Error
Cloud AWS IAMCredsNotFound	cloud.aws.iamCredsNotFound	Node	Error
Cloud AWS IAMCredsNotInitialized	cloud.aws.iamNotInitialized	Node	Information
Cloud AWS IAMRoleInvalid	cloud.aws.iamRoleInvalid	Node	Error
Cloud AWS IAMRoleNotFound	cloud.aws.iamRoleNotFound	Node	Error
Cloud Tier Host Unresolvable	objstore.host.unresolvable	Node	Error
Cloud Tier Intercluster LIF Down	objstore.interclusterlifDown	Node	Error

Unified Manager Event name	EMS Event name	Affected resource	Unified Manager severity
Request Mismatch Cloud Tier Signature	osc.signatureMismatch	Node	Error
One of NFSv4 Pools Exhausted	Nblade.nfsV4PoolExhaust	Node	Critical
QoS Monitor Memory Maxed	qos.monitor.memory.maxed	Node	Error
QoS Monitor Memory Abated	qos.monitor.memory.abated	Node	Information
NVMeNS Destroy	NVMeNS.destroy	Namespace	Information
NVMeNS Online	NVMeNS.offline	Namespace	Information
NVMeNS Offline	NVMeNS.online	Namespace	Information
NVMeNS Out of Space	NVMeNS.out.of.space	Namespace	Warning
Synchronous Replication Out Of Sync	sms.status.out.of.sync	SnapMirror relationship	Warning
Synchronous Replication Restored	sms.status.in.sync	SnapMirror relationship	Information
Synchronous Replication Auto Resync Failed	sms.resync.attempt.failed	SnapMirror relationship	Error
Many CIFS Connections	Nblade.cifsManyAuths	SVM	Error
Max CIFS Connection Exceeded	Nblade.cifsMaxOpenSameFile	SVM	Error
Max Number of CIFS Connection Per User Exceeded	Nblade.cifsMaxSessPerUsrConn	SVM	Error
CIFS NetBIOS Name Conflict	Nblade.cifsNbNameConflict	SVM	Error
Attempts to Connect Nonexistent CIFS Share	Nblade.cifsNoPrivShare	SVM	Critical

Unified Manager Event name	EMS Event name	Affected resource	Unified Manager severity
CIFS Shadow Copy Operation Failed	cifs.shadowcopy.failure	SVM	Error
Virus Found By AV Server	Nblade.vscanVirusDetected	SVM	Error
No AV Server Connection for Virus Scan	Nblade.vscanNoScannerConn	SVM	Critical
No AV Server Registered	Nblade.vscanNoRegdScanner	SVM	Error
No Responsive AV Server Connection	Nblade.vscanConnInactive	SVM	Information
AV Server too Busy to Accept New Scan Request	Nblade.vscanConnBackPressure	SVM	Error
Unauthorized User Attempt to AV Server	Nblade.vscanBadUserPrivAccess	SVM	Error
FlexGroup Constituents Have Space Issues	flexgroup.constituents.have.space.issues	Volume	Error
FlexGroup Constituents Space Status All OK	flexgroup.constituents.space.status.all.ok	Volume	Information
FlexGroup Constituents Have Inodes Issues	flexgroup.constituents.have.inodes.issues	Volume	Error
FlexGroup Constituents Inodes Status All OK	flexgroup.constituents.inodes.status.all.ok	Volume	Information
Volume Logical Space Nearly Full	monitor.vol.nearFull.inc.sav	Volume	Warning
Volume Logical Space Full	monitor.vol.full.inc.sav	Volume	Error
Volume Logical Space Normal	monitor.vol.one.ok.inc.sav	Volume	Information
WAFL Volume AutoSize Fail	wafl.vol.autoSize.fail	Volume	Error

Unified Manager Event name	EMS Event name	Affected resource	Unified Manager severity
WAFL Volume AutoSize Done	wafl.vol.autoSize.done	Volume	Information
WAFL READDIR File Operation Timeout	wafl.readdir.expired	Volume	Error

Subscribing to ONTAP EMS events

You can subscribe to receive Event Management System (EMS) events that are generated by systems that are installed with ONTAP software. A subset of EMS events are reported to Unified Manager automatically, but additional EMS events are reported only if you have subscribed to these events.

What you'll need

Do not subscribe to EMS events that are already added to Unified Manager automatically as this can cause confusion when receiving two events for the same issue.

You can subscribe to any number of EMS events. All the events to which you subscribe are validated, and only the validated events are applied to the clusters you are monitoring in Unified Manager. The *ONTAP 9 EMS Event Catalog* provides detailed information for all of the EMS messages for the specified version of ONTAP 9 software. Locate the appropriate version of the *EMS Event Catalog* from the ONTAP 9 Product Documentation page for a list of the applicable events.

ONTAP 9 Product Library

You can configure alerts for the ONTAP EMS events to which you subscribe, and you can create custom scripts to be executed for these events.

If you do not receive the ONTAP EMS events to which you have subscribed, there might be an issue with the DNS configuration of the cluster which is preventing the cluster from reaching the Unified Manager server. To resolve this issue, the cluster administrator must correct the DNS configuration of the cluster, and then restart Unified Manager. Doing so will flush the pending EMS events to the Unified Manager server.

Steps

1. In the left navigation pane, click **Storage Management** > **Event Setup**.
2. In the Event Setup page, click the **Subscribe to EMS events** button.
3. In the Subscribe to EMS events dialog box, enter the name of the ONTAP EMS event to which you want to subscribe.

   To view the names of the EMS events to which you can subscribe, from the ONTAP cluster shell, you can use the `event route show` command (prior to ONTAP 9) or the `event catalog show` command (ONTAP 9 or later).

   How to configure and receive alerts from ONTAP EMS Event Subscription in Active IQ Unified Manager

4. Click **Add**.

The EMS event is added to the Subscribed EMS events list, but the Applicable to Cluster column displays the status as “Unknown” for the EMS event that you added.

5. Click **Save and Close** to register the EMS event subscription with the cluster.
6. Click **Subscribe to EMS events** again.

   The status “Yes” appears in the Applicable to Cluster column for the EMS event that you added.

   If the status is not “Yes”, check the spelling of the ONTAP EMS event name. If the name is entered incorrectly, you must remove the incorrect event, and then add the event again.

When the ONTAP EMS event occurs, the event is displayed on the Events page. You can select the event to view details about the EMS event in the Event details page. You can also manage the disposition of the event or create alerts for the event.

What happens when an event is received

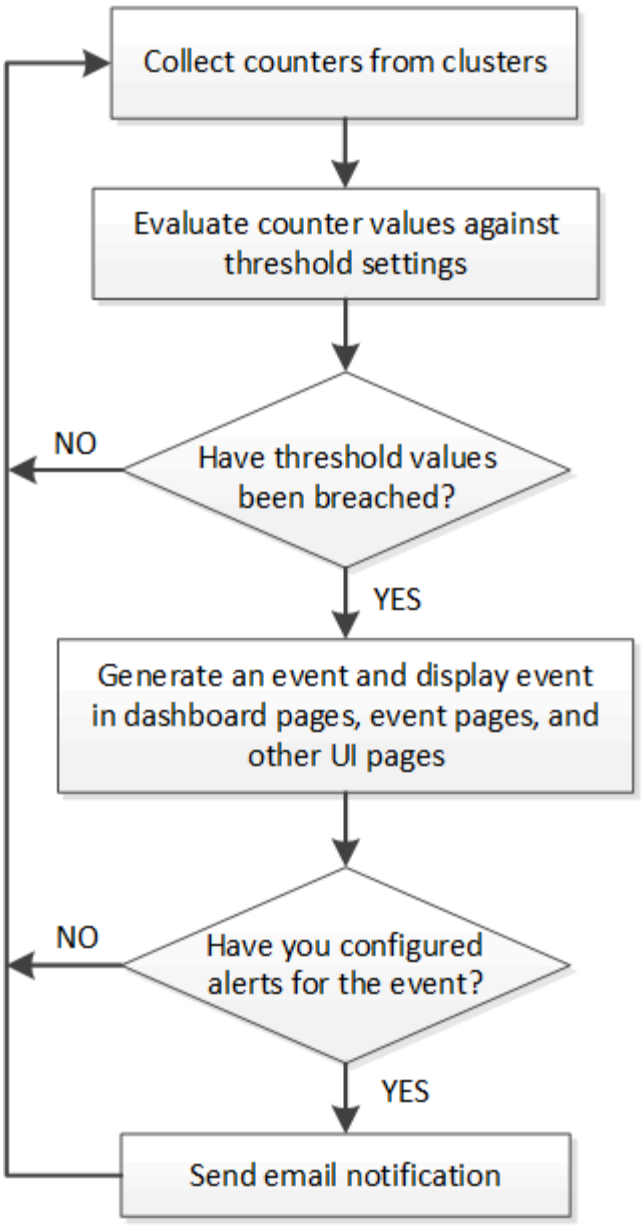
When Unified Manager receives an event, it is displayed in the Dashboard page, in the Event Management inventory page, in the Summary and Explorer tabs of the Cluster/Performance page, and in the object-specific inventory page (for example, the Volumes/Health inventory page).

When Unified Manager detects multiple continuous occurrences of the same event condition for the same cluster component, it treats all occurrences as a single event, not as separate events. The duration of the event is incremented to indicate that the event is still active.

Depending on how you configure settings in the Alert Setup page, you can notify other users about these events. The alert causes the following actions to be initiated:

- An email about the event can be sent to all Unified Manager Administrator users.
- The event can be sent to additional email recipients.
- An SNMP trap can be sent to the trap receiver.
- A custom script can be executed to perform an action.

This workflow is shown in the following diagram.



Viewing events and event details

You can view details about an event that is triggered by Unified Manager to take corrective action. For example, if there is a health event Volume Offline, you can click that event to view the details and perform corrective actions.

What you'll need

You must have the Operator, Application Administrator, or Storage Administrator role.

The event details include information such as the source of the event, cause of the event, and any notes related to the event.

Steps

1. In the left navigation pane, click **Event Management**.

   By default, the All active events view displays the New and Acknowledged (active) events that have been

generated over the previous 7 days that have an Impact Level of Incident or Risk.

2. If you want to view a particular category of events, for example, capacity events or performance events, click **View** and select from the menu of event types.
3. Click the event name for which you want to view the details.

   The event details are displayed in the Event details page.

Viewing unassigned events

You can view unassigned events and then assign each of them to a user who can resolve them.

What you'll need

You must have the Operator, Application Administrator, or Storage Administrator role.

Steps

1. In the left navigation pane, click **Event Management**.

   By default, New and Acknowledged events are displayed on the Event Management inventory page.

2. From the **Filters** pane, select the **Unassigned** filter option in the **Assigned To** area.

Acknowledging and resolving events

You should acknowledge an event before you start working on the issue that generated the event so that you do not continue to receive repeat alert notifications. After you take corrective action for a particular event, you should mark the event as resolved.

What you'll need

You must have the Operator, Application Administrator, or Storage Administrator role.

You can acknowledge and resolve multiple events simultaneously.

You cannot acknowledge Information events.

Steps

1. In the left navigation pane, click **Event Management**.
2. From the events list, perform the following actions to acknowledge the events:

If you want to…	Do this…
Acknowledge and mark a single event as resolved	a. Click the event name. b. From the Event details page, determine the cause of the event. c. Click **Acknowledge**. d. Take appropriate corrective action. e. Click **Mark As Resolved**.
Acknowledge and mark multiple events as resolved	a. Determine the cause of the events from the respective Event details page. b. Select the events. c. Click **Acknowledge**. d. Take appropriate corrective actions. e. Click **Mark As Resolved**.

After the event is marked resolved, the event is moved to the resolved events list.

3. **Optional**: In the **Notes and Updates** area, add a note about how you addressed the event, and then click **Post**.

Assigning events to specific users

You can assign unassigned events to yourself or to other users, including remote users. You can reassign assigned events to another user, if required. For example, when frequent issues occur on a storage object, you can assign the events for these issues to the user who manages that object.

What you'll need

- The user's name and email ID must be configured correctly.
- You must have the Operator, Application Administrator, or Storage Administrator role.

Steps

1. In the left navigation pane, click **Event Management**.
2. In the **Event Management** inventory page, select one or more events that you want to assign.
3. Assign the event by choosing one of the following options:

If you want to assign the event to…	Then do this…
Yourself	Click **Assign To** > **Me**.

If you want to assign the event to…	Then do this…
Another user	a. Click **Assign To** > **Another user**. b. In the Assign Owner dialog box, enter the user name, or select a user from the drop-down list. c. Click **Assign**. An email notification is sent to the user. If you do not enter a user name or select a user from the drop-down list, and click **Assign**, the event remains unassigned.

Disabling unwanted events

All events are enabled by default. You can disable events globally to prevent the generation of notifications for events that are not important in your environment. You can enable events that are disabled when you want to resume receiving notifications for them.

What you'll need

You must have the Application Administrator or Storage Administrator role.

When you disable events, the previously generated events in the system are marked obsolete, and the alerts that are configured for these events are not triggered. When you enable events that are disabled, the notifications for these events are generated starting with the next monitoring cycle.

When you disable an event for an object (for example, the `vol offline` event), and then later you enable the event, Unified Manager does not generate new events for objects that went offline when the event was in the disabled state. Unified Manager generates a new event only when there is a change in the object state after the event was re-enabled.

Steps

1. In the left navigation pane, click **Storage Management** > **Event Setup**.
2. In the **Event Setup** page, disable or enable events by choosing one of the following options:

If you want to…	Then do this…
Disable events	a. Click **Disable**. b. In the Disable Events dialog box, select the event severity. c. In the Matching Events column, select the events that you want to disable based on the event severity, and then click the right arrow to move those events to the Disable Events column. d. Click **Save and Close**. e. Verify that the events that you disabled are displayed in the list view of the Event Setup page.
Enable events	a. Select the check box for the event, or events, that you want to enable. b. Click **Enable**.

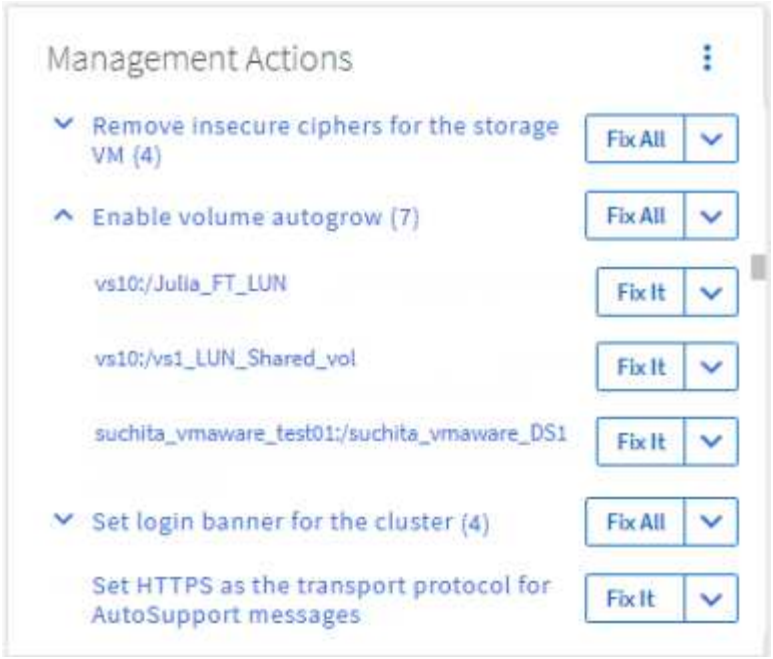
Fixing issues using Unified Manager automatic remediation

There are certain events that Unified Manager can diagnose thoroughly and provide a single resolution using the **Fix It** button. When available, those resolutions are displayed in the Dashboard, from the Event details page, and from the Workload Analysis selection on the left-navigation menu.

Most events have a variety of possible resolutions that are displayed in the Event details page so you can implement the best solution using ONTAP System Manager or the ONTAP CLI. A **Fix It** action is available when Unified Manager has determined that there is a single resolution to fix the issue, and that it can be resolved using an ONTAP CLI command.

Steps

1. To view events that can be fixed from the **Dashboard**, click **Dashboard**.



2. To resolve any of the issues that Unified Manager can fix, click the **Fix It** button. To fix an issue that exists on multiple objects, click the **Fix All** button.

For information about the issues that can be fixed by automatic remediation, see What issues can Unified Manager fix

Enabling and disabling Active IQ event reporting

Active IQ platform events are generated and displayed in the Unified Manager user interface by default. If you find that these events are too "noisy", or that you do not want to view these events in Unified Manager, then you can disable these events from being generated. You can enable them at a later time if you want to resume receiving these notifications.

What you'll need

You must have the Application Administrator role.

When you disable this feature, Unified Manager stops receiving Active IQ platform events immediately.

When you enable this feature, Unified Manager starts receiving Active IQ platform events shortly after midnight based on the timezone of the cluster. The start time is based on when Unified Manager receives AutoSupport messages from each cluster.

Steps

1. In the left navigation pane, click **General** > **Feature Settings**.
2. In the **Feature Settings** page, disable or enable Active IQ platform events by choosing one of the following options:

If you want to…	Then do this…
Disable Active IQ platform events	In the **Active IQ Portal Events** panel, move the slider button to the left.
Enable Active IQ platform events	In the **Active IQ Portal Events** panel, move the slider button to the right.

Uploading a new Active IQ rules file

Unified Manager checks for a new Active IQ rules file automatically and downloads a new file when there are newer rules. However, in sites with no external network access, you need to upload the rules file manually.

What you'll need

- Active IQ event reporting must be enabled.
- You must download the rules file from the NetApp Support Site.

