Remediate alerts

NetApp Console local deployment

NetApp
August 10, 2026

Table of Contents

Remediate alerts

Learn about alerts in NetApp Console local deployment

NetApp Console local deployment generates alerts that identify health issues on your on-premises ONTAP clusters and for NetApp Backup and Recovery operations.

Console local deployment consolidates alerts from ONTAP clusters and Backup and Recovery operations into a single view. The Alerts page includes a dashboard, an alerts list, and a systems view so you can review alerts across the entire organization or scope them to a specific fleet or system. Each alert identifies the affected system, its severity, and its impact area.

Use alerts in Console local deployment to:

- Detect capacity, connectivity, data protection, performance, and security issues.
- Prioritize alerts by severity and impact area.
- Open an alert in System Manager or Workload Analyzer, then run a guided or automated Fix-It action when the page offers one.
- Route notifications through email to users with specified access roles, or send alert data to an external system through a webhook.
- Export the alerts list to a CSV file for offline analysis.

Alert severity and impact areas

Each alert includes a severity and an impact area:

- **Severity** indicates urgency, from highest to lowest: Critical, Major, Minor, Warning, and Info.
- **Impact area** identifies the affected domain: Capacity, Connectivity, Data protection, Performance, and Security.

Alert sources and scope

- **ONTAP alerts** originate from the ONTAP Event Management System (EMS) on the on-premises clusters that Console local deployment has discovered. Learn more about the ONTAP EMS and available alerts.
- **NetApp Backup and Recovery alerts** originate from Backup and Recovery actions. Learn more about NetApp Backup and Recovery alerts.
- Your permissions determine which fleets you can view. Scope the view to the entire organization, a specific fleet, or an individual system. The **Systems health** tab shows per-system status and the **Alerts** tab shows the current alert list for the selected scope.
- The CSV export reflects the current scope, search text, and filters.

Alert notification rules

Create notification rules to determine which alerts generate notifications and who receives them. A notification rule has the following characteristics:

- It matches alerts on the service (such as ONTAP management or Backup and Recovery), severity, impact area, and target system.

- For email delivery, it sends notifications to users with the specified access roles. For webhook delivery, it sends alert data to the configured endpoint—access to that data is controlled by the receiving application, not by Console local deployment.
- It applies to specific systems, not to fleets.
- It can be muted during a planned maintenance window to suppress expected alerts.

Console local deployment includes a default notification rule that is active immediately after installation. The default rule monitors all services and systems for Critical-severity alerts and delivers notifications to the Console Notification Center only—no email or webhook delivery is configured until you set it up. You can view and adjust this rule, and create custom rules to match your environment.

Info-level alerts are visible in the Alerts page but are not delivered by notification unless you explicitly create a rule that includes the Info severity level.

Related information

- Monitor and investigate alerts
- Create and manage alert notification rules
- Learn about ONTAP alerts in NetApp Console local deployment

Monitor and investigate alerts in NetApp Console local deployment

Monitor and investigate alerts in NetApp Console local deployment to keep your storage healthy and minimize disruption.

View active alerts across your entire organization or a specific fleet, prioritize them by severity and impact area, and investigate root causes so you can resolve issues before they escalate. When an alert includes a recommended action or Fix It option, you can move from investigation directly into remediation.

Required access role

All roles except Federation admin and Federation viewer. Users with the Federation admin or Federation viewer role cannot view alerts. Learn about access roles.

For ONTAP alerts, you can access tools such as System Manager and Workload Analyzer directly from the Alerts page to investigate and resolve issues.

For external reporting, you can export the alerts list to a CSV file for offline analysis.

You can also set up notification rules to receive alerts by email or webhook. Learn how to set up alert notifications.

Available alerts

NetApp Console local deployment supports alerts for ONTAP and NetApp Backup and Recovery.

- Learn about ONTAP alerts in NetApp Console local deployment
- Learn more about NetApp Backup and Recovery alerts.

