



Understanding more about events

OnCommand Unified Manager 9.5

NetApp

October 23, 2024

This PDF was generated from <https://docs.netapp.com/us-en/oncommand-unified-manager-95/online-help/concept-event-state-definitions.html> on October 23, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Understanding more about events 1
 - Event state definitions 1
 - Description of event severity types 1
 - Description of event impact levels 2
 - Description of event impact areas 3
 - How object status is computed 3
 - Sources of performance events 3
 - Dynamic performance event chart details 4
 - Types of system-defined performance threshold policies 5
 - List of events and severity types 8

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The state of an event when it is automatically corrected or when the cause of the event is no longer valid.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 Therefore, the Cluster Not Reachable event is no longer valid, and the event state changes to Obsolete in the next monitoring cycle.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, or Event) 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.

Description of event impact areas

Events are categorized into five impact areas (availability, capacity, configuration, performance, and protection) 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.

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.

Sources of performance events

Performance events are issues related to workload performance on a cluster. They help you identify storage objects with slow response times, also known as high latency. Together with other health events that occurred at the same time, you can determine the issues that might have caused, or contributed to, the slow response times.

Unified Manager receives performance events from the following sources:

- **User-defined performance threshold policy events**

Performance issues based on custom threshold values that you have set. You configure performance threshold policies for storage objects; for example, aggregates and volumes, so that events are generated when a threshold value for a performance counter has been breached.

You must define a performance threshold policy and assign it to a storage object to receive these events.

- **System-defined performance threshold policy events**

Performance issues based on threshold values that are system-defined. These threshold policies are included with the installation of Unified Manager to cover common performance problems.

These threshold policies are enabled by default, and you might see events shortly after adding a cluster.

- **Dynamic performance threshold events**

Performance issues that are the result of failures or errors in an IT infrastructure, or from workloads overutilizing cluster resources. The cause of these events might be a simple issue that corrects itself over a period of time or that can be addressed with a repair or configuration change. A dynamic threshold event indicates that volume workloads on an ONTAP system are slow due to other workloads with high usage of shared cluster components.

These thresholds are enabled by default, and you might see events after three days of collecting data from a new cluster.

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 MBps 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.

Types of system-defined performance threshold policies

Unified Manager provides some standard threshold policies that monitor cluster performance and generate events automatically. These policies are enabled by default, and they generate warning or information events when the monitored performance thresholds are breached.



System-defined performance threshold policies are not enabled on Cloud Volumes ONTAP, ONTAP Edge, or ONTAP Select systems.

If you are receiving unnecessary events from any system-defined performance threshold policies, you can disable individual policies from the Configuration/Manage Events page.

Node threshold policies

The system-defined node performance threshold policies are assigned, by default, to every node in the clusters being monitored by Unified Manager:

- **Node resources over-utilized**

Identifies situations in which a single node is operating above the bounds of its operational efficiency, and therefore potentially affecting workload latencies. This is a warning event.

For nodes installed with ONTAP 8.3.x and earlier software, it does this by looking for nodes that are using more than 85% of their CPU and RAM resources (node utilization) for more than 30 minutes.

For nodes installed with ONTAP 9.0 and later software, it does this by looking for nodes that are using more than 100% of their performance capacity for more than 30 minutes.

- **Node HA pair over-utilized**

Identifies situations in which nodes in an HA pair are operating above the bounds of the HA pair operational efficiency. This is an informational event.

For nodes installed with ONTAP 8.3.x and earlier software, it does this by looking at the CPU and RAM usage for the two nodes in the HA pair. If the combined node utilization of the two nodes exceeds 140% for more than one hour, then a controller failover will impact workload latencies.

For nodes installed with ONTAP 9.0 and later software, it does this by looking at the performance capacity used value for the two nodes in the HA pair. If the combined performance capacity used of the two nodes exceeds 200% for more than one hour, then a controller failover will impact workload latencies.

- **Node disk fragmentation**

Identifies situations in which a disk or disks in an aggregate are fragmented, slowing key system services and potentially affecting workload latencies on a node.