It is recommended that you download a new rules file approximately once a month to make sure your storage systems are being protected and that they are running optimally. The rules file is located at: http://mysupport.netapp.com/NOW/public/unified_manager/bin/secure_rules.zip

Steps

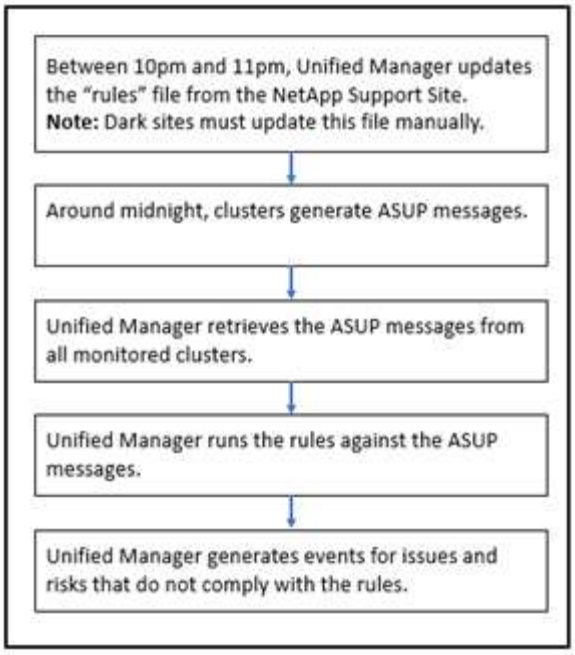
1. On a computer that has network access, navigate to the NetApp Support Site and download the current rules `.zip` file.
2. Transfer the rules file to some media that you can bring into the secure area and then copy it onto a system in the secure area.
3. In the left navigation pane, click **Storage Management** > **Event Setup**.
4. In the **Event Setup** page, click the **Upload Rules** button.
5. In the **Upload Rules** dialog box, navigate to and select the rules `.zip` file you downloaded and click **Upload**.

   This process can take a few minutes.

The rules file is unzipped on the Unified Manager server. After your managed clusters generate an AutoSupport file after midnight Unified Manager will check the clusters against the rules file and generate new risk and incident events if required.

How Active IQ platform events are generated

Active IQ platform incidents and risks are converted to Unified Manager events as shown in the following diagram.

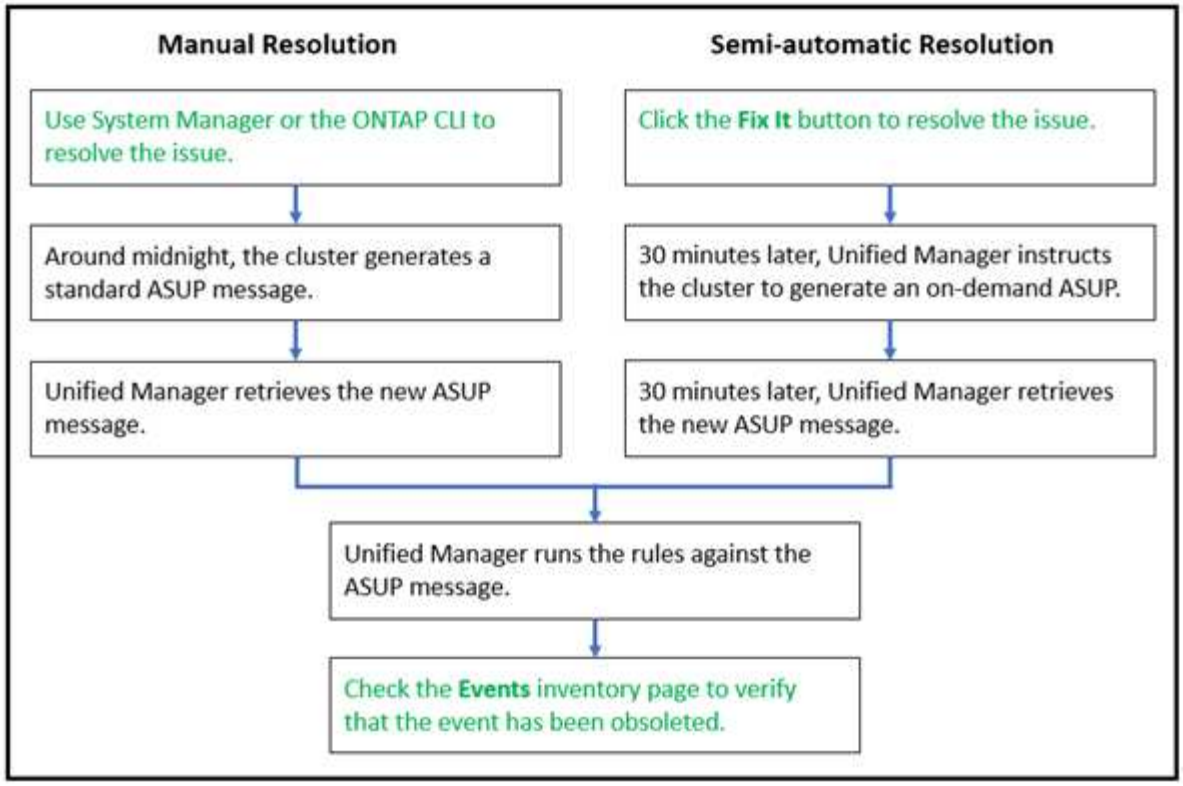


As you can see, the rules file that is compiled on the Active IQ platform is kept current, cluster AutoSupport messages are generated daily, and Unified Manager updates the list of events on a daily basis.

Resolving Active IQ platform events

Active IQ platform incidents and risks are similar to other Unified Manager events because they can be assigned to other users for resolution and they have the same available states. However, when you resolve these types of events using the **Fix It** button you can verify the resolution within hours.

The following diagram shows the actions you must take (in green) and the action that Unified Manager takes (in black) when resolving events that were generated from the Active IQ platform.



When performing a manual resolution you must log into System Manager or the ONTAP command-line interface to fix the issue. You will be able to verify the issue only after the cluster generates a new AutoSupport message at midnight.

When performing a semi-automatic resolution using the **Fix It** button you are able to verify that the fix was successful within hours.

Configuring event retention settings

You can specify the number of months an event is retained in the Unified Manager server before it is automatically deleted.

What you'll need

You must have the Application Administrator role.

Retaining events for more than 6 months could affect the server performance and is not recommended.

Steps

1. In the left navigation pane, click **General** > **Data Retention**.
2. In the **Data Retention** page, select the slider in the Event Retention area and move it to the number of months that events should be retained, and click **Save**.

What a Unified Manager maintenance window is

You define a Unified Manager maintenance window to suppress events and alerts for a specific timeframe when you have scheduled cluster maintenance and you do not want to receive a flood of unwanted notifications.

When the maintenance window starts, an "Object Maintenance Window Started" event is posted to the Event Management inventory page. This event is obsoleted automatically when the maintenance window ends.

During a maintenance window the events related to all objects on that cluster are still generated, but they do not appear in any of the UI pages, and no alerts or other types of notification are sent for these events. You can, however, view the events that were generated for all storage objects during a maintenance window by selecting one of the View options on the Event Management inventory page.

You can schedule a maintenance window to be initiated in the future, you can change the start and end times for a scheduled maintenance window, and you can cancel a scheduled maintenance window.

Scheduling a maintenance window to disable cluster event notifications

If you have a planned downtime for a cluster, for example, to upgrade the cluster or to move one of the nodes, you can suppress the events and alerts that would normally be generated during that timeframe by scheduling a Unified Manager maintenance window.

What you'll need

You must have the Application Administrator or Storage Administrator role.

During a maintenance window, the events related to all objects on that cluster are still generated, but they do not appear in the event page, and no alerts or other types of notification are sent for these events.

The time you enter for the maintenance window is based on the time at the Unified Manager server.

Steps

1. In the left navigation pane, click **Storage Management** > **Cluster Setup**.
2. In the **Maintenance Mode** column for the cluster, select the slider button and move it to the right.

   The calendar window is displayed.

3. Select the start and end date and time for the maintenance window and click **Apply**.

   The message "Scheduled" appears next to the slider button.

When the start time is reached the cluster goes into maintenance mode and an "Object Maintenance Window Started" event is generated.

Changing or canceling a scheduled maintenance window

If you have configured a Unified Manager maintenance window to occur in the future, you can change the start and end times or cancel the maintenance window from occurring.

What you'll need

You must have the Application Administrator or Storage Administrator role.

Canceling a currently running maintenance window is useful if you have completed cluster maintenance before the scheduled maintenance window end time and you want to start receiving events and alerts from the cluster again.

Steps

1. In the left navigation pane, click **Storage Management** > **Cluster Setup**.
2. In the **Maintenance Mode** column for the cluster:

If you want to…	Perform this step…
Change the timeframe for a scheduled maintenance window	a. Click the text "Scheduled" next to the slider button. b. Change the start and/or end date and time and click **Apply**.
Extend the length of an active maintenance window	a. Click the text "Active" next to the slider button. b. Change the end date and time and click **Apply**.
Cancel a scheduled maintenance window	Select the slider button and move it to the left.
Cancel an active maintenance window	Select the slider button and move it to the left.

Viewing events that occurred during a maintenance window

If necessary, you can view the events that were generated for all storage objects during a Unified Manager maintenance window. Most events will appear in the Obsolete state once the maintenance window has completed and all system resources are back up and running.

What you'll need

At least one maintenance window must have completed before any events are available.

Events that occurred during a maintenance window do not appear on the Event Management inventory page by default.

Steps

1. In the left navigation pane, click **Events**.

   By default, all active (New and Acknowledged) events are displayed on the Event Management inventory page.

2. From the View pane, select the option **All events generated during maintenance**.

   The list of events trigged during the last 7 days from all maintenance window sessions and from all clusters are displayed.

3. If there have been multiple maintenance windows for a single cluster, you can click the **Triggered Time** calendar icon and select the period of time for the maintenance window events that you are interested in viewing.

Managing host system resource events

Unified Manager includes a service that monitors resource issues on the host system on

which Unified Manager is installed. Issues such as lack of available disk space or lack of memory on the host system may trigger management station events that are displayed as banner messages across the top of the UI.

Management station events indicate an issue with the host system on which Unified Manager is installed. Examples of management station issues include disk space running low on the host system; Unified Manager missing a regular data collection cycle; and noncompletion, or late completion, of statistics analysis because the next collection poll was initiated.

Unlike all other Unified Manager event messages, these particular management station warning and critical events are displayed in banner messages.

Step

1. To view management station event information, perform these actions:

If you want to…	Do this…
View details of the event	Click the event banner to display the Event details page that includes suggested solutions for the issue.
View all management station events	a. In the left navigation pane, click **Event Management**. b. In the Filters pane on the Event Management inventory page, click the box for Management Station in the Source Type list.

Understanding more about events

Understanding the concepts about events helps you to manage your clusters and cluster objects efficiently and to define alerts appropriately.

Event state definitions

The state of an event helps you identify whether an appropriate corrective action is required. An event can be New, Acknowledged, Resolved, or Obsolete. Note that both New and Acknowledged events are considered to be active events.

The event states are as follows:

- **New**

  The state of a new event.

- **Acknowledged**

  The state of an event when you have acknowledged it.

- **Resolved**

  The state of an event when it is marked as resolved.

- **Obsolete**

  The state of an event when it is automatically corrected or when the cause of the event is no longer valid.

  You cannot acknowledge or resolve an obsolete event.

Example of different states of an event

The following examples illustrate the manual and automatic event state changes.

When the event Cluster Not Reachable is triggered, the event state is New. When you acknowledge the event, the event state changes to Acknowledged. When you have taken an appropriate corrective action, you must mark the event as resolved. The event state then changes to Resolved.

If the Cluster Not Reachable event is generated due to a power outage, then when the power is restored the cluster starts functioning without any administrator intervention. Therefore, the Cluster Not Reachable event is no longer valid, and the event state changes to Obsolete in the next monitoring cycle.

Unified Manager sends an alert when an event is in the Obsolete or Resolved state. The email subject line and email content of an alert provides information about the event state. An SNMP trap also includes information about the event state.

Description of event severity types

Each event is associated with a severity type to help you prioritize the events that require immediate corrective action.

- **Critical**

  A problem occurred that might lead to service disruption if corrective action is not taken immediately.

  Performance critical events are sent from user-defined thresholds only.

- **Error**

  The event source is still performing; however, corrective action is required to avoid service disruption.

- **Warning**

  The event source experienced an occurrence that you should be aware of, or a performance counter for a cluster object is out of normal range and should be monitored to make sure it does not reach the critical severity. Events of this severity do not cause service disruption, and immediate corrective action might not be required.

  Performance warning events are sent from user-defined, system-defined, or dynamic thresholds.

- **Information**

  The event occurs when a new object is discovered, or when a user action is performed. For example, when any storage object is deleted or when there are any configuration changes, the event with severity type Information is generated.

  Information events are sent directly from ONTAP when it detects a configuration change.

Description of event impact levels

Each event is associated with an impact level (Incident, Risk, Event, or Upgrade) to help you prioritize the events that require immediate corrective action.

- **Incident**

  An incident is a set of events that can cause a cluster to stop serving data to the client and run out of space for storing data. Events with an impact level of Incident are the most severe. Immediate corrective action should be taken to avoid service disruption.

- **Risk**

  A risk is a set of events that can potentially cause a cluster to stop serving data to the client and run out of space for storing data. Events with an impact level of Risk can cause service disruption. Corrective action might be required.

- **Event**

  An event is a state or status change of storage objects and their attributes. Events with an impact level of Event are informational and do not require corrective action.

- **Upgrade**

  Upgrade events are a specific type of event reported from the Active IQ platform. These events identify issues where the resolution requires you to upgrade ONTAP software, node firmware, or operating system software (for security advisories). You may want to perform immediate corrective action for some of these issues, whereas other issues may be able to wait until your next scheduled maintenance.

Description of event impact areas

Events are categorized into six impact areas (availability, capacity, configuration, performance, protection, and security) to enable you to concentrate on the types of events for which you are responsible.

- **Availability**

  Availability events notify you if a storage object goes offline, if a protocol service goes down, if an issue with storage failover occurs, or if an issue with hardware occurs.

- **Capacity**

  Capacity events notify you if your aggregates, volumes, LUNs, or namespaces are approaching or have reached a size threshold, or if the rate of growth is unusual for your environment.

- **Configuration**

  Configuration events inform you of the discovery, deletion, addition, removal, or renaming of your storage objects. Configuration events have an impact level of Event and a severity type of Information.

- **Performance**

  Performance events notify you of resource, configuration, or activity conditions on your cluster that might adversely affect the speed of data storage input or retrieval on your monitored storage objects.

- **Protection**

  Protection events notify you of incidents or risks involving SnapMirror relationships, issues with destination capacity, problems with SnapVault relationships, or issues with protection jobs. Any ONTAP object (especially aggregates, volumes, and SVMs) that host secondary volumes and protection relationships are categorized in the protection impact area.

- **Security**

  Security events notify you of how secure your ONTAP clusters, storage virtual machines (SVMs), and volumes are based on parameters defined in the NetApp Security Hardening Guide for ONTAP 9.

  Additionally, this area includes upgrade events that are reported from the Active IQ platform.

How object status is computed

Object status is determined by the most severe event that currently holds a New or Acknowledged state. For example, if an object status is Error, then one of the object's events has a severity type of Error. When corrective action has been taken, the event state moves to Resolved.

Dynamic performance event chart details

For dynamic performance events, the System Diagnosis section of the Event details page lists the top workloads with the highest latency or usage of the cluster component that is in contention. The performance statistics are based on the time the performance event was detected up to the last time the event was analyzed. The charts also display historical performance statistics for the cluster component that is in contention.

For example, you can identify workloads with high utilization of a component to determine which workload to move to a less-utilized component. Moving the workload would reduce the amount of work on the current component, possibly bringing the component out of contention. At the of this section is the time and date range when an event was detected and last analyzed. For active events (new or acknowledged), the last analyzed time continues to update.

The latency and activity charts display the names of the top workloads when you hover your cursor over the chart. Clicking the Workload Type menu at the right of the chart enables you to sort the workloads based on their role in the event, including *sharks*, *bullies*, or *victims*, and displays details about their latency and their usage on the cluster component in contention. You can compare the actual value to the expected value to see when the workload was outside its expected range of latency or usage. See *Workloads monitored by Unified Manager*.

> When you sort by peak deviation in latency, system-defined workloads are not displayed in the table, because latency applies only to user-defined workloads. Workloads with very low latency values are not displayed in the table.

For more information about the dynamic performance thresholds, see *What events are*. For information about how Unified Manager ranks the workloads and determines the sort order, see *How Unified Manager determines the performance impact for an event*.

The data in the graphs shows 24 hours of performance statistics prior to the last time the event was analyzed. The actual values and expected values for each workload are based on the time the workload was involved in

the event. For example, a workload might become involved in an event after the event was detected, so its performance statistics might not match the values at the time of event detection. By default, the workloads are sorted by peak (highest) deviation in latency.

Because Unified Manager retains a maximum of 30 days of 5-minute historical performance and event data, if the event is more than 30 days old, no performance data is displayed.

- **Workload Sort column**
  - **Latency chart**

    Displays the impact of the event to the latency of the workload during the last analysis.

  - **Component Usage column**

    Displays details about the workload usage of the cluster component in contention. In the graphs, the actual usage is a blue line. A red bar highlights the event duration, from the detection time to the last analyzed time. For more information, see *Workload performance measurements*.

    For the network component, because network performance statistics come from activity off the cluster, this column is not displayed.

  - **Component Usage**

    Displays the history of utilization, in percent, for the network processing, data processing, and aggregate components or the history of activity, in percent, for the QoS policy group component. The chart is not displayed for the network or interconnect components. You can point to the statistics to view the usage statistics at a specific point in time.

  - **Total Write MB/s History**

    For the MetroCluster Resources component only, shows the total write throughput, in megabytes per second (MBps), for all volume workloads that are being mirrored to the partner cluster in a MetroCluster configuration.