View the alerts dashboard

Use the alerts dashboard to get a quick view of current alert activity for the scope you selected. The dashboard summarizes active alerts by severity and impact area, and it includes a chart that shows alert distribution over the past 24 hours so you can spot trends quickly.

You can filter the dashboard to focus on critical alerts or alerts for a specific impact area.

Steps

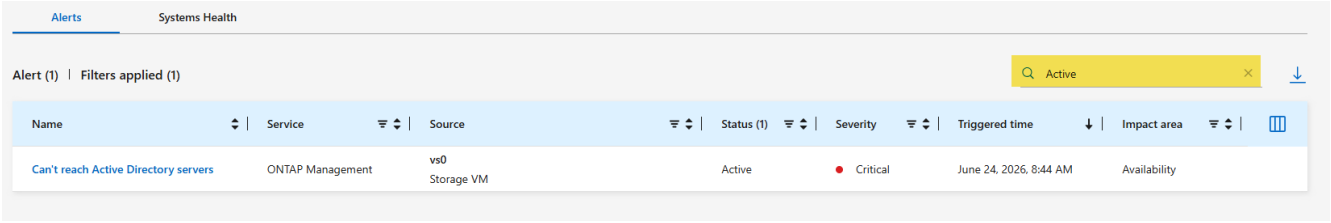
1. Select **Health > Alerts > Overview**.
2. From the scope selector, choose one of the following:
   - **All** (default) to see alerts across all fleets you have access to
   - A specific fleet to see alerts only for that fleet
3. Filter the dashboard according to the alerts you need to view, including:
   - Severity (Critical, Warning, or Informational)
   - Critical alerts grouped by impact area
   - Impact area (Security, Protection, Availability, Performance, Capacity, or Configuration)

View all alerts

Use the Alerts tab to view the full list of active alerts for the scope you've selected. The list updates to reflect the current organization or fleet scope, and you can search the list for specific alerts by name or description.

Steps

1. Select **Health > Alerts > Overview**.
2. From the scope selector, choose one of the following:
   - **All** (default) to see alerts across all fleets you have access to
   - A specific fleet to see alerts only for that fleet
3. Select the **Alerts** tab to view the full list of active alerts for the selected scope.
4. Optionally, search the list for a specific alert by name or description.



View alerts by system

You can view alerts for a specific system within a fleet or your organization.

Steps

1. Select **Health > Alerts > Overview**.
2. From the scope selector, choose one of the following:
   - **All** (default) to see alerts across all fleets you have access to

- A specific fleet to see alerts only for that fleet

3. Select the **Systems health** tab to view a summary of the alerts associated with the systems within the scope you've selected.
4. Select **View alerts** on the row of the respective system to view the full list of active alerts associated with that system.

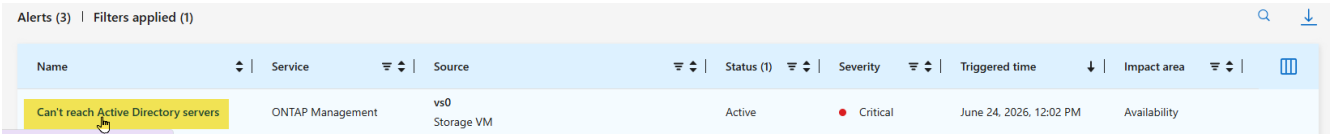
Investigate an alert

You can investigate an alert to see what triggered it and who received the notification.