It does this by looking at certain read and write operation ratios across all aggregates on a node. This policy might also be triggered during SyncMirror resynchronization or when errors are found during disk scrub operations. This is a warning event.



The “Node disk fragmentation” policy analyzes HDD-only aggregates; Flash Pool, SSD, and FabricPool aggregates are not analyzed.

Aggregate threshold policies

The system-defined aggregate performance threshold policy is assigned by default to every aggregate in the clusters being monitored by Unified Manager.

- **Aggregate disks over-utilized**

Identifies situations in which an aggregate is operating above the limits of its operational efficiency, thereby potentially affecting workload latencies. It identifies these situations by looking for aggregates where the disks in the aggregate are more than 95% utilized for more than 30 minutes. This multicondition policy then

performs the following analysis to help determine the cause of the issue:

- Is a disk in the aggregate currently undergoing background maintenance activity?

Some of the background maintenance activities a disk could be undergoing are disk reconstruction, disk scrub, SyncMirror resynchronization, and reparity.

- Is there a communications bottleneck in the disk shelf Fibre Channel interconnect?
- Is there too little free space in the aggregate? A warning event is issued for this policy only if one (or more) of the three subordinate policies are also considered breached. A performance event is not triggered if only the disks in the aggregate are more than 95% utilized.



The “Aggregate disks over-utilized” policy analyzes HDD-only aggregates and Flash Pool (hybrid) aggregates; SSD and FabricPool aggregates are not analyzed.

QoS threshold policies

The system-defined QoS performance threshold policies are assigned to any workload that has a configured ONTAP QoS maximum throughput policy (IOPS, IOPS/TB, or MBps). Unified Manager triggers an event when the workload throughput value is 15% less than the configured QoS value.

• QoS Max IOPS or MBps threshold

Identifies volumes and LUNs that have exceeded their QoS maximum IOPS or MBps throughput limit, and that are affecting workload latency. This is a warning event.

When a single workload is assigned to a policy group, it does this by looking for workloads that have exceeded the maximum throughput threshold defined in the assigned QoS policy group during each collection period for the previous hour.

When multiple workloads share a single QoS policy, it does this by adding the IOPS or MBps of all workloads in the policy and checking that total against the threshold.

• QoS Peak IOPS/TB or IOPS/TB with Block Size threshold

Identifies volumes that have exceeded their adaptive QoS peak IOPS/TB throughput limit (or IOPS/TB with Block Size limit), and that are affecting workload latency. This is a warning event.

It does this by converting the peak IOPS/TB threshold defined in the adaptive QoS policy into a QoS maximum IOPS value based on the size of each volume, and then it looks for volumes that have exceeded the QoS max IOPS during each performance collection period for the previous hour.



This policy is applied to volumes only when the cluster is installed with ONTAP 9.3 and later software.

When the “block size” element has been defined in the adaptive QoS policy, the threshold is converted into a QoS maximum MBps value based on the size of each volume. Then it looks for volumes that have exceeded the QoS max MBps during each performance collection period for the previous hour.



This policy is applied to volumes only when the cluster is installed with ONTAP 9.5 and later software.

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
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

Event name(Trap name)	Impact level	Source type	Severity
MetroCluster Aggregate Left Behind(ocumEvtMetroClusterAggregateLeftBehind)	Risk	Aggregate	Error
MetroCluster Aggregate Mirroring Degraded(ocumEvtMetroClusterAggregateMirrorDegraded)	Risk	Aggregate	Error
Object-store Access Denied for Aggregate Relocation *	Risk	Aggregate	Error
Object-store Access Denied for Aggregate Relocation During Storage Failover *	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

Event name(Trap name)	Impact level	Source type	Severity
Aggregate Snapshot Reserve Full(ocumEvtAggregateSnapshotReserveFull)	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 MBps Critical Threshold Breached(ocumAggregateMbpsIncident)	Incident	Aggregate	Critical
Aggregate MBps Warning Threshold Breached(ocumAggregateMbpsWarning)	Risk	Aggregate	Warning