  - **Event History**

    Displays red-shaded lines to indicate the historic events for the component in contention. For obsolete events, the chart displays events that occurred before the selected event was detected and after it was resolved.

Configuration changes detected by Unified Manager

Unified Manager monitors your clusters for configuration changes to help you determine whether a change might have caused or contributed to a performance event. The Performance Explorer pages display a change event icon ( ) to indicate the date and time when the change was detected.

You can review the performance charts in the Performance Explorer pages and in the Workload Analysis page to see whether the change event impacted the performance of the selected cluster object. If the change was detected at or around the same time as a performance event, the change might have contributed to the issue, which caused the event alert to trigger.

Unified Manager can detect the following change events, which are categorized as Informational events:

- A volume moves between aggregates.

  Unified Manager can detect when the move is in progress, completed, or failed. If Unified Manager is down during a volume move, when it is back up it detects the volume move and displays a change event for it.

- The throughput (MB/s or IOPS) limit of a QoS policy group that contains one or more monitored workloads changes.

  Changing a policy group limit can cause intermittent spikes in the latency (response time), which might also trigger events for the policy group. The latency gradually returns to normal and any events caused by the spikes become obsolete.

- A node in an HA pair takes over or gives back the storage of its partner node.

  Unified Manager can detect when the takeover, partial takeover, or giveback operation has been completed. If the takeover is caused by a panicked node, Unified Manager does not detect the event.

- An ONTAP upgrade or revert operation is completed successfully.

  The previous version and new version are displayed.

List of events and severity types

You can use the list of events to become more familiar with event categories, event names, and the severity type of each event that you might see in Unified Manager. Events are listed in alphabetical order by object category.

Aggregate events

Aggregate events provide you with information about the status of aggregates so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

An asterisk (*) identifies EMS events that have been converted to Unified Manager events.

Event name(Trap name)	Impact level	Source type	Severity
Aggregate Offline(ocumEvtAggregateStateOffline)	Incident	Aggregate	Critical
Aggregate Failed(ocumEvtAggregateStateFailed)	Incident	Aggregate	Critical

Event name(Trap name)	Impact level	Source type	Severity
Aggregate Restricted(ocumEvtAggregateStateRestricted)	Risk	Aggregate	Warning
Aggregate Reconstructing(ocumEvtAggregateRaidStateReconstructing)	Risk	Aggregate	Warning
Aggregate Degraded(ocumEvtAggregateRaidStateDegraded)	Risk	Aggregate	Warning
Cloud Tier Partially Reachable(ocumEventCloudTierPartiallyReachable)	Risk	Aggregate	Warning
Cloud Tier Unreachable(ocumEventCloudTierUnreachable)	Risk	Aggregate	Error
Cloud Tier Access Denied for Aggregate Relocation *(arlNetraCaCheckFailed)	Risk	Aggregate	Error
Cloud Tier Access Denied for Aggregate Relocation During Storage Failover *(gbNetraCaCheckFailed)	Risk	Aggregate	Error
MetroCluster Aggregate Left Behind(ocumEvtMetroClusterAggregateLeftBehind)	Risk	Aggregate	Error
MetroCluster Aggregate Mirroring Degraded(ocumEvtMetroClusterAggregateMirrorDegraded)	Risk	Aggregate	Error

Impact area: capacity

Event name(Trap name)	Impact level	Source type	Severity
Aggregate Space Nearly Full(ocumEvtAggregateNearlyFull)	Risk	Aggregate	Warning
Aggregate Space Full(ocumEvtAggregateFull)	Risk	Aggregate	Error
Aggregate Days Until Full(ocumEvtAggregateDaysUntilFullSoon)	Risk	Aggregate	Error
Aggregate Overcommitted(ocumEvtAggregateOvercommitted)	Risk	Aggregate	Error
Aggregate Nearly Overcommitted(ocumEvtAggregateAlmostOvercommitted)	Risk	Aggregate	Warning
Aggregate Snapshot Reserve Full(ocumEvtAggregateSnapReserveFull)	Risk	Aggregate	Warning
Aggregate Growth Rate Abnormal(ocumEvtAggregateGrowthRateAbnormal)	Risk	Aggregate	Warning

Impact area: configuration

Event name(Trap name)	Impact level	Source type	Severity
Aggregate Discovered(Not applicable)	Event	Aggregate	Information
Aggregate Renamed(Not applicable)	Event	Aggregate	Information
Aggregate Deleted(Not applicable)	Event	Node	Information

Impact area: performance

Event name(Trap name)	Impact level	Source type	Severity
Aggregate IOPS Critical Threshold Breached(ocumAggregateIopsIncident)	Incident	Aggregate	Critical
Aggregate IOPS Warning Threshold Breached(ocumAggregateIopsWarning)	Risk	Aggregate	Warning
Aggregate MB/s Critical Threshold Breached(ocumAggregateMbpsIncident)	Incident	Aggregate	Critical
Aggregate MB/s Warning Threshold Breached(ocumAggregateMbpsWarning)	Risk	Aggregate	Warning
Aggregate Latency Critical Threshold Breached(ocumAggregateLatencyIncident)	Incident	Aggregate	Critical
Aggregate Latency Warning Threshold Breached(ocumAggregateLatencyWarning)	Risk	Aggregate	Warning
Aggregate Performance Capacity Used Critical Threshold Breached(ocumAggregatePerfCapacityUsedIncident)	Incident	Aggregate	Critical
Aggregate Performance Capacity Used Warning Threshold Breached(ocumAggregatePerfCapacityUsedWarning)	Risk	Aggregate	Warning

Event name(Trap name)	Impact level	Source type	Severity
Aggregate Utilization Critical Threshold Breached (ocumAggregateUtilizationIncident)	Incident	Aggregate	Critical
Aggregate Utilization Warning Threshold Breached (ocumAggregateUtilizationWarning)	Risk	Aggregate	Warning
Aggregate Disks Over-utilized Threshold Breached (ocumAggregateDisksOverUtilizedWarning)	Risk	Aggregate	Warning
Aggregate Dynamic Threshold Breached (ocumAggregateDynamicEventWarning)	Risk	Aggregate	Warning

Cluster events

Cluster events provide information about the status of clusters, which enables you to monitor the clusters for potential problems. The events are grouped by impact area, and include the event name, trap name, impact level, source type, and severity.

Impact area: availability

An asterisk (*) identifies EMS events that have been converted to Unified Manager events.

Event name (Trap name)	Impact level	Source type	Severity
Cluster Lacks Spare Disks(ocumEvtDisksNoSpares)	Risk	Cluster	Warning
Cluster Not Reachable(ocumEvtClusterUnreachable)	Risk	Cluster	Error
Cluster Monitoring Failed(ocumEvtClusterMonitoringFailed)	Risk	Cluster	Warning

Event name (Trap name)	Impact level	Source type	Severity
Cluster FabricPool License Capacity Limits Breached (ocumEvtExternalCapacityTierSpaceFull)	Risk	Cluster	Warning
NVMe-oF Grace Period Started *(nvmfGracePeriodStart)	Risk	Cluster	Warning
NVMe-oF Grace Period Active *(nvmfGracePeriodActive)	Risk	Cluster	Warning
NVMe-oF Grace Period Expired *(nvmfGracePeriodExpired)	Risk	Cluster	Warning
Object Maintenance Window Started(objectMaintenanceWindowStarted)	Event	Cluster	Critical
Object Maintenance Window Ended(objectMaintenanceWindowEnded)	Event	Cluster	Information
MetroCluster Spare Disks Left Behind(ocumEvtSpareDiskLeftBehind)	Risk	Cluster	Error
MetroCluster Automatic Unplanned Switchover Disabled(ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	Risk	Cluster	Warning
Cluster user password changed *(cluster.passwd.changed)	Event	Cluster	Information

Impact area: capacity

Event name(Trap name)	Impact level	Source type	Severity
Cluster Capacity Imbalance Threshold Breached(ocumConformanceNodeImbalanceWarning)	Risk	Cluster	Warning
Cluster Cloud Tier Planning (clusterCloudTierPlanningWarning)	Risk	Cluster	Warning
FabricPool Mirror Replication Resync Completed *(waflCaResyncComplete)	Event	Cluster	Warning
FabricPool Space Nearly Full *(fabricpoolNearlyFull)	Risk	Cluster	Error

Impact area: configuration

Event name(Trap name)	Impact level	Source type	Severity
Node Added(Not applicable)	Event	Cluster	Information
Node Removed(Not applicable)	Event	Cluster	Information
Cluster Removed(Not applicable)	Event	Cluster	Information
Cluster Add Failed(Not applicable)	Event	Cluster	Error
Cluster Name Changed(Not applicable)	Event	Cluster	Information
Emergency EMS received (Not applicable)	Event	Cluster	Critical
Critical EMS received (Not applicable)	Event	Cluster	Critical

Event name(Trap name)	Impact level	Source type	Severity
Alert EMS received (Not applicable)	Event	Cluster	Error
Error EMS received (Not applicable)	Event	Cluster	Warning
Warning EMS received (Not applicable)	Event	Cluster	Warning
Debug EMS received (Not applicable)	Event	Cluster	Warning
Notice EMS received (Not applicable)	Event	Cluster	Warning
Informational EMS received (Not applicable)	Event	Cluster	Warning

ONTAP EMS events are categorized into three Unified Manager event severity levels.

Unified Manager event severity level	ONTAP EMS event severity level
Critical	Emergency Critical
Error	Alert
Warning	Error Warning Debug Notice Informational

Impact area: performance

Event name(Trap name)	Impact level	Source type	Severity
Cluster Load Imbalance Threshold Breached()	Risk	Cluster	Warning

Event name(Trap name)	Impact level	Source type	Severity
Cluster IOPS Critical Threshold Breached(ocumClusterIopsIncident)	Incident	Cluster	Critical
Cluster IOPS Warning Threshold Breached(ocumClusterIopsWarning)	Risk	Cluster	Warning
Cluster MB/s Critical Threshold Breached(ocumClusterMbpsIncident)	Incident	Cluster	Critical
Cluster MB/s Warning Threshold Breached(ocumClusterMbpsWarning)	Risk	Cluster	Warning
Cluster Dynamic Threshold Breached(ocumClusterDynamicEventWarning)	Risk	Cluster	Warning

Impact area: security

Event name(Trap name)	Impact level	Source type	Severity
AutoSupport HTTPS Transport Disabled(ocumClusterASUPHttpsConfiguredDisabled)	Risk	Cluster	Warning
Log Forwarding Not Encrypted(ocumClusterAuditLogUnencrypted)	Risk	Cluster	Warning
Default Local Admin User Enabled(ocumClusterDefaultAdminEnabled)	Risk	Cluster	Warning
FIPS Mode Disabled(ocumClusterFipsDisabled)	Risk	Cluster	Warning

Event name(Trap name)	Impact level	Source type	Severity
Login Banner Disabled(ocumClusterLoginBannerDisabled)	Risk	Cluster	Warning
Login Banner Changed(ocumClusterLoginBannerChanged)	Risk	Cluster	Warning
Log Forwarding Destinations Changed(ocumLogForwardDestinationsChanged)	Risk	Cluster	Warning
NTP Server Names Changed(ocumNtpServerNamesChanged)	Risk	Cluster	Warning
NTP Server Count is Low(securityConfigNTPServerCountLowRisk)	Risk	Cluster	Warning
Cluster Peer Communication Not Encrypted(ocumClusterPeerEncryptionDisabled)	Risk	Cluster	Warning
SSH is Using Insecure Ciphers(ocumClusterSSHInsecure)	Risk	Cluster	Warning
Telnet Protocol Enabled(ocumClusterTelnetEnabled)	Risk	Cluster	Warning
Passwords of some ONTAP user accounts use the less secure MD5 hash function(ocumClusterMD5PasswordHashUsed)	Risk	Cluster	Warning
Cluster uses self-signed Certificate(ocumClusterSelfSignedCertificate)	Risk	Cluster	Warning

Event name(Trap name)	Impact level	Source type	Severity
Cluster Remote Shell is Enabled(ocumClusterRshDisabled)	Risk	Cluster	Warning

Disks events

Disks events provide you with information about the status of disks so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Flash Disks - Spare Blocks Almost Consumed(ocumEvtClusterFlashDiskFewerSpareBlockError)	Risk	Cluster	Error
Flash Disks - No Spare Blocks(ocumEvtClusterFlashDiskNoSpareBlockCritical)	Incident	Cluster	Critical
Some Unassigned Disks(ocumEvtClusterUnassignedDisksSome)	Risk	Cluster	Warning
Some Failed Disks(ocumEvtDisksSomeFailed)	Incident	Cluster	Critical

Enclosures events

Enclosures events provide you with information about the status of disk shelf enclosures in your data center so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Disk Shelf Fans Failed(ocumEvtShelfFanFailed)	Incident	Storage shelf	Critical

Event name (Trap name)	Impact level	Source type	Severity
Disk Shelf Power Supplies Failed(ocumEvtShelfPowerSupplyFailed)	Incident	Storage shelf	Critical
Disk Shelf Multipath Not Configured(ocumDiskShelfConnectivityNotInMultiPath) This event does not apply to: • Clusters that are in a MetroCluster configuration • The following platforms: FAS2554, FAS2552, FAS2520, and FAS2240	Risk	Node	Warning
Disk Shelf Path Failure(ocumDiskShelfConnectivityPathFailure)	Risk	Storage Shelf	Warning

Impact area: configuration

Event name (Trap name)	Impact level	Source type	Severity
Disk Shelf Discovered(Not applicable)	Event	Node	Information
Disk Shelves Removed(Not applicable)	Event	Node	Information

Fans events

Fans events provide you with information about the status fans on nodes in your data center so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
One or More Failed Fans(ocumEvtFansOneOrMoreFailed)	Incident	Node	Critical

Flash card events

Flash card events provide you with information about the status of the flash cards installed on nodes in your data center so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Flash Cards Offline(ocumEvtFlashCardOffline)	Incident	Node	Critical

Inodes events

Inode events provide information when the inode is full or nearly full so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: capacity

Event name (Trap name)	Impact level	Source type	Severity
Inodes Nearly Full(ocumEvtInodesAlmostFull)	Risk	Volume	Warning
Inodes Full(ocumEvtInodesFull)	Risk	Volume	Error

Network interface (LIF) events

Network interface events provide information about the status of your network interface (LIFs), so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Network Interface Status Down(ocumEvtLifStatusDown)	Risk	Interface	Error
FC/FCoE Network Interface Status Down(ocumEvtFCLifStatusDown)	Risk	Interface	Error
Network Interface Failover Not Possible(ocumEvtLifFailoverNotPossible)	Risk	Interface	Warning
Network Interface Not At Home Port(ocumEvtLifNotAtHomePort)	Risk	Interface	Warning

Impact area: configuration

Event name (Trap name)	Impact level	Source type	Severity
Network Interface Route Not Configured(Not applicable)	Event	Interface	Information

Impact area: performance

Event name (Trap name)	Impact level	Source type	Severity
Network Interface MB/s Critical Threshold Breached(ocumNetworkLifMbpsIncident)	Incident	Interface	Critical
Network Interface MB/s Warning Threshold Breached(ocumNetworkLifMbpsWarning)	Risk	Interface	Warning
FC Network Interface MB/s Critical Threshold Breached(ocumFcpLifMbpsIncident)	Incident	Interface	Critical

Event name (Trap name)	Impact level	Source type	Severity
FC Network Interface MB/s Warning Threshold Breached(ocumFcpLifMbpsWarning)	Risk	Interface	Warning
NVMf FC Network Interface MB/s Critical Threshold Breached(ocumNvmfFcLifMbpsIncident)	Incident	Interface	Critical
NVMf FC Network Interface MB/s Warning Threshold Breached(ocumNvmfFcLifMbpsWarning)	Risk	Interface	Warning

LUN events

LUN events provide you with information about the status of your LUNs, so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

An asterisk (*) identifies EMS events that have been converted to Unified Manager events.