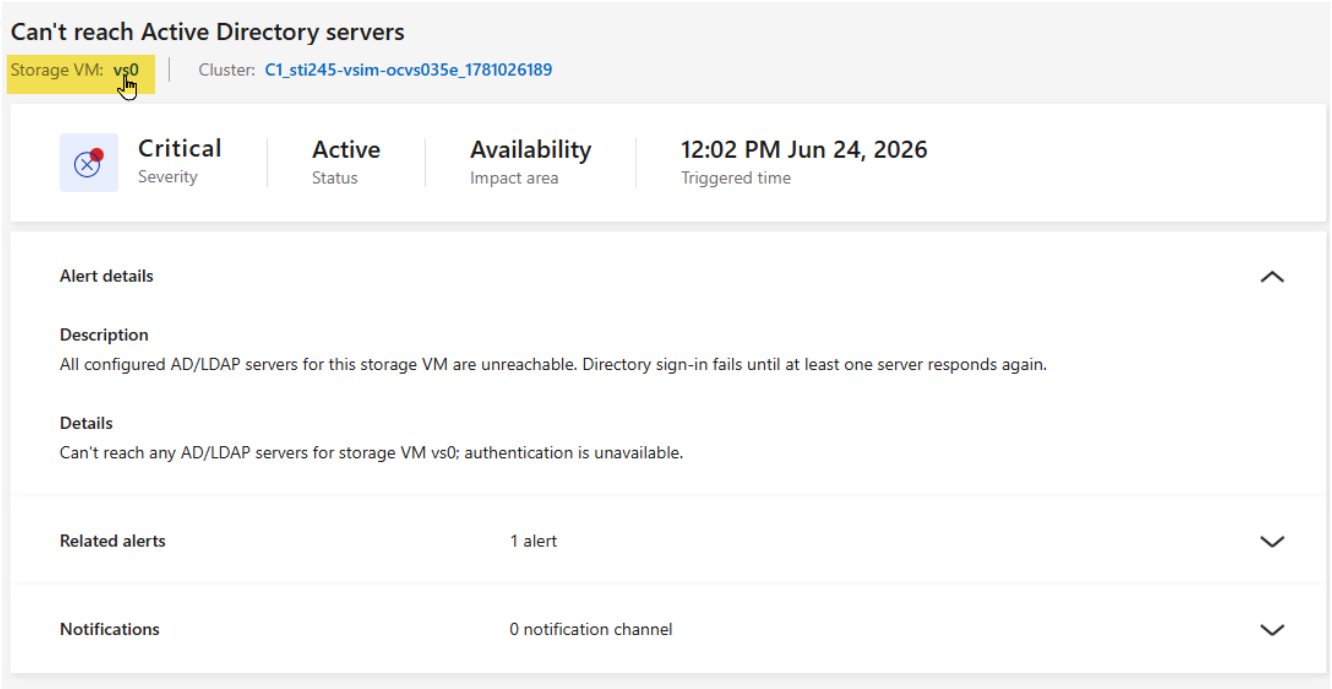
When investigating an ONTAP alert, you can also go directly to the System Manager interface for the system that generated the alert to view additional details and take action.

Steps

1. Select **Health > Alerts > Overview**.
2. From the scope selector, choose one of the following:
   - **All** (default) to see alerts across all fleets you have access to
   - A specific fleet to see alerts only for that fleet
3. In either tab, select the name of the alert you want to investigate to view its details.



4. If applicable, select the VM or cluster name to open the System Manager interface for the system that generated the alert.



Remediate an alert

When an alert includes a recommended action or Fix It option, use it to move from investigation into remediation without leaving the alert details.

Steps

1. Select **Health > Alerts > Overview**.
2. From the scope selector, choose one of the following:
   - **All** (default) to see alerts across all fleets you have access to
   - A specific fleet to see alerts only for that fleet
3. Select the alert you want to remediate.
4. Review the alert details, then select the recommended action or **Fix It** option if one is available.
5. Follow the guided steps to apply the remediation and then return to the alert details to confirm the alert state.

If the action resolves the issue, the alert no longer appears as active for that scope. If the alert remains active, review the alert details again and continue the investigation.