Event name(Trap name)	Impact level	Source type	Severity
Aggregate Latency Critical Threshold Breached(ocumAggregateLatencyIncident)	Incident	Aggregate	Critical
Aggregate Latency Warning Threshold Breached(ocumAggregateLatencyWarning)	Risk	Aggregate	Warning
Aggregate Perf. Capacity Used Critical Threshold Breached(ocumAggregatePerfCapacityUsedIncident)	Incident	Aggregate	Critical
Aggregate Perf. Capacity Used Warning Threshold Breached(ocumAggregatePerfCapacityUsedWarning)	Risk	Aggregate	Warning
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
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

Event name(Trap name)	Impact level	Source type	Severity
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

Impact area: capacity

Event name(Trap name)	Impact level	Source type	Severity
Cluster Cloud Tier Planning (clusterCloudTierPlanningWarning)	Risk	Cluster	Warning
FabricPool Space Nearly Full *	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

Event name(Trap name)	Impact level	Source type	Severity
Emergency EMS received (Not applicable)	Event	Cluster	Critical
Critical EMS received (Not applicable)	Event	Cluster	Critical
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 IOPS Critical Threshold Breached(ocumClusterIopsIncident)	Incident	Cluster	Critical
Cluster IOPS Warning Threshold Breached(ocumClusterIopsWarning)	Risk	Cluster	Warning
Cluster MBps Critical Threshold Breached(ocumClusterMbpsIncident)	Incident	Cluster	Critical
Cluster MBps Warning Threshold Breached(ocumClusterMbpsWarning)	Risk	Cluster	Warning
Cluster Dynamic Threshold Breached(ocumClusterDynamicEventWarning)	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

Event name(Trap name)	Impact level	Source type	Severity
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
Disk Shelf Power Supplies Failed(ocumEvtShelfPowerSupplyFailed)	Incident	Storage shelf	Critical
Disk Shelf Multipath Not Configured(ocumDiskShelfConnectivityNotInMultiPath) This event does not apply to: <ul style="list-style-type: none"> • 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

Logical interface (LIF) events

LIF events provide information about the status of your 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
LIF Status Down(ocumEvtLifStatusDown)	Risk	Interface	Error
LIF Failover Not Possible(ocumEvtLifFailoverNotPossible)	Risk	Interface	Warning
LIF Not At Home Port(ocumEvtLifNotAtHomePort)	Risk	Interface	Warning

Impact area: configuration

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

Impact area: performance

Event name(Trap name)	Impact level	Source type	Severity
Network LIF MBps Critical Threshold Breached(ocumNetworkLifMbpsIncident)	Incident	Interface	Critical

Event name(Trap name)	Impact level	Source type	Severity
Network LIF MBps Warning Threshold Breached(ocumNetworkLifMbpsWarning)	Risk	Interface	Warning
FCP LIF MBps Critical Threshold Breached(ocumFcpLifMbpsIncident)	Incident	Interface	Critical
FCP LIF MBps Warning Threshold Breached(ocumFcpLifMbpsWarning)	Risk	Interface	Warning
NVMf FCP LIF MBps Critical Threshold Breached(ocumNvmfFcLifMbpsIncident)	Incident	Interface	Critical
NVMf FCP LIF MBps 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 *	Event	LUN	Information
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

Impact area: capacity

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

Impact area: performance

Event name(Trap name)	Impact level	Source type	Severity
LUN IOPS Critical Threshold Breached(ocumLunIopsIncident)	Incident	LUN	Critical
LUN IOPS Warning Threshold Breached(ocumLunIopsWarning)	Risk	LUN	Warning
LUN MBps Critical Threshold Breached(ocumLunMbpsIncident)	Incident	LUN	Critical
LUN MBps Warning Threshold Breached(ocumLunMbpsWarning)	Risk	LUN	Warning