Event name (Trap name)	Impact level	Source type	Severity
LUN Offline(ocumEvtLunOffline)	Incident	LUN	Critical
LUN Destroyed *(lunDestroy)	Event	LUN	Information
LUN mapped with unsupported operating system in igroup(igroupUnsupportedOsType)	Incident	LUN	Warning
Single Active Path To Access LUN(ocumEvtLunSingleActivePath)	Risk	LUN	Warning

Event name (Trap name)	Impact level	Source type	Severity
No Active Paths To Access LUN(ocumEvtLunNotReachable)	Incident	LUN	Critical
No Optimized Paths To Access LUN(ocumEvtLunOptimizedPathInactive)	Risk	LUN	Warning
No Paths To Access LUN From HA Partner(ocumEvtLunHaPathInactive)	Risk	LUN	Warning
No Path to Access LUN from one Node in HA-pair(ocumEvtLunNodePathStatusDown)	Risk	LUN	Error

Impact area: capacity

Event name (Trap name)	Impact level	Source type	Severity
Insufficient Space For LUN Snapshot Copy(ocumEvtLunSnapshotNotPossible)	Risk	Volume	Warning

Impact area: configuration

Event name (Trap name)	Impact level	Source type	Severity
LUN mapped with unsupported operating system in igroup(igroupUnsupportedOsType)	Risk	LUN	Warning

Impact area: performance

Event name (Trap name)	Impact level	Source type	Severity
LUN IOPS Critical Threshold Breached(ocumLunIopsIncident)	Incident	LUN	Critical

Event name (Trap name)	Impact level	Source type	Severity
LUN IOPS Warning Threshold Breached(ocumLunIopsWarning)	Risk	LUN	Warning
LUN MB/s Critical Threshold Breached(ocumLunMbpsIncident)	Incident	LUN	Critical
LUN MB/s Warning Threshold Breached(ocumLunMbpsWarning)	Risk	LUN	Warning
LUN Latency ms/op Critical Threshold Breached(ocumLunLatencyIncident)	Incident	LUN	Critical
LUN Latency ms/op Warning Threshold Breached(ocumLunLatencyWarning)	Risk	LUN	Warning
LUN Latency and IOPS Critical Threshold Breached(ocumLunLatencyIopsIncident)	Incident	LUN	Critical
LUN Latency and IOPS Warning Threshold Breached(ocumLunLatencyIopsWarning)	Risk	LUN	Warning
LUN Latency and MB/s Critical Threshold Breached(ocumLunLatencyMbpsIncident)	Incident	LUN	Critical
LUN Latency and MB/s Warning Threshold Breached(ocumLunLatencyMbpsWarning)	Risk	LUN	Warning

Event name (Trap name)	Impact level	Source type	Severity
LUN Latency and Aggregate Performance Capacity Used Critical Threshold Breached(ocumLunLatencyAggregatePerfCapacityUsedIncident)	Incident	LUN	Critical
LUN Latency and Aggregate Performance Capacity Used Warning Threshold Breached(ocumLunLatencyAggregatePerfCapacityUsedWarning)	Risk	LUN	Warning
LUN Latency and Aggregate Utilization Critical Threshold Breached(ocumLunLatencyAggregateUtilizationIncident)	Incident	LUN	Critical
LUN Latency and Aggregate Utilization Warning Threshold Breached(ocumLunLatencyAggregateUtilizationWarning)	Risk	LUN	Warning
LUN Latency and Node Performance Capacity Used Critical Threshold Breached(ocumLunLatencyNodePerfCapacityUsedIncident)	Incident	LUN	Critical
LUN Latency and Node Performance Capacity Used Warning Threshold Breached(ocumLunLatencyNodePerfCapacityUsedWarning)	Risk	LUN	Warning

Event name (Trap name)	Impact level	Source type	Severity
LUN Latency and Node Performance Capacity Used - Takeover Critical Threshold Breached(ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incident	LUN	Critical
LUN Latency and Node Performance Capacity Used - Takeover Warning Threshold Breached(ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risk	LUN	Warning
LUN Latency and Node Utilization Critical Threshold Breached(ocumLunLatencyNodeUtilizationIncident)	Incident	LUN	Critical
LUN Latency and Node Utilization Warning Threshold Breached(ocumLunLatencyNodeUtilizationWarning)	Risk	LUN	Warning
QoS LUN Max IOPS Warning Threshold Breached(ocumQosLunMaxIopsWarning)	Risk	LUN	Warning
QoS LUN Max MB/s Warning Threshold Breached(ocumQosLunMaxMbpsWarning)	Risk	LUN	Warning
Workload LUN Latency Threshold Breached as defined by Performance Service Level Policy(ocumConformanceLatencyWarning)	Risk	LUN	Warning

Management station events

Management station events provide you with information about the status of server on

which Unified Manager is installed so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: configuration

Event name (Trap name)	Impact level	Source type	Severity
Management Server Disk Space Nearly Full(ocumEvtUnifiedManagerDiskSpaceNearlyFull)	Risk	Management station	Warning
Management Server Disk Space Full(ocumEvtUnifiedManagerDiskSpaceFull)	Incident	Management station	Critical
Management Server Low On Memory(ocumEvtUnifiedManagerMemoryLow)	Risk	Management station	Warning
Management Server Almost Out Of Memory(ocumEvtUnifiedManagerMemoryAlmostOut)	Incident	Management station	Critical
MySQL Log File Size Increased; Restart Required(ocumEvtMysqlLogFileSizeWarning)	Incident	Management station	Warning
Total Audit Log Size Allocation is About to Get Full	Risk	Management station	Warning
Syslog Server Certificate About to Expire	Risk	Management station	Warning
Syslog Server Certificate Expired	Risk	Management station	Error
Audit Log File Tampered	Risk	Management station	Warning
Audit Log File Deleted	Risk	Management station	Warning

Event name (Trap name)	Impact level	Source type	Severity
Syslog Server Connection Error	Risk	Management station	Error
Syslog Server Configuration Changed	Event	Management station	Warning

Impact area: performance

Event name (Trap name)	Impact level	Source type	Severity
Performance Data Analysis Is Impacted(ocumEvtUnifiedManagerDataMissingAnalyze)	Risk	Management station	Warning
Performance Data Collection Is Impacted(ocumEvtUnifiedManagerDataMissingCollection)	Incident	Management station	Critical

These last two performance events were available for Unified Manager 7.2 only. If either of these events exist in the New state, and then you upgrade to a newer version of Unified Manager software, the events will not be purged automatically. You will need to move the events to the Resolved state manually.

MetroCluster Bridge events

MetroCluster Bridge events provide you with information about the status of the bridges so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Bridge Unreachable(ocumEvtBridgeUnreachable)	Incident	MetroCluster Bridge	Critical
Bridge Temperature Abnormal(ocumEvtBridgeTemperatureAbnormal)	Incident	MetroCluster Bridge	Critical

MetroCluster Connectivity events

Connectivity events provide you with information about the connectivity between the components of a cluster and between clusters in a MetroCluster configuration so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
All Inter-Switch Links Down(ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Incident	MetroCluster inter-switch connection	Critical
All Links Between MetroCluster Partners Down(ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Incident	MetroCluster relationship	Critical
FC-SAS Bridge To Storage Stack Link Down(ocumEvtBridgeSasPortDown)	Incident	MetroCluster bridge stack connection	Critical
MetroCluster Configuration Switched Over(ocumEvtMetroClusterDRStatusImpacted)	Risk	MetroCluster relationship	Warning
MetroCluster Configuration Partially Switched Over(ocumEvtMetroClusterDRStatusPartiallyImpacted)	Risk	MetroCluster relationship	Error
MetroCluster Disaster Recovery Capability Impacted(ocumEvtMetroClusterDRStatusImpacted)	Risk	MetroCluster relationship	Critical
MetroCluster Partners Not Reachable Over Peering Network(ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Incident	MetroCluster relationship	Critical

Event name (Trap name)	Impact level	Source type	Severity
Node To FC Switch All FC-VI Interconnect Links Down(ocumEvtMccNodeSwitchFcviLinksDown)	Incident	MetroCluster node switch connection	Critical
Node To FC Switch One Or More FC-Initiator Links Down(ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Risk	MetroCluster node switch connection	Warning
Node To FC Switch All FC-Initiator Links Down(ocumEvtMccNodeSwitchFcLinksDown)	Incident	MetroCluster node switch connection	Critical
Switch To FC-SAS Bridge FC Link Down (ocumEvtMccSwitchBridgeFcLinksDown)	Incident	MetroCluster switch bridge connection	Critical
Inter Node All FC VI InterConnect Links Down (ocumEvtMccInterNodeLinksDown)	Incident	Inter-node connection	Critical
Inter Node One Or More FC VI InterConnect Links Down (ocumEvtMccInterNodeLinksOneOrMoreDown)	Risk	Inter-node connection	Warning
Node To Bridge Link Down (ocumEvtMccNodeBridgeLinksDown)	Incident	Node bridge connection	Critical
Node to Storage Stack All SAS Links Down (ocumEvtMccNodeStackLinksDown)	Incident	Node stack connection	Critical
Node to Storage Stack One Or More SAS Links Down (ocumEvtMccNodeStackLinksOneOrMoreDown)	Risk	Node stack connection	Warning

MetroCluster switch events

MetroCluster switch events provide you with information about the status of the MetroCluster switches so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Switch Temperature Abnormal(ocumEvtSwitchTemperatureAbnormal)	Incident	MetroCluster Switch	Critical
Switch Unreachable(ocumEvtSwitchUnreachable)	Incident	MetroCluster Switch	Critical
Switch Fans Failed(ocumEvtSwitchFansOneOrMoreFailed)	Incident	MetroCluster Switch	Critical
Switch Power Supplies Failed(ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Incident	MetroCluster Switch	Critical
Switch Temperature Sensors Failed(ocumEvtSwitchTemperatureSensorFailed) This event is applicable only for Cisco switches.	Incident	MetroCluster Switch	Critical

NVMe Namespace events

NVMe Namespace events provide you with information about the status of your namespaces, so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

An asterisk (*) identifies EMS events that have been converted to Unified Manager events.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
NVMeNS Offline *(nvmeNamespaceStatusOffline)	Event	Namespace	Information
NVMeNS Online *(nvmeNamespaceStatusOnline)	Event	Namespace	Information
NVMeNS Out of Space *(nvmeNamespaceSpaceOutOfSpace)	Risk	Namespace	Warning
NVMeNS Destroy *(nvmeNamespaceDestroy)	Event	Namespace	Information

Impact area: performance

Event name (Trap name)	Impact level	Source type	Severity
NVMe Namespace IOPS Critical Threshold Breached(ocumNvmeNamespaceIopsIncident)	Incident	Namespace	Critical
NVMe Namespace IOPS Warning Threshold Breached(ocumNvmeNamespaceIopsWarning)	Risk	Namespace	Warning
NVMe Namespace MB/s Critical Threshold Breached(ocumNvmeNamespaceMbpsIncident)	Incident	Namespace	Critical
NVMe Namespace MB/s Warning Threshold Breached(ocumNvmeNamespaceMbpsWarning)	Risk	Namespace	Warning
NVMe Namespace Latency ms/op Critical Threshold Breached(ocumNvmeNamespaceLatencyIncident)	Incident	Namespace	Critical

Event name (Trap name)	Impact level	Source type	Severity
NVMe Namespace Latency ms/op Warning Threshold Breached(ocumNvmeNamespaceLatencyWarning)	Risk	Namespace	Warning
NVMe Namespace Latency and IOPS Critical Threshold Breached(ocumNvmeNamespaceLatencyIopsIncident)	Incident	Namespace	Critical
NVMe Namespace Latency and IOPS Warning Threshold Breached(ocumNvmeNamespaceLatencyIopsWarning)	Risk	Namespace	Warning
NVMe Namespace Latency and MB/s Critical Threshold Breached(ocumNvmeNamespaceLatencyMbpsIncident)	Incident	Namespace	Critical
NVMe Namespace Latency and MB/s Warning Threshold Breached(ocumNvmeNamespaceLatencyMbpsWarning)	Risk	Namespace	Warning

Node events

Node events provide you with information about node status so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

An asterisk (*) identifies EMS events that have been converted to Unified Manager events.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Node Root Volume Space Nearly Full(ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Risk	Node	Warning
Cloud AWS MetaDataConnFail *(ocumCloudAwsMetadataConnFail)	Risk	Node	Error
Cloud AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	Risk	Node	Error
Cloud AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	Risk	Node	Error
Cloud AWS IAMCredsNotFound *(ocumCloudAwsIamCredsNotFound)	Risk	Node	Error
Cloud AWS IAMCredsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	Event	Node	Information
Cloud AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	Risk	Node	Error
Cloud AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	Risk	Node	Error
Cloud Tier Host Unresolvable *(ocumObjstoreHostUnresolvable)	Risk	Node	Error

Event name (Trap name)	Impact level	Source type	Severity
Cloud Tier Intercluster LIF Down *(ocumObjstoreInterClusterLifDown)	Risk	Node	Error
One of NFSv4 Pools Exhausted *(nbladeNfsv4PoolEXhaust)	Incident	Node	Critical
Request Mismatch Cloud Tier Signature *(oscSignatureMismatch)	Risk	Node	Error

Impact area: capacity

Event name (Trap name)	Impact level	Source type	Severity
QoS Monitor Memory Maxed *(ocumQosMonitorMemoryMaxed)	Risk	Node	Error
QoS Monitor Memory Abated *(ocumQosMonitorMemoryAbated)	Event	Node	Information

Impact area: configuration

Event name (Trap name)	Impact level	Source type	Severity
Node Renamed(Not applicable)	Event	Node	Information

Impact area: performance

Event name (Trap name)	Impact level	Source type	Severity
Node IOPS Critical Threshold Breached(ocumNodeIopsIncident)	Incident	Node	Critical

Event name (Trap name)	Impact level	Source type	Severity
Node IOPS Warning Threshold Breached(ocumNodeIopsWarning)	Risk	Node	Warning
Node MB/s Critical Threshold Breached(ocumNodeMbpsIncident)	Incident	Node	Critical
Node MB/s Warning Threshold Breached(ocumNodeMbpsWarning)	Risk	Node	Warning
Node Latency ms/op Critical Threshold Breached(ocumNodeLatencyIncident)	Incident	Node	Critical
Node Latency ms/op Warning Threshold Breached(ocumNodeLatencyWarning)	Risk	Node	Warning
Node Performance Capacity Used Critical Threshold Breached(ocumNodePerfCapacityUsedIncident)	Incident	Node	Critical
Node Performance Capacity Used Warning Threshold Breached(ocumNodePerfCapacityUsedWarning)	Risk	Node	Warning
Node Performance Capacity Used - Takeover Critical Threshold Breached(ocumNodePerfCapacityUsedTakeoverIncident)	Incident	Node	Critical

Event name (Trap name)	Impact level	Source type	Severity
Node Performance Capacity Used - Takeover Warning Threshold Breached(ocumNodePerfCapacityUsedTakeoverWarning)	Risk	Node	Warning
Node Utilization Critical Threshold Breached (ocumNodeUtilizationIncident)	Incident	Node	Critical
Node Utilization Warning Threshold Breached (ocumNodeUtilizationWarning)	Risk	Node	Warning
Node HA Pair Over-utilized Threshold Breached (ocumNodeHaPairOverUtilizedInformation)	Event	Node	Information
Node Disk Fragmentation Threshold Breached (ocumNodeDiskFragmentationWarning)	Risk	Node	Warning
Performance Capacity Used Threshold Breached (ocumNodeOverUtilizedWarning)	Risk	Node	Warning
Node Dynamic Threshold Breached (ocumNodeDynamicEventWarning)	Risk	Node	Warning

Impact area: security

Event name (Trap name)	Impact level	Source type	Severity
Advisory ID: NTAP-<*advisory ID*>(ocumx)	Risk	Node	Critical

NVRAM battery events

NVRAM battery events provide you with information about the status of your batteries so

that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
NVRAM Battery Low(ocumEvtNvramBatteryLow)	Risk	Node	Warning
NVRAM Battery Discharged(ocumEvtNvramBatteryDischarged)	Risk	Node	Error
NVRAM Battery Overly Charged(ocumEvtNvramBatteryOverCharged)	Incident	Node	Critical

Port events

Port events provide you with status about cluster ports so that you can monitor changes or problems on the port, like whether the port is down.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Port Status Down(ocumEvtPortStatusDown)	Incident	Node	Critical

Impact area: performance

Event name (Trap name)	Impact level	Source type	Severity
Network Port MB/s Critical Threshold Breached(ocumNetworkPortMbpsIncident)	Incident	Port	Critical
Network Port MB/s Warning Threshold Breached(ocumNetworkPortMbpsWarning)	Risk	Port	Warning

Event name (Trap name)	Impact level	Source type	Severity
FCP Port MB/s Critical Threshold Breached(ocumFcpPortMbpsIncident)	Incident	Port	Critical
FCP Port MB/s Warning Threshold Breached(ocumFcpPortMbpsWarning)	Risk	Port	Warning
Network Port Utilization Critical Threshold Breached(ocumNetworkPortUtilizationIncident)	Incident	Port	Critical
Network Port Utilization Warning Threshold Breached(ocumNetworkPortUtilizationWarning)	Risk	Port	Warning
FCP Port Utilization Critical Threshold Breached(ocumFcpPortUtilizationIncident)	Incident	Port	Critical
FCP Port Utilization Warning Threshold Breached(ocumFcpPortUtilizationWarning)	Risk	Port	Warning

Power supplies events

Power supplies events provide you with information about the status of your hardware so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
One or More Failed Power Supplies(ocumEvtPowerSupplyOneOrMoreFailed)	Incident	Node	Critical

Protection events

Protection events tell you if a job has failed or been aborted so that you can monitor for problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: protection

Event name (Trap name)	Impact level	Source type	Severity
Protection Job Failed(ocumEvtProtectionJobTaskFailed)	Incident	Volume or storage service	Critical
Protection Job Aborted(ocumEvtProtectionJobAborted)	Risk	Volume or storage service	Warning

Qtree events

Qtree events provide you with information about the qtree capacity and the file and disk limits so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: capacity

Event name (Trap name)	Impact level	Source type	Severity
Qtree Space Nearly Full(ocumEvtQtreeSpaceNearlyFull)	Risk	Qtree	Warning
Qtree Space Full(ocumEvtQtreeSpaceFull)	Risk	Qtree	Error
Qtree Space Normal(ocumEvtQtreeSpaceThresholdOk)	Event	Qtree	Information
Qtree Files Hard Limit Reached(ocumEvtQtreeFilesHardLimitReached)	Incident	Qtree	Critical
Qtree Files Soft Limit Breached(ocumEvtQtreeFilesSoftLimitBreached)	Risk	Qtree	Warning

Event name (Trap name)	Impact level	Source type	Severity
Qtree Space Hard Limit Reached(ocumEvtQtreeSpaceHardLimitReached)	Incident	Qtree	Critical
Qtree Space Soft Limit Breached(ocumEvtQtreeSpaceSoftLimitBreached)	Risk	Qtree	Warning

Service processor events

Service processor events provide you with information about the status of your processor so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Service Processor Not Configured(ocumEvtServiceProcessorNotConfigured)	Risk	Node	Warning
Service Processor Offline(ocumEvtServiceProcessorOffline)	Risk	Node	Error

SnapMirror relationship events

SnapMirror relationship events provide you with information about the status of your Asynchronous and Synchronous SnapMirror relationships so that you can monitor for potential problems. Asynchronous SnapMirror relationship events are generated for both Storage VMs and volumes but Synchronous SnapMirror relationship events are generated only for volume relationships. There are no events generated for constituent volumes that are part of Storage VM disaster recovery relationships. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: protection

An asterisk (*) identifies EMS events that have been converted to Unified Manager events.