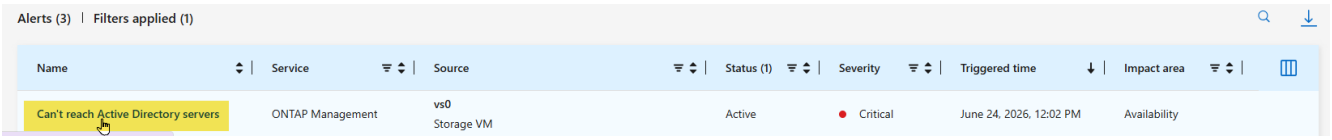
Analyze an alert

You can analyze an ONTAP alert in Workload Analyzer to understand what triggered it.

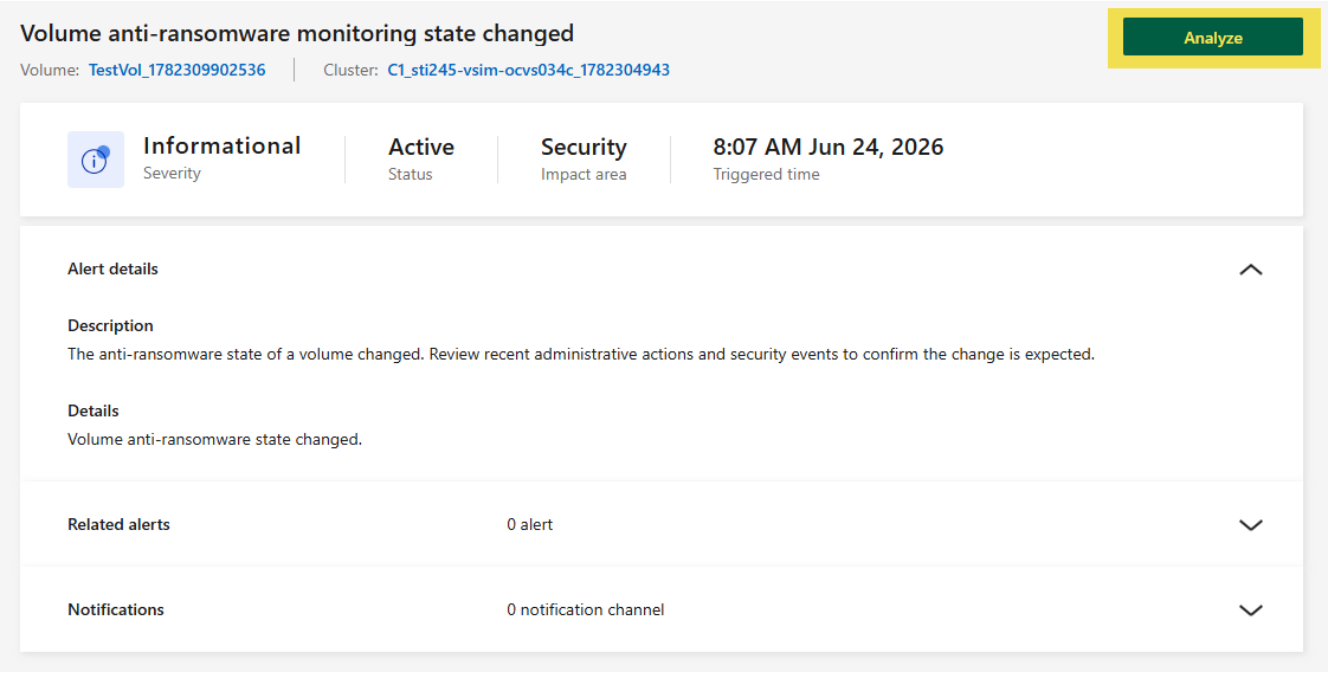
When investigating an ONTAP alert, you can also go directly to the System Manager interface for the system that generated the alert to view additional details and take action.

Steps

1. Select **Health > Alerts > Overview**.
2. From the scope selector, choose one of the following:
   - **All** (default) to see alerts across all fleets you have access to
   - A specific fleet to see alerts only for that fleet
3. Select the **Systems health** tab to view the full list of active alerts for the selected scope.
4. In either tab, select the name of the alert you want to investigate to view its details.