Event name(Trap name)	Impact level	Source type	Severity
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 MBps Critical Threshold Breached(ocumLunLatencyMbpsIncident)	Incident	LUN	Critical
LUN Latency and MBps Warning Threshold Breached(ocumLunLatencyMbpsWarning)	Risk	LUN	Warning
LUN Latency and Aggregate Perf. Capacity Used Critical Threshold Breached(ocumLunLatencyAggregatePerfCapacityUsedIncident)	Incident	LUN	Critical
LUN Latency and Aggregate Perf. Capacity Used Warning Threshold Breached(ocumLunLatencyAggregatePerfCapacityUsedWarning)	Risk	LUN	Warning

Event name(Trap name)	Impact level	Source type	Severity
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 Perf. Capacity Used Critical Threshold Breached(ocumLunLatencyNodePerfCapacityUsedIncident)	Incident	LUN	Critical
LUN Latency and Node Perf. Capacity Used Warning Threshold Breached(ocumLunLatencyNodePerfCapacityUsedWarning)	Risk	LUN	Warning
LUN Latency and Node Perf. Capacity Used - Takeover Critical Threshold Breached(ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incident	LUN	Critical
LUN Latency and Node Perf. Capacity Used - Takeover Warning Threshold Breached(ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risk	LUN	Warning
LUN Latency and Node Utilization Critical Threshold Breached(ocumLunLatencyNodeUtilizationIncident)	Incident	LUN	Critical

Event name(Trap name)	Impact level	Source type	Severity
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 MBps Warning Threshold Breached(ocumQosLunMaxMbpsWarning)	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
Unified Manager Server Disk Space Nearly Full(ocumEvtUnifiedManagerDiskSpaceNearlyFull)	Risk	Management station	Warning
Unified Manager Server Disk Space Full(ocumEvtUnifiedManagerDiskSpaceFull)	Incident	Management station	Critical
Unified Manager Server Low On Memory(ocumEvtUnifiedManagerMemoryLow)	Risk	Management station	Warning

Event name(Trap name)	Impact level	Source type	Severity
Unified Manager Server Almost Out Of Memory(ocumEvtUnified ManagerMemoryAlmostOut)	Incident	Management station	Critical

Impact area: performance

Event name(Trap name)	Impact level	Source type	Severity
Performance Data Analysis Is Impacted(ocumEvtUnified ManagerDataMissingAnalyze)	Risk	Management station	Warning
Performance Data Collection Is Impacted(ocumEvtUnified ManagerDataMissingCollection)	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(ocumEvtBridge TemperatureAbnormal)	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 *(nvmeNamespaceStatus Offline)	Event	Namespace	Information
NVMeNS Online *(nvmeNamespaceStatus Online)	Event	Namespace	Information
NVMeNS Out of Space *(nvmeNamespaceSpace OutOfSpace)	Risk	Namespace	Warning
NVMeNS Destroy *(nvmeNamespaceDestro y)	Event	Namespace	Information

Impact area: performance

Event name(Trap name)	Impact level	Source type	Severity
NVMe Namespace IOPS Critical Threshold Breached(ocumNvmeNa mespacelopsIncident)	Incident	Namespace	Critical
NVMe Namespace IOPS Warning Threshold Breached(ocumNvmeNa mespacelopsWarning)	Risk	Namespace	Warning
NVMe Namespace MBps Critical Threshold Breached(ocumNvmeNa mespaceMbpsIncident)	Incident	Namespace	Critical
NVMe Namespace MBps Warning Threshold Breached(ocumNvmeNa mespaceMbpsWarning)	Risk	Namespace	Warning
NVMe Namespace Latency ms/op Critical Threshold Breached(ocumNvmeNa mespaceLatencyIncident)	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 MBps Critical Threshold Breached(ocumNvmeNamespaceLatencyMbpsIncident)	Incident	Namespace	Critical
NVMe Namespace Latency and MBps 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
Objstore Host Unresolvable *(ocumObjstoreHostUnresolvable)	Risk	Node	Error