The SnapMirror relationships events are generated for Storage VMs that are protected by Storage VM disaster recovery but not for any constituent object relationships.

Event name (Trap name)	Impact level	Source type	Severity
Mirror Replication Unhealthy(ocumEvtSnapmirrorRelationshipUnhealthy)	Risk	SnapMirror relationship	Warning
Mirror Replication Broken-off(ocumEvtSnapmirrorRelationshipStateBrokenoff)	Risk	SnapMirror relationship	Error
Mirror Replication Initialize Failed(ocumEvtSnapmirrorRelationshipInitializeFailed)	Risk	SnapMirror relationship	Error
Mirror Replication Update Failed(ocumEvtSnapmirrorRelationshipUpdateFailed)	Risk	SnapMirror relationship	Error
Mirror Replication Lag Error(ocumEvtSnapMirrorRelationshipLagError)	Risk	SnapMirror relationship	Error
Mirror Replication Lag Warning(ocumEvtSnapMirrorRelationshipLagWarning)	Risk	SnapMirror relationship	Warning
Mirror Replication Resync Failed(ocumEvtSnapmirrorRelationshipResyncFailed)	Risk	SnapMirror relationship	Error
Synchronous Replication Out Of Sync *(syncSnapmirrorRelationshipOutofsync)	Risk	SnapMirror relationship	Warning
Synchronous Replication Restored *(syncSnapmirrorRelationshipInSync)	Event	SnapMirror relationship	Information
Synchronous Replication Auto Resync Failed *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Risk	SnapMirror relationship	Error

Asynchronous Mirror and Vault relationship events

Asynchronous Mirror and Vault relationship events provide you with information about the status of your Asynchronous SnapMirror and Vault relationships so that you can monitor for potential problems. Asynchronous Mirror and Vault relationship events are supported for both volume and Storage VM protection relationships. But only Vault relationships are not supported for Storage VM disaster recovery. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: protection

The SnapMirror and Vault relationships events are also generated for Storage VMs that are protected by Storage VM disaster recovery but not for any constituent object relationships.

Event name (Trap name)	Impact level	Source type	Severity
Asynchronous Mirror and Vault Unhealthy(ocumEvtMirrorVaultRelationshipUnhealthy)	Risk	SnapMirror relationship	Warning
Asynchronous Mirror and Vault Broken-off(ocumEvtMirrorVaultRelationshipStateBrokenoff)	Risk	SnapMirror relationship	Error
Asynchronous Mirror and Vault Initialize Failed(ocumEvtMirrorVaultRelationshipInitializeFailed)	Risk	SnapMirror relationship	Error
Asynchronous Mirror and Vault Update Failed(ocumEvtMirrorVaultRelationshipUpdateFailed)	Risk	SnapMirror relationship	Error
Asynchronous Mirror and Vault Lag Error(ocumEvtMirrorVaultRelationshipLagError)	Risk	SnapMirror relationship	Error
Asynchronous Mirror and Vault Lag Warning(ocumEvtMirrorVaultRelationshipLagWarning)	Risk	SnapMirror relationship	Warning

Event name (Trap name)	Impact level	Source type	Severity
Asynchronous Mirror and Vault Resync Failed(ocumEvtMirrorVaultRelationshipResyncFailed)	Risk	SnapMirror relationship	Error

"SnapMirror update failure" event is raised by Active IQ portal (Config Advisor).

Snapshot events

Snapshot events provide information about the status of snapshots which enables you to monitor the snapshots for potential problems. The events are grouped by impact area, and include the event name, trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Snapshot Auto-delete Disabled(Not applicable)	Event	Volume	Information
Snapshot Auto-delete Enabled(Not applicable)	Event	Volume	Information
Snapshot Auto-delete Configuration Modified(Not applicable)	Event	Volume	Information

SnapVault relationship events

SnapVault relationship events provide you with information about the status of your SnapVault relationships so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: protection

Event name (Trap name)	Impact level	Source type	Severity
Asynchronous Vault Unhealthy(ocumEvtSnapVaultRelationshipUnhealthy)	Risk	SnapMirror relationship	Warning

Event name (Trap name)	Impact level	Source type	Severity
Asynchronous Vault Broken-off(ocumEvtSnapVaultRelationshipStateBrokenoff)	Risk	SnapMirror relationship	Error
Asynchronous Vault Initialize Failed(ocumEvtSnapVaultRelationshipInitializeFailed)	Risk	SnapMirror relationship	Error
Asynchronous Vault Update Failed(ocumEvtSnapVaultRelationshipUpdateFailed)	Risk	SnapMirror relationship	Error
Asynchronous Vault Lag Error(ocumEvtSnapVaultRelationshipLagError)	Risk	SnapMirror relationship	Error
Asynchronous Vault Lag Warning(ocumEvtSnapVaultRelationshipLagWarning)	Risk	SnapMirror relationship	Warning
Asynchronous Vault Resync Failed(ocumEvtSnapvaultRelationshipResyncFailed)	Risk	SnapMirror relationship	Error

Storage failover settings events

Storage failover (SFO) settings events provide you with information about whether your storage failover is disabled or not configured so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Storage Failover Interconnect One Or More Links Down(ocumEvtSfoInterconnectOneOrMoreLinksDown)	Risk	Node	Warning
Storage Failover Disabled(ocumEvtSfoSettingsDisabled)	Risk	Node	Error
Storage Failover Not Configured(ocumEvtSfoSettingsNotConfigured)	Risk	Node	Error
Storage Failover State - Takeover(ocumEvtSfoStateTakeover)	Risk	Node	Warning
Storage Failover State - Partial Giveback(ocumEvtSfoStatePartialGiveback)	Risk	Node	Error
Storage Failover Node Status Down(ocumEvtSfoNodeStatusDown)	Risk	Node	Error
Storage Failover Takeover Not Possible(ocumEvtSfoTakeoverNotPossible)	Risk	Node	Error

Storage services events

Storage services events provide you with information about the creation and subscription of storage services so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: configuration

Event name (Trap name)	Impact level	Source type	Severity
Storage Service Created(Not applicable)	Event	Storage service	Information

Event name (Trap name)	Impact level	Source type	Severity
Storage Service Subscribed(Not applicable)	Event	Storage service	Information
Storage Service Unsubscribed(Not applicable)	Event	Storage service	Information

Impact area: protection

Event name (Trap name)	Impact level	Source type	Severity
Unexpected Deletion of Managed SnapMirror RelationshipocumEvtStorageServiceUnsupportedRelationshipDeletion	Risk	Storage service	Warning
Unexpected Deletion of Storage Service Member Volume(ocumEvtStorageServiceUnexpectedVolumeDeletion)	Incident	Storage service	Critical

Storage shelf events

Storage shelf events tell you if your storage shelf has abnormal so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Abnormal Voltage Range(ocumEvtShelfVoltageAbnormal)	Risk	Storage shelf	Warning
Abnormal Current Range(ocumEvtShelfCurrentAbnormal)	Risk	Storage shelf	Warning
Abnormal Temperature(ocumEvtShelfTemperatureAbnormal)	Risk	Storage shelf	Warning

Storage VM events

Storage VM (storage virtual machine, also known as SVM) events provide you with information about the status of your storage VMs (SVMs) so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

An asterisk (*) identifies EMS events that have been converted to Unified Manager events.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
SVM CIFS Service Down(ocumEvtVserverCifsServiceStatusDown)	Incident	SVM	Critical
SVM CIFS Service Not Configured(Not applicable)	Event	SVM	Information
Attempts to Connect Nonexistent CIFS Share *(nbladeCifsNoPrivShare)	Incident	SVM	Critical
CIFS NetBIOS Name Conflict *(nbladeCifsNbNameConflict)	Risk	SVM	Error
CIFS Shadow Copy Operation Failed *(cifsShadowCopyFailure)	Risk	SVM	Error
Many CIFS Connections *(nbladeCifsManyAuths)	Risk	SVM	Error
Max CIFS Connection Exceeded *(nbladeCifsMaxOpenSameFile)	Risk	SVM	Error
Max Number of CIFS Connection Per User Exceeded *(nbladeCifsMaxSessPerUsrConn)	Risk	SVM	Error

Event name (Trap name)	Impact level	Source type	Severity
SVM FC/FCoE Service Down(ocumEvtVserverFcServiceStatusDown)	Incident	SVM	Critical
SVM iSCSI Service Down(ocumEvtVserverIscsiServiceStatusDown)	Incident	SVM	Critical
SVM NFS Service Down(ocumEvtVserverNfsServiceStatusDown)	Incident	SVM	Critical
SVM FC/FCoE Service Not Configured(Not applicable)	Event	SVM	Information
SVM iSCSI Service Not Configured(Not applicable)	Event	SVM	Information
SVM NFS Service Not Configured(Not applicable)	Event	SVM	Information
SVM Stopped(ocumEvtVserverDown)	Risk	SVM	Warning
AV Server too Busy to Accept New Scan Request *(nbladeVscanConnBackPressure)	Risk	SVM	Error
No AV Server Connection for Virus Scan *(nbladeVscanNoScannerConn)	Incident	SVM	Critical
No AV Server Registered *(nbladeVscanNoRegdScanner)	Risk	SVM	Error
No Responsive AV Server Connection *(nbladeVscanConnInactive)	Event	SVM	Information

Event name (Trap name)	Impact level	Source type	Severity
Unauthorized User Attempt to AV Server *(nbladeVscanBadUserPrivAccess)	Risk	SVM	Error
Virus Found By AV Server *(nbladeVscanVirusDetected)	Risk	SVM	Error

Impact area: configuration

Event name (Trap name)	Impact level	Source type	Severity
SVM Discovered(Not applicable)	Event	SVM	Information
SVM Deleted(Not applicable)	Event	Cluster	Information
SVM Renamed(Not applicable)	Event	SVM	Information

Impact area: performance

Event name (Trap name)	Impact level	Source type	Severity
SVM IOPS Critical Threshold Breached(ocumSvmIopsIncident)	Incident	SVM	Critical
SVM IOPS Warning Threshold Breached(ocumSvmIopsWarning)	Risk	SVM	Warning
SVM MB/s Critical Threshold Breached(ocumSvmMbpsIncident)	Incident	SVM	Critical
SVM MB/s Warning Threshold Breached(ocumSvmMbpsWarning)	Risk	SVM	Warning

Event name (Trap name)	Impact level	Source type	Severity
SVM Latency Critical Threshold Breached(ocumSvmLatencyIncident)	Incident	SVM	Critical
SVM Latency Warning Threshold Breached(ocumSvmLatencyWarning)	Risk	SVM	Warning

Impact area: security

Event name (Trap name)	Impact level	Source type	Severity
Audit Log Disabled(ocumVserverAuditLogDisabled)	Risk	SVM	Warning
Login Banner Disabled(ocumVserverLoginBannerDisabled)	Risk	SVM	Warning
SSH is Using Insecure Ciphers(ocumVserverSSHInsecure)	Risk	SVM	Warning
Login Banner Changed(ocumVserverLoginBannerChanged)	Risk	SVM	Warning
Storage VM anti-ransomware monitoring is Disabled (antiRansomwareSvmStateDisabled)	Risk	SVM	Warning
Storage VM anti-ransomware monitoring is Enabled (Learning Mode) (antiRansomwareSvmStateDryrun)	Event	SVM	Information
Storage VM suitable for anti-ransomware monitoring (Learning Mode) (ocumEvtSvmArwCandidate)	Event	SVM	Information

User and group quota events

User and group quota events provide you with information about the capacity of the user and user group quota as well as the file and disk limits so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: capacity

Event name (Trap name)	Impact level	Source type	Severity
User or Group Quota Disk Space Soft Limit Breached(ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Risk	User or group quota	Warning
User or Group Quota Disk Space Hard Limit Reached(ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Incident	User or group quota	Critical
User or Group Quota File Count Soft Limit Breached(ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Risk	User or group quota	Warning
User or Group Quota File Count Hard Limit Reached(ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Incident	User or group quota	Critical

Volume events

Volume events provide information about the status of volumes which enables you to monitor for potential problems. The events are grouped by impact area, and include the event name, trap name, impact level, source type, and severity.

An asterisk (*) identifies EMS events that have been converted to Unified Manager events.

Impact area: availability

Event name (Trap name)	Impact level	Source type	Severity
Volume Restricted(ocumEvtVolumeRestricted)	Risk	Volume	Warning

Event name (Trap name)	Impact level	Source type	Severity
Volume Offline(ocumEvtVolumeOffline)	Incident	Volume	Critical
Volume Partially Available(ocumEvtVolumePartiallyAvailable)	Risk	Volume	Error
Volume Unmounted(Not applicable)	Event	Volume	Information
Volume Mounted(Not applicable)	Event	Volume	Information
Volume Remounted(Not applicable)	Event	Volume	Information
Volume Junction Path Inactive(ocumEvtVolumeJunctionPathInactive)	Risk	Volume	Warning
Volume Autosize Enabled(Not applicable)	Event	Volume	Information
Volume Autosize-Disabled(Not applicable)	Event	Volume	Information
Volume Autosize Maximum Capacity Modified(Not applicable)	Event	Volume	Information
Volume Autosize Increment Size Modified(Not applicable)	Event	Volume	Information

Impact area: capacity

Event name (Trap name)	Impact level	Source type	Severity
Thin-Provisioned Volume Space At Risk(ocumThinProvisionVolumeSpaceAtRisk)	Risk	Volume	Warning
Volume Space Full(ocumEvtVolumeFull)	Risk	Volume	Error

Event name (Trap name)	Impact level	Source type	Severity
Volume Space Nearly Full(ocumEvtVolumeNearlyFull)	Risk	Volume	Warning
Volume Logical Space Full *(volumeLogicalSpaceFull)	Risk	Volume	Error
Volume Logical Space Nearly Full *(volumeLogicalSpaceNearlyFull)	Risk	Volume	Warning
Volume Logical Space Normal *(volumeLogicalSpaceAllOK)	Event	Volume	Information
Volume Snapshot Reserve Space Full(ocumEvtSnapshotFull)	Risk	Volume	Warning
Too Many Snapshot Copies(ocumEvtSnapshotTooMany)	Risk	Volume	Error
Volume Qtree Quota Overcommitted(ocumEvtVolumeQtreeQuotaOvercommitted)	Risk	Volume	Error
Volume Qtree Quota Nearly Overcommitted(ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	Risk	Volume	Warning
Volume Growth Rate Abnormal(ocumEvtVolumeGrowthRateAbnormal)	Risk	Volume	Warning
Volume Days Until Full(ocumEvtVolumeDaysUntilFullSoon)	Risk	Volume	Error

Event name (Trap name)	Impact level	Source type	Severity
Volume Space Guarantee Disabled(Not applicable)	Event	Volume	Information
Volume Space Guarantee Enabled(Not Applicable)	Event	Volume	Information
Volume Space Guarantee Modified(Not applicable)	Event	Volume	Information
Volume Snapshot Reserve Days Until Full(ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Risk	Volume	Error
FlexGroup Constituents Have Space Issues *(flexGroupConstituentsHaveSpaceIssues)	Risk	Volume	Error
FlexGroup Constituents Space Status All OK *(flexGroupConstituentsSpaceStatusAllOK)	Event	Volume	Information
FlexGroup Constituents Have Inodes Issues *(flexGroupConstituentsHaveInodesIssues)	Risk	Volume	Error
FlexGroup Constituents Inodes Status All OK *(flexGroupConstituentsInodesStatusAllOK)	Event	Volume	Information
WAFL Volume AutoSize Fail *(waflVolAutoSizeFail)	Risk	Volume	Error
WAFL Volume AutoSize Done *(waflVolAutoSizeDone)	Event	Volume	Information
FlexGroup Volume Is Over 80% Utilized*	Incident	Volume	Error

Event name (Trap name)	Impact level	Source type	Severity
FlexGroup Volume Is Over 90% Utilized*	Incident	Volume	Critical
Volume storage efficiency anomaly (ocumVolumeAbnormalStorageEfficiencyWarning)	Risk	Volume	Warning

Impact area: configuration

Event name (Trap name)	Impact level	Source type	Severity
Volume Renamed(Not applicable)	Event	Volume	Information
Volume Discovered(Not applicable)	Event	Volume	Information
Volume Deleted(Not applicable)	Event	Volume	Information

Impact area: performance

Event name (Trap name)	Impact level	Source type	Severity
QoS Volume Max IOPS Warning Threshold Breached(ocumQosVolumeMaxIopsWarning)	Risk	Volume	Warning
QoS Volume Max MB/s Warning Threshold Breached(ocumQosVolumeMaxMbpsWarning)	Risk	Volume	Warning
QoS Volume Max IOPS/TB Warning Threshold Breached(ocumQosVolumeMaxIopsPerTbWarning)	Risk	Volume	Warning

Event name (Trap name)	Impact level	Source type	Severity
Workload Volume Latency Threshold Breached as defined by Performance Service Level Policy(ocumConformanceLatencyWarning)	Risk	Volume	Warning
Volume IOPS Critical Threshold Breached(ocumVolumeIopsIncident)	Incident	Volume	Critical
Volume IOPS Warning Threshold Breached(ocumVolumeIopsWarning)	Risk	Volume	Warning
Volume MB/s Critical Threshold Breached(ocumVolumeMbpsIncident)	Incident	Volume	Critical
Volume MB/s Warning Threshold Breached(ocumVolumeMbpsWarning)	Risk	Volume	Warning
Volume Latency ms/op Critical Threshold Breached(ocumVolumeLatencyIncident)	Incident	Volume	Critical
Volume Latency ms/op Warning Threshold Breached(ocumVolumeLatencyWarning)	Risk	Volume	Warning
Volume Cache Miss Ratio Critical Threshold Breached(ocumVolumeCacheMissRatioIncident)	Incident	Volume	Critical
Volume Cache Miss Ratio Warning Threshold Breached(ocumVolumeCacheMissRatioWarning)	Risk	Volume	Warning