5. If applicable, select **Analyze** to open the Workload Analyzer interface for the system that generated the alert.



6. Enter the time range that covers the period when the alert was triggered, then select **Analyze** to view the analysis results. Learn about Workload Analyzer.

Export alerts to CSV

Export the alerts list in the NetApp Console local deployment to a CSV file for offline analysis or reporting. The export reflects the current scope (organization or fleet), search text, and filters.

Steps

1. Select **Health > Alerts** and then select the **Alerts** tab.
2. Set the scope (organization or fleet) and apply any filters or search text you want included in the export.
3. Select the download icon to export the alerts list to a CSV file.

Configure notification rules for alerts in NetApp Console local deployment

Configure notification rules in NetApp Console local deployment to control which alerts raise notifications, who receives them, and how they are delivered.

Required access roles

Super admin, Organization admin, Storage admin, Operations support analyst, or any of the admin roles for NetApp Backup and Recovery. Learn about access roles.

Use notification rules to route the right alerts to the right people through the channels that fit your environment, while reducing noise from alerts that aren't relevant to you. Notification rules complement the Alerts page: you investigate or remediate the alert in the Alerts workflow, then use rules to control how similar alerts are delivered in the future.

A notification rule matches alerts based on conditions you define—such as service, severity, and impact area—and then delivers a notification through the channels you select. The Console local deployment includes default notification rules that you can view and adjust, and you can create your own custom rules. You can also

mute rules to temporarily suppress notifications during planned events like maintenance windows.

- Learn more about the ONTAP EMS and available alerts.

Before you begin

- To deliver notifications by email, your Organization admin must configure an email server in the Console local deployment. To deliver notifications to an external system, your Organization admin must configure a webhook. For the steps, see Configure notification delivery.
- The Console local deployment Notification Center displays notifications by default, so no additional setup is required for in-console notifications.

View notification rules

The notification rules page is the central place to review and manage every rule that applies to your organization. Each rule shows its key attributes so that you can quickly assess and adjust your alerting behavior.

Steps

1. From the left navigation, select **Health > Alerts**.
2. Select **Notification settings**.
3. Review the rules in the list. Each rule shows its active status, name, the services and severity levels it monitors, the roles authorized to receive notifications, the enabled delivery channels, when it was last modified, and any scheduled mute period.
4. To find a specific rule, use the filter and search controls to filter by active status, service, severity, role, channel, or mute status.

Create a notification rule

Create a notification rule to define the conditions that trigger a notification and how that notification is delivered.

You can’t set notification rules for fleets. You can set them only for specific systems. In large environments with many systems, consider creating broader rules by severity rather than duplicating rules per system—for example, one Critical rule that covers all systems acts as a catch-all, with additional targeted rules for systems that need different routing or recipients.

Example notification rule for Critical alerts across all systems

Suppose you want to ensure no critical alert goes unnoticed, regardless of which system it originates from. You can create a broad rule that routes all critical alerts to the Console Notification Center for storage admins.

In this example, you create a rule with the following settings:

- **Services**: All
- **Severity**: Critical
- **IAM role**: Storage admin
- **System**: (Leave this blank to apply to all systems)
- **Delivery method**: Console Notification Center

With this rule in place, storage admins see a notification in the Console for every critical alert across all

systems. This rule acts as a baseline that you can supplement with more targeted rules.

Example of a targeted notification rule for Storage admin capacity alerts

Suppose your storage admins need to respond immediately to critical capacity issues on a specific production system, but you don't want lower-severity alerts to flood their inboxes. You can create a targeted rule that emails storage admins only when a critical capacity alert fires on that system.

In this example, you create a rule with the following settings:

- **Services**: ONTAP management
- **Severity**: Critical
- **Impact area**: Capacity
- **IAM role**: Storage admin
- **System**: <system_name>
- **Delivery method**: Email

With this rule in place, Console local deployment emails all storage admins for the specified system when a critical capacity alert occurs. Alerts with a lower severity, such as warning or informational, don't generate an email, so the team can focus on the issues that require urgent attention.