Event name(Trap name)	Impact level	Source type	Severity
Objstore InterClusterLifDown *(ocumObjstoreInterClusterLifDown)	Risk	Node	Error
Request Mismatch Object-store Signature *	Risk	Node	Error
One of NFSv4 Pools Exhausted *	Incident	Node	Critical

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
Node IOPS Warning Threshold Breached(ocumNodeIopsWarning)	Risk	Node	Warning

Event name(Trap name)	Impact level	Source type	Severity
Node MBps Critical Threshold Breached(ocumNodeMbpsIncident)	Incident	Node	Critical
Node MBps 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 Perf. Capacity Used Critical Threshold Breached(ocumNodePerfCapacityUsedIncident)	Incident	Node	Critical
Node Perf. Capacity Used Warning Threshold Breached(ocumNodePerfCapacityUsedWarning)	Risk	Node	Warning
Node Perf.Capacity Used - Takeover Critical Threshold Breached(ocumNodePerfCapacityUsedTakeoverIncident)	Incident	Node	Critical
Node Perf.Capacity Used - Takeover Warning Threshold Breached(ocumNodePerfCapacityUsedTakeoverWarning)	Risk	Node	Warning
Node Utilization Critical Threshold Breached (ocumNodeUtilizationIncident)	Incident	Node	Critical

Event name(Trap name)	Impact level	Source type	Severity
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
Node Over-utilized Threshold Breached (ocumNodeOverUtilizedWarning)	Risk	Node	Warning
Node Dynamic Threshold Breached (ocumNodeDynamicEventWarning)	Risk	Node	Warning

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(ocumEvtPortStatus Down)	Incident	Node	Critical

Impact area: performance

Event name(Trap name)	Impact level	Source type	Severity
Network Port MBps Critical Threshold Breached(ocumNetworkPortMbpsIncident)	Incident	Port	Critical
Network Port MBps Warning Threshold Breached(ocumNetworkPortMbpsWarning)	Risk	Port	Warning
FCP Port MBps Critical Threshold Breached(ocumFcpPortMbpsIncident)	Incident	Port	Critical
FCP Port MBps 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

Event name(Trap name)	Impact level	Source type	Severity
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
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

Event name(Trap name)	Impact level	Source type	Severity
Service Processor Offline(ocumEvtServiceProcessorOffline)	Risk	Node	Error

SnapMirror relationship events

SnapMirror relationship events provide you with information about the status of your SnapMirror 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

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

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

Event name(Trap name)	Impact level	Source type	Severity
Mirror Replication Resync Failed(ocumEvtSnapmirrorRelationshipResyncFailed)	Risk	SnapMirror relationship	Error
Mirror Replication DeletedocumEvtSnapmirrorRelationshipDeleted	Risk	SnapMirror relationship	Warning
Synchronous Replication Out Of Sync *	Risk	SnapMirror relationship	Warning
Synchronous Replication Restored *	Event	SnapMirror relationship	Information
Synchronous Replication Auto Resync Failed *	Risk	SnapMirror relationship	Error

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
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
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 Relationship(ocumEvtStorageServiceUnsupportedRelationshipDeletion)	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

Event name(Trap name)	Impact level	Source type	Severity
Abnormal Temperature(ocumEvtShelfTemperatureAbnormal)	Risk	Storage shelf	Warning

SVM events

SVM events provide you with information about the status of your 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.

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
SVM CIFS Service Down(ocumEvtVserverCifsServiceStatusDown)	Incident	SVM	Critical
SVM CIFS Service Not Configured(Not applicable)	Event	SVM	Information
Attempts to Connect Nonexistent CIFS Share *	Incident	SVM	Critical
CIFS NetBIOS Name Conflict *	Risk	SVM	Error
CIFS Shadow Copy Operation Failed *	Risk	SVM	Error
Many CIFS Connections *	Risk	SVM	Error
Max CIFS Connection Exceeded *	Risk	SVM	Error
Max Number of CIFS Connection Per User Exceeded *	Risk	SVM	Error
SVM FC/FCoE Service Down(ocumEvtVserverFcServiceStatusDown)	Incident	SVM	Critical