Event name (Trap name)	Impact level	Source type	Severity
Volume Latency and IOPS Critical Threshold Breached(ocumVolumeLatencyIopsIncident)	Incident	Volume	Critical
Volume Latency and IOPS Warning Threshold Breached(ocumVolumeLatencyIopsWarning)	Risk	Volume	Warning
Volume Latency and MB/s Critical Threshold Breached(ocumVolumeLatencyMbpsIncident)	Incident	Volume	Critical
Volume Latency and MB/s Warning Threshold Breached(ocumVolumeLatencyMbpsWarning)	Risk	Volume	Warning
Volume Latency and Aggregate Performance Capacity Used Critical Threshold Breached(ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	Incident	Volume	Critical
Volume Latency and Aggregate Performance Capacity Used Warning Threshold Breached(ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	Risk	Volume	Warning
Volume Latency and Aggregate Utilization Critical Threshold Breached(ocumVolumeLatencyAggregateUtilizationIncident)	Incident	Volume	Critical
Volume Latency and Aggregate Utilization Warning Threshold Breached(ocumVolumeLatencyAggregateUtilizationWarning)	Risk	Volume	Warning

Event name (Trap name)	Impact level	Source type	Severity
Volume Latency and Node Performance Capacity Used Critical Threshold Breached(ocumVolumeLatencyNodePerfCapacityUsedIncident)	Incident	Volume	Critical
Volume Latency and Node Performance Capacity Used Warning Threshold Breached(ocumVolumeLatencyNodePerfCapacityUsedWarning)	Risk	Volume	Warning
Volume Latency and Node Performance Capacity Used - Takeover Critical Threshold Breached(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incident	Volume	Critical
Volume Latency and Node Performance Capacity Used - Takeover Warning Threshold Breached(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risk	Volume	Warning
Volume Latency and Node Utilization Critical Threshold Breached(ocumVolumeLatencyNodeUtilizationIncident)	Incident	Volume	Critical
Volume Latency and Node Utilization Warning Threshold Breached(ocumVolumeLatencyNodeUtilizationWarning)	Risk	Volume	Warning

Impact area: security

Event name (Trap name)	Impact level	Source type	Severity
Volume anti-ransomware monitoring is Enabled (Active Mode) (antiRansomwareVolumeStateEnabled)	Event	Volume	Information
Volume anti-ransomware monitoring is Disabled (antiRansomwareVolumeStateDisabled)	Risk	Volume	Warning
Volume anti-ransomware monitoring is Enabled (Learning Mode) (antiRansomwareVolumeStateDryrun)	Event	Volume	Information
Volume anti-ransomware monitoring is Paused (Learning Mode) (antiRansomwareVolumeStateDryrunPaused)	Risk	Volume	Warning
Volume anti-ransomware monitoring is Paused (Active Mode) (antiRansomwareVolumeStateEnablePaused)	Risk	Volume	Warning
Volume anti-ransomware monitoring is Disabling (antiRansomwareVolumeStateDisableInProgress)	Risk	Volume	Warning
Ransomware Activity Seen (callHomeRansomwareActivitySeen)	Incident	Volume	Critical
Volume suitable for anti-ransomware monitoring (Learning Mode) (ocumEvtVolumeArwCandidate)	Event	Volume	Information

Event name (Trap name)	Impact level	Source type	Severity
Volume suitable for anti-ransomware monitoring (Active Mode) (ocumVolumeSuitedForActiveAntiRansomwareDetection)	Risk	Volume	Warning
Volume exhibits noisy anti-ransomware alerting (antiRansomwareFeatureNoisyVolume)	Risk	Volume	Warning

Volume move status events

Volume move status events tell you about the status of your volume move so that you can monitor for potential problems. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

Impact area: capacity

Event name (Trap name)	Impact level	Source type	Severity
Volume Move Status: In Progress(Not applicable)	Event	Volume	Information
Volume Move Status - Failed(ocumEvtVolumeMoveFailed)	Risk	Volume	Error
Volume Move Status: Completed(Not applicable)	Event	Volume	Information
Volume Move - Cutover Deferred(ocumEvtVolumeMoveCutoverDeferred)	Risk	Volume	Warning

Description of event windows and dialog boxes

Events notify you about any issues in your environment. You can use the Event Management inventory page and Event details page to monitor all the events. You can use the Notification Setup Options dialog box to configure notification. You can use the Event Setup page to disable or enable events.

Notifications page

You can configure the Unified Manager server to send notifications when an event is

generated or when it is assigned to a user. You can also configure the notification mechanisms. For example, notifications can be sent as emails or SNMP traps.

You must have the Application Administrator or Storage Administrator role.

Email

This area enables you to configure the following email settings for alert notification:

- **From Address**

  Specifies the email address from which the alert notification is sent. This value is also used as the from address for a report when shared. If the From Address is pre-filled with the address "ActiveIQUnifiedManager@localhost.com", you should change it to a real, working email address to make sure that all email notifications are delivered successfully.

SMTP Server

This area enables you to configure the following SMTP server settings:

- **Host Name or IP Address**

  Specifies the host name of your SMTP host server, which is used to send the alert notification to the specified recipients.

- **User Name**

  Specifies the SMTP user name. SMTP user name is required only when the SMTPAUTH is enabled in the SMTP server.

- **Password**

  Specifies the SMTP password. SMTP user name is required only when the SMTPAUTH is enabled in the SMTP server.

- **Port**

  Specifies the port that is used by the SMTP host server to send alert notification.

  The default value is 25.

- **Use START/TLS**

  Checking this box provides secure communication between the SMTP server and the management server by using the TLS/SSL protocols (also known as start_tls and StartTLS).

- **Use SSL**

  Checking this box provides secure communication between the SMTP server and the management server by using the SSL protocol.

SNMP

This area enables you to configure the following SNMP trap settings:

- **Version**

  Specifies the SNMP version you want to use depending on the type of security you require. Options include Version 1, Version 3, Version 3 with Authentication, and Version 3 with Authentication and Encryption. The default value is Version 1.

- **Trap Destination Host**

  Specifies the host name or IP address (IPv4 or IPv6) that receives the SNMP traps that are sent by the management server. To specify multiple trap destinations, separate each host with a comma.

  > All other SNMP settings, such as "Version" and "Outbound Port", must be the same for all hosts in the list.

- **Outbound Trap Port**

  Specifies the port through which the SNMP server receives the traps that are sent by the management server.

  The default value is 162.

- **Community**

  The community string to access the host.

- **Engine ID**

  Specifies the unique identifier of the SNMP agent and is automatically generated by the management server. Engine ID is available with SNMP Version 3, SNMP Version 3 with Authentication, and SNMP Version 3 with Authentication and Encryption.

- **Username**

  Specifies the SNMP user name. User name is available with SNMP Version 3, SNMP Version 3 with Authentication, and SNMP Version 3 with Authentication and Encryption.

- **Authentication Protocol**

  Specifies the protocol used to authenticate a user. Protocol options include MD5 and SHA. MD5 is the default value. Authentication protocol is available with SNMP Version 3 with Authentication and SNMP Version 3 with Authentication and Encryption.

- **Authentication Password**

  Specifies the password used when authenticating a user. Authentication password is available with SNMP Version 3 with Authentication and SNMP Version 3 with Authentication and Encryption.

- **Privacy Protocol**

  Specifies the privacy protocol used to encrypt SNMP messages. Protocol options include AES 128 and DES. The default value is AES 128. Privacy protocol is available with SNMP Version 3 with Authentication and Encryption.

- **Privacy Password**

Specifies the password when using privacy protocol. Privacy password is available with SNMP Version 3 with Authentication and Encryption.

Event Management inventory page

The Event Management inventory page enables you to view a list of current events and their properties. You can perform tasks such as acknowledging, resolving, and assigning events. You can also add an alert for specific events.

The information on this page is refreshed automatically every 5 minutes to ensure that the most current new events are displayed.

Filter components

Enable you to customize the information that is displayed in the events list. You can refine the list of events that are displayed using the following components:

- View menu to select from a pre-defined list of filter selections.

  This includes items such as all active (new and acknowledged) events, active performance events, events assigned to me (the logged in user), and all events generated during all maintenance windows.

- Search pane to refine the list of events by entering full or partial terms.
- Filter button that launches the Filters pane so you can select from every available field and field attribute to refine the list of events.

Command buttons

The command buttons enable you to perform the following tasks:

- **Assign To**

  Enables you to select the user to whom the event is assigned. When you assign an event to a user, the user name and the time when you assigned the event is added in the events list for the selected events.

  - Me

    Assigns the event to the currently logged in user.

  - Another user

    Displays the Assign Owner dialog box, which enables you to assign or reassign the event to other users. You can also unassign events by leaving the ownership field blank.

- **Acknowledge**

  Acknowledges the selected events.

  When you acknowledge an event, your user name and the time when you acknowledged the event are added in the events list for the selected events. When you acknowledge an event, you are responsible for managing that event.

  You cannot acknowledge Information events.

- **Mark As Resolved**

  Enables you to change the event state to resolved.

  When you resolve an event, your user name and the time when you resolved the event are added in the events list for the selected events. After you have taken corrective action for the event, you must mark the event as resolved.

- **Add Alert**

  Displays the Add Alert dialog box, which enables you to add alerts for the selected events.

- **Reports**

  Enables you to export details of the current event view to a comma-separated values (.csv) file or PDF document.

- **Show/Hide Column Selector**

  Enables you to choose the columns that display on the page and select the order in which they are displayed.

Events list

Displays details of all the events ordered by triggered time.

By default the All active events view is displayed to show the New and Acknowledged events for the previous seven days that have an Impact Level of Incident or Risk.

- **Triggered Time**

  The time at which the event was generated.

- **Severity**

  The event severity: Critical (), Error (), Warning (), and Information ().

- **State**

  The event state: New, Acknowledged, Resolved, or Obsolete.

- **Impact Level**

  The event impact level: Incident, Risk, Event, or Upgrade.

- **Impact Area**

  The event impact area: Availability, Capacity, Performance, Protection, Configuration, or Security.

- **Name**

  The event name. You can select the name to display the Event details page for that event.

- **Source**

  The name of the object on which the event has occurred. You can select the name to display the health or

performance details page for that object.

When a shared QoS policy breach occurs, only the workload object that is consuming the most IOPS or MB/s is shown in this field. Additional workloads that are using this policy are displayed in the Event details page.

- **Source Type**

  The object type (for example, Storage VM, Volume, or Qtree) with which the event is associated.

- **Assigned To**

  The name of the user to whom the event is assigned.

- **Event Origin**

  Whether the event originated from the "Active IQ Portal" or directly from "Active IQ Unified Manager".

- **Annotation Name**

  The name of the annotation that is assigned to the storage object.

- **Notes**

  The number of notes that are added for an event.

- **Days Outstanding**

  The number of days since the event was initially generated.

- **Assigned Time**

  The time that has elapsed since the event was assigned to a user. If the time elapsed exceeds a week, the timestamp when the event was assigned to a user is displayed.

- **Acknowledged By**

  The name of the user who acknowledged the event. The field is blank if the event is not acknowledged.

- **Acknowledged Time**

  The time that has elapsed since the event was acknowledged. If the time elapsed exceeds a week, the timestamp when the event was acknowledged is displayed.

- **Resolved By**

  The name of the user who resolved the event. The field is blank if the event is not resolved.

- **Resolved Time**

  The time that has elapsed since the event was resolved. If the time elapsed exceeds a week, the timestamp when the event was resolved is displayed.

- **Obsoleted Time**

  The time when the state of the event became Obsolete.

Event details page

From the Event details page, you can view the details of a selected event, such as the event severity, impact level, impact area, and event source. You can also view additional information about possible remediations to resolve the issue.

- **Event Name**

  The name of the event and the time the event was last seen.

  For non-performance events, while the event is in the New or Acknowledged state the last seen information is not known and is therefore hidden.

- **Event Description**

  A brief description of the event.

  In some cases a reason for the event being triggered is provided in the event description.

- **Component in Contention**

  For dynamic performance events, this section displays icons that represent the logical and physical components of the cluster. If a component is in contention, its icon is circled and highlighted red.

  See *Cluster components and why they can be in contention* for a description of the components that are displayed here.

The Event Information, System Diagnosis, and Suggested Actions sections are described in other topics.

Command buttons

The command buttons enable you to perform the following tasks:

- **Notes icon**

  Enables you to add or update a note about the event, and review all notes left by other users.

Actions menu

- **Assign to Me**

  Assigns the event to you.

- **Assign to Others**

  Opens the Assign Owner dialog box, which enables you to assign or reassign the event to other users.

  When you assign an event to a user, the user's name and the time when the event was assigned are added in the events list for the selected events.

  You can also unassign events by leaving the ownership field blank.

- **Acknowledge**

  Acknowledges the selected events so that you do not continue to receive repeat alert notifications.

When you acknowledge an event, your user name and the time that you acknowledged the event are added in the events list (Acknowledged By) for the selected events. When you acknowledge an event, you take responsibility for managing that event.

- **Mark As Resolved**

  Enables you to change the event state to Resolved.

  When you resolve an event, your user name and the time that you resolved the event are added in the events list (Resolved By) for the selected events. After you have taken corrective action for the event, you must mark the event as resolved.

- **Add Alert**

  Displays the Add Alert dialog box, which enables you to add an alert for the selected event.

What the Event Information section displays

You use the Event Information section on the Event details page to view the details about a selected event, such as the event severity, impact level, impact area, and event source.

Fields that are not applicable to the event type are hidden. You can view the following event details:

- **Event Trigger Time**

  The time at which the event was generated.

- **State**

  The event state: New, Acknowledged, Resolved, or Obsolete.

- **Obsoleted Cause**

  The actions that caused the event to be obsoleted, for example, the issue was fixed.

- **Event Duration**

  For active (new and acknowledged) events, this is the time between detection and the time when the event was last analyzed. For obsolete events, this is the time between detection and when the event was resolved.

  This field is displayed for all performance events, and for other event types only after they have been resolved or obsoleted.

- **Last Seen**

  The date and time at which the event was last seen as active.

  For performance events this value may be more recent than the Event Trigger Time as this field is updated after each new collection of performance data as long as the event is active. For other types of events, when in the New or Acknowledged state, this content is not updated and the field is therefore hidden.

- **Severity**

  The event severity: Critical (), Error (), Warning (), and Information ().

- **Impact Level**

  The event impact level: Incident, Risk, Event, or Upgrade.

- **Impact Area**

  The event impact area: Availability, Capacity, Performance, Protection, Configuration, or Security.

- **Source**

  The name of the object on which the event has occurred.

  When viewing the details for a shared QoS policy event, up to three of the workload objects that are consuming the most IOPS or MBps are listed in this field.

  You can click the source name link to display the health or performance details page for that object.

- **Source Annotations**

  Displays the annotation name and value for the object to which the event is associated.

  This field is displayed only for health events on clusters, SVMs, and volumes.

- **Source Groups**

  Displays the names of all the groups of which the impacted object is a member.

  This field is displayed only for health events on clusters, SVMs, and volumes.

- **Source Type**

  The object type (for example, SVM, Volume, or Qtree) with which the event is associated.

- **On Cluster**

  The name of the cluster on which the event occurred.

  You can click the cluster name link to display the health or performance details page for that cluster.

- **Affected Objects Count**

  The number of objects affected by the event.

  You can click the object link to display the inventory page populated with the objects that are currently affected by this event.

  This field is displayed only for performance events.

- **Affected Volumes**

  The number of volumes that are being affected by this event.

  This field is displayed only for performance events on nodes or aggregates.

- **Triggered Policy**

The name of the threshold policy that issued the event.

You can hover your cursor over the policy name to see the details of the threshold policy. For adaptive QoS policies the defined policy, block size, and allocation type (allocated space or used space) is also displayed.

This field is displayed only for performance events.

- **Rule Id**

  For Active IQ platform events, this is the number of the rule that was triggered to generate the event.

- **Acknowledged by**

  The name of the person who acknowledged the event and the time that the event was acknowledged.

- **Resolved by**

  The name of the person who resolved the event and the time that the event was resolved.

- **Assigned to**

  The name of the person who is assigned to work on the event.

- **Alert Settings**

  The following information about alerts is displayed:

  - If there are no alerts associated with the selected event, an **Add alert** link is displayed.

    You can open the Add Alert dialog box by clicking the link.

  - If there is one alert associated with the selected event, the alert name is displayed.

    You can open the Edit Alert dialog box by clicking the link.

  - If there is more than one alert associated with the selected event, the number of alerts is displayed.

    You can open the Alert Setup page by clicking the link to view more details about these alerts.

  Alerts that are disabled are not displayed.

- **Last Notification Sent**

  The date and time at which the most recent alert notification was sent.

- **Send by**

  The mechanism that was used to send the alert notification: email or SNMP trap.

- **Previous Script Run**

  The name of the script that was executed when the alert was generated.

What the Suggested Actions section displays

The Suggested Actions section of the Event details page provides possible reasons for the event and suggests a few actions so that you can try to resolve the event on your own. The suggested actions are customized based on the type of event or type of threshold that has been breached.

This area is displayed only for some types of events.

In some cases there are **Help** links provided on the page that reference additional information for many suggested actions, including instructions for performing a specific action. Some of the actions may involve using Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, ONTAP CLI commands, or a combination of these tools.

You should consider the actions suggested here as only a guidance in resolving this event. The action you take to resolve this event should be based on the context of your environment.

If you want to analyze the object and event in more detail, click the **Analyze Workload** button to display the Workload Analysis page.

There are certain events that Unified Manager can diagnose thoroughly and provide a single resolution. When available, those resolutions are displayed with a **Fix It** button. Click this button to have Unified Manager fix the issue causing the event.

For Active IQ platform events, this section may contain a link to a NetApp Knowledgebase article, when available, that describes the issue and possible resolutions. In sites with no external network access, a PDF of the Knowledgebase article is opened locally; the PDF is part of the rules file that you manually download to the Unified Manager instance.