Steps

1. From the left navigation, select **Health > Alerts**.
2. Select **Notification settings**, and then select **Add rule**.
3. Define the conditions that the rule matches:
    - **Rule name**: enter a concise, descriptive name. This field is required.
    - **Rule description**: optionally, enter additional context about the rule's purpose.
    - **Services**: select one or more ONTAP or platform services that the rule applies to.
    - **Roles**: select the access roles that users must have to receive notifications when the rule is triggered.
    - **Severity levels**: select which severity levels the rule monitors, such as Critical, Warning, Error, or Information.
    - **Impact area**: select the operational areas to match, such as Capacity or Performance.
    - **Alert name**: select the specific alert types that trigger the rule.
    - **System**: select the system context that the rule applies to.
4. Select the delivery channels for the notification:
    - **Email**: sends alert emails to users who have the selected roles. Requires a configured email server.
    - **Webhook**: sends alert data to an external system. Requires selecting a configured webhook integration.
    - **Console Notification Center**: displays real-time alerts for users who have the selected roles.
5. Optionally, to suppress notifications from this rule during a planned period, such as a maintenance window, set a **Mute notifications** schedule, and choose a recurrence if you want the mute period to repeat. You can add multiple mute windows per rule, which is useful for recurring maintenance cycles such as weekly patching.
6. Select **Create**.

Enable or disable a notification rule

Enable or disable individual notification rules to control which conditions raise notifications. Disable rules that aren't relevant to your environment to reduce noise, and enable rules to start receiving their notifications again.

Steps

1. From the left navigation, select **Health > Alerts**.
2. Select **Notification settings**.
3. Locate the rule you want to change.
4. Toggle the rule's **Active** switch on or off. The change takes effect immediately.

Mute a notification rule

Mute a notification rule to suppress alert delivery during a planned event, such as a maintenance window, without disabling the rule. Alerts continue to appear in the Alerts page during the mute period—only the email, webhook, and in-console notifications are suppressed. When the mute window expires, notifications resume automatically.

You can add multiple mute windows to a single rule and configure each one to recur on a schedule.

Examples of mute windows

- **One-off maintenance window**: You're running a firmware upgrade on a storage system Saturday night and want to suppress the expected alerts during that window. Set a mute window for Saturday 10:00 PM to Sunday 2:00 AM with no recurrence. When the window expires, notifications resume automatically.
- **Recurring weekly patching window**: Your team patches systems every Sunday from midnight to 4:00 AM. Add a mute window with weekly recurrence so notifications are suppressed automatically each week without manual intervention. If a second system has its own patching schedule at a different time, add a second mute window to the same rule with its own start time and recurrence.

Steps

1. From the left navigation, select **Health > Alerts**.
2. Select **Notification rules**.
3. In the rules list, locate the rule you want to mute and select the action menu for that rule.
4. Select **Edit**.
5. In the **Mute notifications** section, set the start and end date and time for the mute window.
6. Optionally, select a recurrence to repeat the window on a schedule.
7. To add additional mute windows, select **Add mute window** and repeat the previous steps.
8. Select **Save**.

Delete a notification rule

Delete a notification rule if you no longer need it. Deleting a rule permanently removes it, so you can't recover it.

Steps

1. From the left navigation, select **Health > Alerts**.
2. Select **Notification settings**.

3. In the rules list, locate the rule you want to delete and select the action menu for that rule.
4. Select **Delete** from the action menu.

Related information

- Configure notification delivery
- Learn about Console alerts
- View alerts

Remediate storage class drift in NetApp Console local deployment

In NetApp Console local deployment, find drift-related alerts, analyze the drift findings, and remediate workloads that no longer match their storage class intent.