Event name(Trap name)	Impact level	Source type	Severity
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 *	Risk	SVM	Error
No AV Server Connection for Virus Scan *	Incident	SVM	Critical
No AV Server Registered *	Risk	SVM	Error
No Responsive AV Server Connection *	Event	SVM	Information
Unauthorized User Attempt to AV Server *	Risk	SVM	Error
Virus Found By AV Server *	Risk	SVM	Error
SVM with Infinite Volume Storage Not Available(ocumEvtVserverStorageNotAvailable)	Incident	SVMs with Infinite Volume	Critical

Event name(Trap name)	Impact level	Source type	Severity
SVM with Infinite Volume Storage Partially Available(ocumEvtVserverStoragePartiallyAvailable)	Risk	SVMs with Infinite Volume	Error
SVM with Infinite Volume Namespace Mirror Constituents Having Availability Issues(ocumEvtVserverNsMirrorAvailabilityHavingIssues)	Risk	SVMs with Infinite Volume	Warning

Impact area: capacity

The following capacity events apply only to SVMs with Infinite Volume.

Event name(Trap name)	Impact level	Source type	Severity
SVM with Infinite Volume Space Full(ocumEvtVserverFull)	Risk	SVM	Error
SVM with Infinite Volume Space Nearly Full(ocumEvtVserverNearlyFull)	Risk	SVM	Warning
SVM with Infinite Volume Snapshot Usage Limit Exceeded(ocumEvtVserverSnapshotUsageExceeded)	Risk	SVM	Warning
SVM with Infinite Volume Namespace Space Full(ocumEvtVserverNamespaceFull)	Risk	SVM	Error
SVM with Infinite Volume Namespace Space Nearly Full(ocumEvtVserverNamespaceNearlyFull)	Risk	SVM	Warning

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 MBps Critical Threshold Breached(ocumSvmMbpsIncident)	Incident	SVM	Critical
SVM MBps Warning Threshold Breached(ocumSvmMbpsWarning)	Risk	SVM	Warning
SVM Latency Critical Threshold Breached(ocumSvmLatencyIncident)	Incident	SVM	Critical
SVM Latency Warning Threshold Breached(ocumSvmLatencyWarning)	Risk	SVM	Warning

SVM storage class events

SVM storage class events provide you with information about the status of your storage classes so that you can monitor for potential problems. SVM storage classes exist only in

SVMs with Infinite Volume. Events are grouped by impact area and include the event and trap name, impact level, source type, and severity.

The following SVM storage class events apply only to SVMs with Infinite Volume.

Impact area: availability

Event name(Trap name)	Impact level	Source type	Severity
SVM Storage Class Not Available(ocumEvtVserverStorageClassNotAvailable)	Incident	Storage class	Critical
SVM Storage Class Partially Available(ocumEvtVserverStorageClassPartiallyAvailable)	Risk	Storage class	Error

Impact area: capacity

Event name(Trap name)	Impact level	Source type	Severity
SVM Storage Class Space Nearly Full(ocumEvtVserverStorageClassNearlyFull)	Risk	Storage class	Warning
SVM Storage Class Space Full(ocumEvtVserverStorageClassFull)	Risk	Storage class	Error
SVM Storage Class Snapshot Usage Limit Exceeded(ocumEvtVserverStorageClassSnapshotUsageExceeded)	Risk	Storage class	Warning

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
Volume Offline(ocumEvtVolumeOffline)	Incident	Volume	Critical

Event name(Trap name)	Impact level	Source type	Severity
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
Volume Space Nearly Full(ocumEvtVolumeNearlyFull)	Risk	Volume	Warning

Event name(Trap name)	Impact level	Source type	Severity
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
Volume Space Guarantee Disabled(Not applicable)	Event	Volume	Information