What the System Diagnosis section displays

The System Diagnosis section of the Event details page provides information that can help you diagnose issues that may have been responsible for the event.

This area is displayed only for some events.

Some performance events provide charts that are relevant to the particular event that has been triggered. Typically this includes and IOPS or MBps chart and a latency chart for the previous ten days. When arranged this way you can see which storage components are most affecting latency, or being affected by latency, when the event is active.

For dynamic performance events, the following charts are displayed:

- Workload Latency - Displays the history of latency for the top victim, bully, or shark workloads at the component in contention.
- Workload Activity - Displays details about the workload usage of the cluster component in contention.
- Resource Activity - Display historical performance statistics for the cluster component in contention.

Other charts are displayed when some cluster components are in contention.

Other events provide a brief description of the type of analysis the system is performing on the storage object. In some cases there will be one or more lines; one for each component that has been analyzed, for system-defined performance policies that analyze multiple performance counters. In this scenario, a green or red icon

displays next to the diagnosis to indicate whether an issue was found, or not, in that particular diagnosis.

Event Setup page

The Event Setup page displays the list of events that are disabled, and provides information such as the associated object type and severity of the event. You can also perform tasks such as disabling or enabling events globally.

You can access this page only if you have the Application Administrator or Storage Administrator role.

Command buttons

The command buttons enable you to perform the following tasks for selected events:

- **Disable**

  Launches the Disable Events dialog box, which you can use to disable events.

- **Enable**

  Enables selected events that you had chosen to disable previously.

- **Upload Rules**

  Launches the Upload Rules dialog box, which enables sites with no external network access to manually upload the Active IQ rules file to Unified Manager. The rules are run against cluster AutoSupport messages to generate events for system configuration, cabling, best practice, and availability as defined by the Active IQ platform.

- **Subscribe to EMS Events**

  Launches the Subscribe to EMS Events dialog box, which enables you to subscribe to receive specific Event Management System (EMS) events from the clusters that you are monitoring. The EMS collects information about events that occur on the cluster. When a notification is received for a subscribed EMS event, a Unified Manager event is generated with the appropriate severity.

List view

The List view displays (in tabular format) information about events that are disabled. You can use the column filters to customize the data that is displayed.

- **Event**

  Displays the name of the event that is disabled.

- **Severity**

  Displays the severity of the event. The severity can be Critical, Error, Warning, or Information.

- **Source Type**

  Displays the source type for which the event is generated.

Disable Events dialog box

The Disable Events dialog box displays the list of event types for which you can disable events. You can disable events for an event type based on a particular severity or for a set of events.

You must have the Application Administrator or Storage Administrator role.

Event Properties area

The Event Properties area specifies the following event properties:

- **Event Severity**

  Enables you to select events based on the severity type, which can be Critical, Error, Warning, or Information.

- **Event Name Contains**

  Enables you to filter events whose name contains the specified characters.

- **Matching events**

  Displays the list of events matching the event severity type and the text string you specify.

- **Disable events**

  Displays the list of events that you have selected for disabling.

  The severity of the event is also displayed along with the event name.

Command buttons

The command buttons enable you to perform the following tasks for the selected events:

- **Save and close**

  Disables the event type and closes the dialog box.

- **Cancel**

  Discards the changes and closes the dialog box.

Managing alerts

You can configure alerts to send notification automatically when specific events or events of certain severity types occur. You can also associate an alert with a script that is executed when an alert is triggered.

What alerts are

While events occur continuously, the Unified Manager generates an alert only when an

event meets specified filter criteria. You can choose the events for which alerts should be generated—for example, when a space threshold is exceeded or an object goes offline. You can also associate an alert with a script that is executed when an alert is triggered.

Filter criteria include object class, name, or event severity.

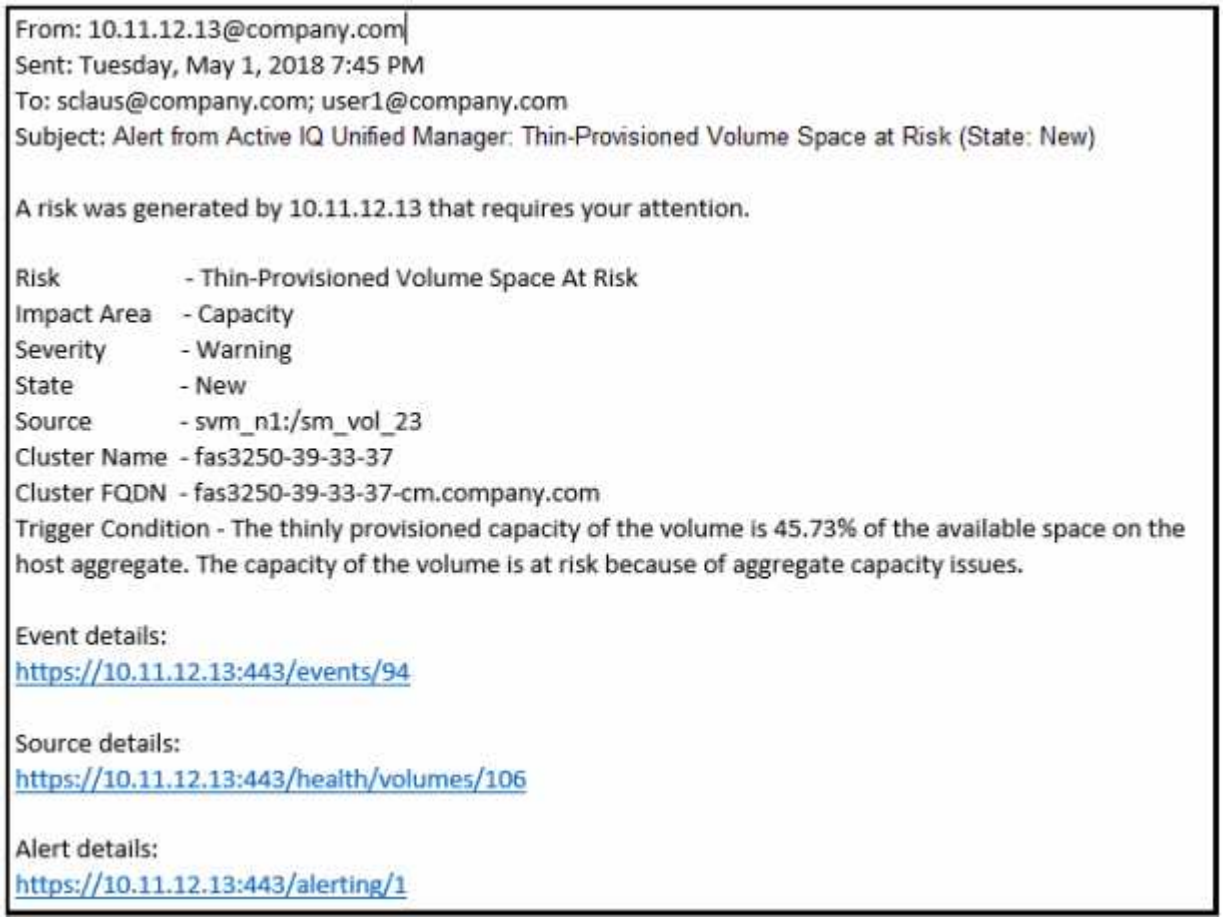
What information is contained in an alert email

Unified Manager alert emails provide the type of event, the severity of the event, the name of the policy or threshold that was breached to cause the event, and a description of the event. The email message also provides a hyperlink for each event that enables you to view the details page for the event in the UI.

Alert emails are sent to all users who have subscribed to receive alerts.

If a performance counter or capacity value has a large change during a collection period, it could cause both a critical and a warning event to be triggered at the same time for the same threshold policy. In this case, you may receive one email for the warning event and one for the critical event. This is because Unified Manager enables you to subscribe separately to receive alerts for warning and critical threshold breaches.

A sample alert email is shown below:


From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from Active IQ Unified Manager: Thin-Provisioned Volume Space at Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1

Adding alerts

You can configure alerts to notify you when a particular event is generated. You can

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

What you'll need

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

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

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. In the **Alert Setup** page, click **Add**.
3. In the **Add Alert** dialog box, click **Name**, and enter a name and description for the alert.
4. Click **Resources**, and select the resources to be included in or excluded from the alert.

   You can set a filter by specifying a text string in the **Name contains** field to select a group of resources. Based on the text string that you specify, the list of available resources displays only those resources that match the filter rule. The text string that you specify is case-sensitive.

   If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule, and the alert is not generated for events related to the excluded resource.

5. Click **Events**, and select the events based on the event name or event severity type for which you want to trigger an alert.

   To select more than one event, press the Ctrl key while you make your selections.

6. Click **Actions**, and select the users that you want to notify, choose the notification frequency, choose whether an SNMP trap will be sent to the trap receiver, and assign a script to be executed when an alert is generated.

   If you modify the email address that is specified for the user and reopen the alert for editing, the Name field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you modified the email address of the selected user from the Users page, the modified email address is not updated for the selected user.

   You can also choose to notify users through SNMP traps.

7. Click **Save**.

Example of adding an alert

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

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

Perform the following steps in the Add Alert dialog box:

1. Click **Name**, and enter **`HealthTest`** in the **Alert Name** field.
2. Click **Resources**, and in the Include tab, select **Volumes** from the drop-down list.
   a. Enter **`abc`** in the **Name contains** field to display the volumes whose name contains "abc".
   b. Select **<<All Volumes whose name contains 'abc'>>** from the Available Resources area, and move it to the Selected Resources area.
   c. Click **Exclude**, and enter **`xyz`** in the **Name contains** field, and then click **Add**.
3. Click **Events**, and select **Critical** from the Event Severity field.
4. Select **All Critical Events** from the Matching Events area, and move it to the Selected Events area.
5. Click **Actions**, and enter **`sample@domain.com`** in the Alert these users field.
6. Select **Remind every 15 minutes** to notify the user every 15 minutes.

   You can configure an alert to repeatedly send notifications to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.

7. In the Select Script to Execute menu, select **Test** script.
8. Click **Save**.

Guidelines for adding alerts

You can add alerts based on a resource, such as a cluster, node, aggregate, or volume, and events of a particular severity type. As a best practice, you can add an alert for any of your critical objects after you have added the cluster to which the object belongs.

You can use the following guidelines and considerations to create alerts to manage your systems effectively:

- Alert description

  You should provide a description for the alert so that it helps you track your alerts effectively.

- Resources

  You should decide which physical or logical resource requires an alert. You can include and exclude resources, as required. For example, if you want to closely monitor your aggregates by configuring an alert, you must select the required aggregates from the list of resources.

  If you select a category of resources, for example, **<<All User or Group Quotas>>**, then you will receive

alerts for all objects in that category.

> Selecting a cluster as the resource does not automatically select the storage objects within that cluster. For example, if you create an alert for all critical events for all clusters you will receive alerts only for cluster critical events. You will not receive alerts for critical events on nodes, aggregates, and so forth.

- Event severity

  You should decide if an event of a specified severity type (Critical, Error, Warning) should trigger the alert and, if so, which severity type.

- Selected Events

  If you add an alert based on the type of event generated, you should decide which events require an alert.

  If you select an event severity, but do not select any individual events (if you leave the "Selected Events" column empty) then you will receive alerts for all events in the category.

- Actions

  You must provide the user names and email addresses of the users who receive the notification. You can also specify an SNMP trap as a mode of notification. You can associate your scripts to an alert so that they are executed when an alert is generated.

- Notification frequency

  You can configure an alert to repeatedly send notification to the recipients for a specified time. You should determine the time from which the event notification is active for the alert. If you want the event notification to be repeated until the event is acknowledged, you should determine how often you want the notification to be repeated.

- Execute Script

  You can associate your script with an alert. Your script is executed when the alert is generated.

Adding alerts for performance events

You can configure alerts for individual performance events just like any other events received by Unified Manager. Additionally, if you want to treat all performance events alike and have email sent to the same person, you can create a single alert to notify you when any critical or warning performance events are triggered.

What you'll need

You must have the Application Administrator or Storage Administrator role.

The example below shows how to create an event for all critical latency, IOPS, and MBps events. You can use this same methodology to select events from all performance counters, and for all warning events.

Steps

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

2. In the **Alert Setup** page, click **Add**.
3. In the **Add Alert** dialog box, click **Name**, and enter a name and description for the alert.
4. Do not select any resources on the **Resources** page.

   Because no resources are selected, the alert is applied to all clusters, aggregates, volumes, and so on, for which these events are received.

5. Click **Events** and perform the following actions:
   a. In the Event Severity list, select **Critical**.
   b. In the Event Name Contains field, enter `latency` and then click the arrow to select all the matching events.
   c. In the Event Name Contains field, enter `iops` and then click the arrow to select all the matching events.
   d. In the Event Name Contains field, enter `mbps` and then click the arrow to select all the matching events.
6. Click **Actions** and then select the name of the user who will receive the alert email in the **Alert these users** field.
7. Configure any other options on this page for issuing SNMP traps and executing a script.
8. Click **Save**.

Testing alerts

You can test an alert to verify that you have configured it correctly. When an event is triggered, an alert is generated, and an alert email is sent to the configured recipients. You can verify whether the notification is sent and whether your script is executed by using the test alert.

What you'll need

- You must have configured notification settings such as the email address of the recipients, SMTP server, and SNMP trap.

  The Unified Manager server can use these settings to send notifications to users when an event is generated.

- You must have assigned a script and configured the script to run when the alert is generated.
- You must have the Application Administrator role.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. In the **Alert Setup** page, select the alert that you want to test, and then click **Test**.

   A test alert email is sent to the email addresses that you specified while creating the alert.

Enabling and Disabling alerts for Resolved and Obsolete events

For all events that you have configured to send alerts, an alert message is sent when

those events transition through all available states: New, Acknowledged, Resolved, and Obsolete. If you do not want to receive alerts for events as they move into the Resolved and Obsolete states, you can configure a global setting to suppress those alerts.

What you'll need

You must have the Application Administrator or Storage Administrator role.

By default, alerts are not sent for events as they move into the Resolved and Obsolete states.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. In the **Alert Setup** page, perform one of the following actions using the slider control next to the item **Alerts for Resolved and Obsolete events**:

To…	Do this…
Stop sending alerts as events are resolved or obsoleted	Move the slider control to the left
Start sending alerts as events are resolved or obsoleted	Move the slider control to the right

Excluding disaster recovery destination volumes from generating alerts

When configuring volume alerts you can specify a string in the Alert dialog box that identifies a volume or group of volumes. If you have configured disaster recovery for SVMs, however, the source and destination volumes have the same name, so you will receive alerts for both volumes.

What you'll need

You must have the Application Administrator or Storage Administrator role.

You can disable alerts for disaster recovery destination volumes by excluding volumes that have the name of the destination SVM. This is possible because the identifier for volume events contains both the SVM name and volume name in the format "<svm_name>:/<volume_name>".

The example below shows how to create alerts for volume "vol1" on the primary SVM "vs1", but exclude the alert from being generated on a volume with the same name on SVM "vs1-dr".

Perform the following steps in the Add Alert dialog box:

Steps

1. Click **Name** and enter a name and description for the alert.
2. Click **Resources**, and then select the **Include** tab.
   a. Select **Volume** from the drop-down list, and then enter **`vol1`** in the **Name contains** field to display the volumes whose name contains "vol1".
   b. Select **<<All Volumes whose name contains 'vol1'>>** from the **Available Resources** area, and move

it to the **Selected Resources** area.

3. Select the **Exclude** tab, select **Volume**, enter **`vs1-dr`** in the **Name contains** field, and then click **Add**.

   This excludes the alert from being generated for volume "vol1" on SVM "vs1-dr".

4. Click **Events** and select the event or events that you want to apply to the volume or volumes.
5. Click **Actions** and then select the name of the user who will receive the alert email in the **Alert these users** field.
6. Configure any other options on this page for issuing SNMP traps and executing a script, and then click **Save**.

Viewing alerts

You can view the list of alerts that is created for various events from the Alert Setup page. You can also view alert properties such as the alert description, notification method and frequency, events that trigger the alert, email recipients of the alerts, and affected resources such as clusters, aggregates, and volumes.

What you'll need

You must have the Operator, Application Administrator, or Storage Administrator role.

Step

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

   The list of alerts is displayed in the Alert Setup page.

Editing alerts

You can edit alert properties such as the resource with which the alert is associated, events, recipients, notification options, notification frequency, and associated scripts.

What you'll need

You must have the Application Administrator role.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. In the **Alert Setup** page, select the alert that you want to edit, and click **Edit**.
3. In the **Edit Alert** dialog box, edit the name, resources, events, and actions sections, as required.

   You can change or remove the script that is associated with the alert.

4. Click **Save**.

Deleting alerts

You can delete an alert when it is no longer required. For example, you can delete an alert that was created for a particular resource when that resource is no longer monitored

by Unified Manager.

What you'll need

You must have the Application Administrator role.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. On the **Alert Setup** page, select the alerts that you want to delete, and click **Delete**.
3. Click **Yes** to confirm the delete request.

Description of alert windows and dialog boxes

You should configure alerts to receive notifications about events by using the Add Alert dialog box. You can also view the list of alerts from the Alert Setup page.

Alert Setup page

The Alert Setup page displays a list of alerts and provides information about the alert name, status, notification method, and notification frequency. You can also add, edit, remove, enable, or disable alerts from this page.

You must have the Application Administrator or Storage Administrator role.

Command buttons

- **Add**

  Displays the Add Alert dialog box, which enables you to add new alerts.

- **Edit**

  Displays the Edit Alert dialog box, which enables you to edit selected alerts.

- **Delete**

  Deletes the selected alerts.

- **Enable**

  Enables the selected alerts to send notifications.

- **Disable**

  Disables the selected alerts when you want to temporarily stop sending notifications.