Required roles

Storage admin

You can only view and remediate workloads in fleets where you have permission.

Remediate drift

When a workload no longer matches its storage class intent, NetApp Console local deployment raises an alert. Use the alert to analyze the drift and apply the recommended remediation.

You can apply some remediations directly from the alert. For other issues, update the workload configuration or assign a different storage class to restore compliance. The remediation workflow shows the expected impact before you apply changes.

Steps

1. Select **Storage > Storage classes**.

   A summary of storage class drift appears in the **Drifts by storage class** area. The complete list appears in the table.

2. In the **Drifts** column, select **View** for the relevant storage class.

   The **Alerts > Overview** page opens with filters applied.

3. Select an alert to open the alert details page.
4. Select **Analyze**.
5. Review the findings in **Workload analyzer**.

   For configuration drift findings, compare the intended and actual settings to determine what changed.

6. Select the recommended remediation action, such as **Fix it**.
7. Review the proposed changes and apply the remediation.
8. Return to **Storage > Storage classes** and verify that the workload no longer appears as drifted.

Compliance evaluations can take several minutes to reflect recent configuration changes. If the workload is still listed as drifted, return to the alert details page and select **Analyze** to review any remaining findings.

Related information

- Learn about storage class drift and compliance in NetApp Console local deployment
- Learn about storage alerts
- View alerts

Alert remediation actions in NetApp Console local deployment

Use this reference to understand the remediation actions available from **Fix it** in NetApp Console local deployment. For each action, the table describes what the action does and the related alert. Review the action details in the confirmation dialog before you run it.

Remediation actions

Remediation action	Alert name	Alert description	Impact area	Remediation summary
Enable automatic volume growth	Volume full	The volume is running low on space and is nearing full capacity.	Capacity	Automatically increases a volume's size (up to a configured limit) to reduce the risk of running out of space.
Resize volume	Volume full	The volume is running low on space and is nearing full capacity.	Capacity	Increases a volume's size to provide more space immediately.
Bring volume online	Volume offline	The volume is offline and not serving data.	Availability	Brings an offline volume online so it can resume serving data.
Bring aggregate online	Aggregate offline	The aggregate is not online and volumes hosted on it may be unavailable.	Availability	Brings an offline aggregate online to restore access to the volumes it hosts.
Bring LUN online	LUN offline	The LUN is offline and host access is unavailable.	Availability	Brings an offline LUN online so hosts can resume access and I/O.
Unrestrict volume	Volume restricted	The volume is in a restricted state and may not serve I/O normally.	Availability	Returns a restricted volume to an online state so clients can access it again.
Bring NVMe namespace online	NVMe namespace is offline	The NVMe namespace is offline and host access is unavailable.	Availability	Brings an offline NVMe namespace online to restore host access.

Remediation action	Alert name	Alert description	Impact area	Remediation summary
Bring intercluster LIF up	Intercluster LIF down	An intercluster LIF is down and cluster-to-cluster communication may be impacted.	Connectivity	Brings an intercluster LIF up to restore cluster-to-cluster connectivity used for replication.
Re-enable MetroCluster AUSO	MetroCluster automatic unplanned switchover disabled	Automatic unplanned switchover is disabled on this cluster.	Availability	Re-enables automatic unplanned switchover (AUSO) so MetroCluster protection works as intended.
Configure Service Processor network	Service Processor is not configured	The Service Processor (SP) network is not configured.	Manageability	Configures the Service Processor (SP) network settings to enable out-of-band management access.
Assign unassigned disks	Unassigned disks detected	Unassigned disks are present and available capacity may be unused. Assign the disks to a node so they can be used for storage.	Availability	Assigns currently unassigned disks to a node so they can be used for storage.
Root volume space recovery	Node root volume space low	Available space on the node root volume is low and may affect normal system operation.	System health	Frees space on the node root volume by deleting the largest snapshot or the largest core dump file. Deletions are permanent.

Copyright information

Trademark information