Event name(Trap name)	Impact level	Source type	Severity
Volume Space Guarantee Enabled(Not Applicable)	Event	Volume	Information
Volume Space Guarantee Modified(Not applicable)	Event	Volume	Information
Volume Snapshot Reserve Days Until Full(ocumEvtVolumeSnapshotReserveDaysUntilFull Soon)	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 *	Risk	Volume	Error
WAFL Volume AutoSize Done *	Event	Volume	Information

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

Event name(Trap name)	Impact level	Source type	Severity
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 MBps Warning Threshold Breached(ocumQosVolumeMaxMbpsWarning)	Risk	Volume	Warning
QoS Volume Max IOPS/TB Warning Threshold Breached(ocumQosVolumeMaxIopsPerTbWarning)	Risk	Volume	Warning
Volume IOPS Critical Threshold Breached(ocumVolumeIopsIncident)	Incident	Volume	Critical
Volume IOPS Warning Threshold Breached(ocumVolumeIopsWarning)	Risk	Volume	Warning
Volume MBps Critical Threshold Breached(ocumVolumeMbpsIncident)	Incident	Volume	Critical
Volume MBps Warning Threshold Breached(ocumVolumeMbpsWarning)	Risk	Volume	Warning
Volume Latency ms/op Critical Threshold Breached(ocumVolumeLatencyIncident)	Incident	Volume	Critical

Event name(Trap name)	Impact level	Source type	Severity
Volume Latency ms/op Warning Threshold Breached(ocumVolumeLa tencyWarning)	Risk	Volume	Warning
Volume Cache Miss Ratio Critical Threshold Breached(ocumVolumeC acheMissRatioIncident)	Incident	Volume	Critical
Volume Cache Miss Ratio Warning Threshold Breached(ocumVolumeC acheMissRatioWarning)	Risk	Volume	Warning
Volume Latency and IOPS Critical Threshold Breached(ocumVolumeLa tencyIopsIncident)	Incident	Volume	Critical
Volume Latency and IOPS Warning Threshold Breached(ocumVolumeLa tencyIopsWarning)	Risk	Volume	Warning
Volume Latency and MBps Critical Threshold Breached(ocumVolumeLa tencyMbpsIncident)	Incident	Volume	Critical
Volume Latency and MBps Warning Threshold Breached(ocumVolumeLa tencyMbpsWarning)	Risk	Volume	Warning
Volume Latency and Aggregate Perf. Capacity Used Critical Threshold Breached(ocumVolumeLa tencyAggregatePerfCapa cityUsedIncident)	Incident	Volume	Critical
Volume Latency and Aggregate Perf. Capacity Used Warning Threshold Breached(ocumVolumeLa tencyAggregatePerfCapa cityUsedWarning)	Risk	Volume	Warning

Event name(Trap name)	Impact level	Source type	Severity
Volume Latency and Aggregate Utilization Critical Threshold Breached(ocumVolumeLatencyAggregateUtilizationIncident)	Incident	Volume	Critical
Volume Latency and Aggregate Utilization Warning Threshold Breached(ocumVolumeLatencyAggregateUtilizationWarning)	Risk	Volume	Warning
Volume Latency and Node Perf. Capacity Used Critical Threshold Breached(ocumVolumeLatencyNodePerfCapacityUsedIncident)	Incident	Volume	Critical
Volume Latency and Node Perf. Capacity Used Warning Threshold Breached(ocumVolumeLatencyNodePerfCapacityUsedWarning)	Risk	Volume	Warning
Volume Latency and Node Perf. Capacity Used - Takeover Critical Threshold Breached(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incident	Volume	Critical
Volume Latency and Node Perf. Capacity Used - Takeover Warning Threshold Breached(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risk	Volume	Warning

Event name(Trap name)	Impact level	Source type	Severity
Volume Latency and Node Utilization Critical Threshold Breached(ocumVolumeLatencyNodeUtilizationIncident)	Incident	Volume	Critical
Volume Latency and Node Utilization Warning Threshold Breached(ocumVolumeLatencyNodeUtilizationWarning)	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

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

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