- **Test**

  Tests the selected alerts to verify their configuration after being added or edited.

- **Alerts for Resolved and Obsolete Events**

  Allows you to enable or disable the sending of alerts when events are moved to the Resolved or Obsolete

states. This can help users from receiving unnecessary notifications.

List view

The list view displays, in tabular format, information about the alerts that are created. You can use the column filters to customize the data that is displayed. You can also select an alert to view more information about it in the details area.

- **Status**

  Specifies whether an alert is enabled () or disabled ().

- **Alert**

  Displays the name of the alert.

- **Description**

  Displays a description for the alert.

- **Notification Method**

  Displays the notification method that is selected for the alert. You can notify users through email or SNMP traps.

- **Notification Frequency**

  Specifies the frequency (in minutes) with which the management server continues to send notifications until the event is acknowledged, resolved, or moved to the Obsolete state.

Details area

The details area provides more information about the selected alert.

- **Alert Name**

  Displays the name of the alert.

- **Alert Description**

  Displays a description for the alert.

- **Events**

  Displays the events for which you want to trigger the alert.

- **Resources**

  Displays the resources for which you want to trigger the alert.

- **Includes**

  Displays the group of resources for which you want to trigger the alert.

- **Excludes**

Displays the group of resources for which you do not want to trigger the alert.

- **Notification Method**

  Displays the notification method for the alert.

- **Notification Frequency**

  Displays the frequency with which the management server continues to send alert notifications until the event is acknowledged, resolved, or moved to the Obsolete state.

- **Script Name**

  Displays the name of the script associated with the selected alert. This script is executed when an alert is generated.

- **Email Recipients**

  Displays the email addresses of users who receive the alert notification.

Add Alert dialog box

You can create alerts to notify you when a particular event is generated, so that you can address the issue quickly and thereby minimize impact to your environment. You can create alerts for a single resource or a set of resources, and for events of a particular severity type. You can also specify the notification method and frequency of the alerts.

You must have the Application Administrator or Storage Administrator role.

Name

This area enables you to specify a name and description for the alert:

- **Alert Name**

  Enables you to specify an alert name.

- **Alert Description**

  Enables you to specify a description for the alert.

Resources

This area enables you to select an individual resource or group the resources based on a dynamic rule for which you want to trigger the alert. A *dynamic rule* is the set of resources filtered based on the text string you specify. You can search for resources by selecting a resource type from the drop-down list or you can specify the exact resource name to display a specific resource.

If you are creating an alert from any of the storage object details pages, the storage object is automatically included in the alert.

- **Include**

  Enables you to include the resources for which you want to trigger alerts. You can specify a text string to

group resources that match the string and select this group to be included in the alert. For example, you can group all volumes whose name contains the "abc" string.

- **Exclude**

  Enables you to exclude resources for which you do not want to trigger alerts. For example, you can exclude all volumes whose name contains the "xyz" string.

  The Exclude tab is displayed only when you select all resources of a particular resource type: for example, <<All Volumes>> or <<All Volumes whose name contains 'xyz'>>.

  If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule and the alert is not generated for the event.

Events

This area enables you to select the events for which you want to create the alerts. You can create alerts for events based on a particular severity or for a set of events.

To select more than one event, you should hold down the Ctrl key while you make your selections.

- **Event Severity**

  Enables you to select events based on the severity type, which can be Critical, Error, or Warning.

- **Event Name Contains**

  Enables you to select events whose name contains specified characters.

Actions

This area enables you to specify the users that you want to notify when an alert is triggered. You can also specify the notification method and the frequency of notification.

- **Alert these users**

  Enables you to specify the email address or user name of the user to receive notifications.

  If you modify the email address that is specified for the user and reopen the alert for editing, the Name field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you have modified the email address of the selected user from the Users page, the modified email address is not updated for the selected user.

- **Notification Frequency**

  Enables you to specify the frequency with which the management server sends notifications until the event is acknowledged, resolved, or moved to the obsolete state.

  You can choose the following notification methods:

  - Notify only once
  - Notify at a specified frequency
  - Notify at a specified frequency within the specified time range

- **Issue SNMP trap**

  Selecting this box enables you to specify whether SNMP traps should be sent to the globally configured SNMP host.

- **Execute Script**

  Enables you to add your custom script to the alert. This script is executed when an alert is generated.

> If you do not see this capability available in the user interface it is because the functionality has been disabled by your administrator. If required, you can enable this functionality from **Storage Management** > **Feature Settings**.

Command buttons

- **Save**

  Creates an alert and closes the dialog box.

- **Cancel**

  Discards the changes and closes the dialog box.

Edit Alert dialog box

You can edit alert properties such as the resource with which the alert is associated, events, script, and notification options.

Name

This area enables you to edit the name and description for the alert.

- **Alert Name**

  Enables you to edit the alert name.

- **Alert Description**

  Enables you to specify a description for the alert.

- **Alert State**

  Enables you to enable or disable the alert.

Resources

This area enables you to select an individual resource or group the resources based on a dynamic rule for which you want to trigger the alert. You can search for resources by selecting a resource type from the drop-down list or you can specify the exact resource name to display a specific resource.

- **Include**

  Enables you to include the resources for which you want to trigger alerts. You can specify a text string to

group resources that match the string and select this group to be included in the alert. For example, you can group all volumes whose name contains the “vol0” string.

- **Exclude**

  Enables you to exclude resources for which you do not want to trigger alerts. For example, you can exclude all volumes whose name contains the “xyz” string.

  The Exclude tab is displayed only when you select all resources of a particular resource type—for example, <<All Volumes>> or <<All Volumes whose name contains 'xyz'>>.

Events

This area enables you to select the events for which you want to trigger the alerts. You can trigger an alert for events based on a particular severity or for a set of events.

- **Event Severity**

  Enables you to select events based on the severity type, which can be Critical, Error, or Warning.

- **Event Name Contains**

  Enables you to select events whose name contains the specified characters.

Actions

This area enables you to specify the notification method and the frequency of notification.

- **Alert these users**

  Enables you to edit the email address or user name, or specify a new email address or user name to receive notifications.

- **Notification Frequency**

  Enables you to edit the frequency with which the management server sends notifications until the event is acknowledged, resolved, or moved to the obsolete state.

  You can choose the following notification methods:

  - Notify only once
  - Notify at a specified frequency
  - Notify at a specified frequency within the specified time range

- **Issue SNMP trap**

  Enables you to specify whether SNMP traps should be sent to the globally configured SNMP host.

- **Execute Script**

  Enables you to associate a script with the alert. This script is executed when an alert is generated.

Command buttons

- **Save**

  Saves the changes and closes the dialog box.

- **Cancel**

  Discards the changes and closes the dialog box.

Managing scripts

You can use scripts to automatically modify or update multiple storage objects in Unified Manager. The script is associated with an alert. When an event triggers an alert, the script is executed. You can upload custom scripts and test their execution when an alert is generated.

The ability to upload scripts to Unified Manager and run them is enabled by default. If your organization does not want to allow this functionality because of security reasons, you can disable this functionality from **Storage Management** > **Feature Settings**.

Related information

Enabling and disabling the ability to upload scripts

How scripts work with alerts

You can associate an alert with your script so that the script is executed when an alert is raised for an event in Unified Manager. You can use the scripts to resolve issues with storage objects or identify which storage objects are generating the events.

When an alert is generated for an event in Unified Manager, an alert email is sent to the specified recipients. If you have associated an alert with a script, the script is executed. You can get the details of the arguments passed to the script from the alert email.

If you have created a custom script and associated it with an alert for a specific event type, actions are taken based on your custom script for that event type, and the **Fix it** actions are not available by default on the Management Actions page or Unified Manager dashboard.

The script uses the following arguments for execution:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`

- `-eventArgs`

You can use the arguments in your scripts and gather related event information or modify storage objects.

Example for obtaining arguments from scripts

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

When an alert is generated, this script is executed and the following output is displayed:

```
-`eventID : 290`
-`eventSourceID : 4138`
```

Adding scripts

You can add scripts in Unified Manager, and associate the scripts with alerts. These scripts are executed automatically when an alert is generated, and enable you to obtain information about storage objects for which the event is generated.

What you'll need

- You must have created and saved the scripts that you want to add to the Unified Manager server.
- The supported file formats for scripts are Perl, Shell, PowerShell, Python, and `.bat` files.

Platform on which Unified Manager is installed	Supported languages
VMware	Perl and Shell scripts
Linux	Perl, Python, and Shell scripts
Windows	PowerShell, Perl, Python, and .bat scripts

  - For Perl scripts, Perl must be installed on the Unified Manager server. For VMware installations, Perl 5 is installed by default and scripts will support only what Perl 5 supports. If Perl was installed after Unified Manager, you must restart the Unified Manager server.
  - For PowerShell scripts, the appropriate PowerShell execution policy must be set on the Windows server so that the scripts can be executed.

> If your script creates log files to track the alert script progress, you must make sure that the log files are not created anywhere within the Unified Manager installation folder.

- You must have the Application Administrator or Storage Administrator role.

You can upload custom scripts and gather event details about the alert.

If you do not see this capability available in the user interface it is because the functionality has been disabled by your administrator. If required, you can enable this functionality from **Storage Management** > **Feature Settings**.

Steps

1. In the left navigation pane, click **Storage Management** > **Scripts**.
2. In the **Scripts** page, click **Add**.
3. In the **Add Script** dialog box, click **Browse** to select your script file.
4. Enter a description for the script that you select.
5. Click **Add**.

Related information

Enabling and disabling the ability to upload scripts

Deleting scripts

You can delete a script from Unified Manager when the script is no longer required or valid.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- The script must not be associated with an alert.

Steps

1. In the left navigation pane, click **Storage Management** > **Scripts**.
2. In the **Scripts** page, select the script that you want to delete, and then click **Delete**.
3. In the **Warning** dialog box, confirm the deletion by clicking **Yes**.

Testing script execution

You can verify that your script is executed correctly when an alert is generated for a storage object.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have uploaded a script in the supported file format to Unified Manager.

Steps

1. In the left navigation pane, click **Storage Management** > **Scripts**.
2. In the **Scripts** page, add your test script.
3. In the left navigation pane, click **Storage Management** > **Alert Setup**.
4. In the **Alert Setup** page, perform one of the following actions:

To…	Do this…
Add an alert	a. Click **Add**. b. In the Actions section, associate the alert with your test script.
Edit an alert	a. Select an alert, and then click **Edit**. b. In the Actions section, associate the alert with your test script.

5. Click **Save**.
6. In the **Alert Setup** page, select the alert that you added or modified, and then click **Test**.

   The script is executed with the "-test" argument, and a notification alert is sent to the email addresses that were specified when the alert was created.

Supported Unified Manager CLI commands

As a storage administrator you can use the CLI commands to perform queries on the storage objects; for example, on clusters, aggregates, volumes, qtrees, and LUNs. You can use the CLI commands to query the Unified Manager internal database and the ONTAP database. You can also use CLI commands in scripts that are executed at the beginning or end of an operation or are executed when an alert is triggered.

All commands must be preceded with the command `um cli login` and a valid user name and password for authentication.

CLI command	Description	Output
`um cli login -u <username> [-p <password>]`	Logs in to the CLI. Because of security implications, you should enter only the user name following the "-u" option. When used in this manner you will be prompted for the password, and the password will not be captured in the history or process table. The session expires after three hours from the time of login, after which the user must login again.	Displays the corresponding message.
`um cli logout`	Logs out of the CLI.	Displays the corresponding message.
`um help`	Displays all first level subcommands.	Displays all first level subcommands.

CLI command	Description	Output
`um run cmd [ -t <timeout> ] <cluster> <command>`	The simplest way to run a command on one or more hosts. Mainly used for alert scripting to get or perform an operation on ONTAP. The optional timeout argument sets a maximum time limit (in seconds) for the command to complete on the client. The default is 0 (wait forever).	As received from ONTAP.
`um run query <sql command>`	Executes an SQL query. Only queries that read from the database are allowed. Any update, insert, or delete operations are not supported.	Results are displayed in a tabular form. If an empty set is returned, or if there is any syntax error or bad request, it displays the appropriate error message.
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	Adds a datasource to the list of managed storage systems. A datasource describes how connections to storage systems are made. The options -u (username) and -P (password) must be specified when adding a datasource. The option -t (protocol) specifies the protocol used to communicate with the cluster (http or https). If the protocol is not specified, then both protocols will be attempted The option -p (port) specifies the port used to communicate with the cluster. If the port is not specified, then the default value of the appropriate protocol will be attempted. This command can be executed only by the storage admin.	Prompts for the user accept the certificate and prints the corresponding message.
`um datasource list [ <datasource-id>]`	Displays the datasources for managed storage systems.	Displays the following values in tabular format: `ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message.`

CLI command	Description	Output
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	Modifies one or more datasource options. Can be executed only by the storage admin.	Displays the corresponding message.
`um datasource remove <datasource-id>`	Removes the datasource (cluster) from Unified Manager.	Displays the corresponding message.
`um option list [ <option> .. ]`	Lists all the options that you can configure using the set command.	Displays the following values in tabular format: `Name, Value, Default Value, and Requires Restart.`
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	Sets one or more options. The command can be executed only by the storage admin.	Displays the corresponding message.
`um version`	Displays the Unified Manager software version.	`Version ("9.6")`
`um lun list [-q] [ -ObjectType <object-id>]`	Lists the LUNs after filtering on the specified object. -q is applicable for all commands to show no header. ObjectType can be lun, qtree, cluster, volume, quota, or svm. For example: **`um lun list -cluster 1`** In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the LUNs within the cluster with ID 1.	Displays the following values in tabular format: `ID and LUN path.`

CLI command	Description	Output
`um svm list [-q] [ -ObjectType <object-id>]`	Lists the storage VMs after filtering on the specified object. ObjectType can be lun, qtree, cluster, volume, quota, or svm. For example: **`um svm list -cluster 1`** In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the storage VMs within the cluster with ID 1.	Displays the following values in tabular format: `Name and Cluster ID.`
`um qtree list [-q] [ -ObjectType <object-id>]`	Lists the qtrees after filtering on the specified object. -q is applicable for all commands to show no header. ObjectType can be lun, qtree, cluster, volume, quota, or svm. For example: **`um qtree list -cluster 1`** In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the qtrees within the cluster with ID 1.	Displays the following values in tabular format: `Qtree ID and Qtree Name.`
`um disk list [-q] [- ObjectType <object-id>]`	Lists the disks after filtering on the specified object. ObjectType can be disk, aggr, node, or cluster. For example: **`um disk list -cluster 1`** In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the disks within the cluster with ID 1.	Displays the following values in tabular format `ObjectType and object-id`.

CLI command	Description	Output
`um cluster list [-q] [-ObjectType <object-id>]`	Lists the clusters after filtering on the specified object. ObjectType can be disk, aggr, node, cluster, lun, qtree, volume, quota, or svm. For example: **`um cluster list -aggr 1`** In this example, "-aggr" is the objectType and "1" is the objectId. The command lists the cluster to which the aggregate with ID 1 belongs.	Displays the following values in tabular format: `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key`.
`um cluster node list [-q] [-ObjectType <object-id>]`	Lists the cluster nodes after filtering on the specified object. ObjectType can be disk, aggr, node, or cluster. For example: **`um cluster node list -cluster 1`** In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the nodes within the cluster with ID 1.	Displays the following values in tabular format `Name and Cluster ID`.
`um volume list [-q] [-ObjectType <object-id>]`	Lists the volumes after filtering on the specified object. ObjectType can be lun, qtree, cluster, volume, quota, svm, or aggregate. For example: **`um volume list -cluster 1`** In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the volumes within the cluster with ID 1.	Displays the following values in tabular format `Volume ID and Volume Name`.

CLI command	Description	Output
`um quota user list [-q] [-ObjectType <object-id>]`	Lists the quota users after filtering on the specified object. ObjectType can be qtree, cluster, volume, quota, or svm. For example: **`um quota user list -cluster 1`** In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the quota users within the cluster with ID 1.	Displays the following values in tabular format `ID, Name, SID and Email`.
`um aggr list [-q] [-ObjectType <object-id>]`	Lists the aggregates after filtering on the specified object. ObjectType can be disk, aggr, node, cluster, or volume. For example: **`um aggr list -cluster 1`** In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the aggregates within the cluster with ID 1.	Displays the following values in tabular format `Aggr ID, and Aggr Name`.
`um event ack <event-ids>`	Acknowledges one or more events.	Displays the corresponding message.
`um event resolve <event-ids>`	Resolves one or more events.	Displays the corresponding message.
`um event assign -u <username> <event-id>`	Assigns an event to a user.	Displays the corresponding message.
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	Lists the events generated by the system or user. Filters events based on source, state, and IDs.	Displays the following values in tabular format `Source, Source type, Name, Severity, State, User and Timestamp`.
`um backup restore -f <backup_file_path_and_name>`	Restores a MySQL database backup using .7z files.	Displays the corresponding message.

Description of script windows and dialog boxes

The Scripts page enables you to add scripts to Unified Manager.

Scripts page

The Scripts page enables you to add your custom scripts to Unified Manager. You can associate these scripts with alerts to enable automatic reconfiguration of storage objects.

The Scripts page enables you to add or delete scripts from Unified Manager.

Command buttons

- **Add**

  Displays the Add Script dialog box, which enables you to add scripts.

- **Delete**

  Deletes the selected script.

List view

The list view displays, in tabular format, the scripts that you added to Unified Manager.

- **Name**

  Displays the name of the script.

- **Description**

  Displays the description of the script.

Add Script dialog box

The Add Script dialog box enables you to add scripts to Unified Manager. You can configure alerts with your scripts to automatically resolve events that are generated for storage objects.

You must have the Application Administrator or Storage Administrator role.

- **Select Script File**

  Enables you to select a script for the alert.

- **Description**

  Enables you to specify a description for the script.