NetApp

Alerting with Monitors

Cloud Insights

Tony Lavoie, Michael Ryan
October 19, 2021

Table of Contents

Alerting with Monitors

You create monitors to set thresholds that trigger alerts to notify you about issues related to the resources in your network. For example, you can create a monitor to alert for *node write latency* for any of a multitude of protocols.

💡   Monitors and Alerting is available in Cloud Insights Standard Edition and higher.

When the monitored threshold and conditions are reached or exceeded, Cloud Insights creates an alert. A Monitor can have a *Warning* threshold, a *Critical* threshold, or both.

Monitors allow you to set thresholds on "infrastructure" objects such as storage, VM, EC2, and ports, as well as for "integration" data such as those collected for Kubernetes, ONTAP advanced metrics, and Telegraf plugins . Monitors alert you when thresholds are crossed, and you can set thresholds for Warning-level alerts, Critical-level alerts, or both.

See below for [System-Defined Monitors](#) preview documentation.

Creating a Monitor

In the example below, we will create a Monitor to give a Warning alert when *Volume Node NFS Write Latency* reaches or exceeds 200ms, and a Critical alert when it reaches or exceeds 400ms. We only want to be alerted when either threshold is exceeded for at least 15 continuous minutes.

Requirements

- Cloud Insights must be configured to collect integration data, and that data is being collected.

Create the Monitor

1. From the Cloud Insights menu, click **Alerts > Manage Monitors**

   The Monitors list page is displayed, showing currently configured monitors.

2. To add a monitor, Click **+ Monitor**. To modify an existing monitor, click the monitor name in the list.

   The Monitor Configuration dialog is displayed.

3. In the drop-down, search for and choose an object type and metric to monitor, for example *netapp_ontap_volume_node_nfs_write_latency*.

You can set filters to narrow down which object attributes or metrics to monitor.

1 **Select a metric to monitor**

netapp_ontap.aggregate.cp_reads

Filter By   **+**

Group

Unit Displa

Search...

Metrics

cp_read_blocks

cp_reads

data_compaction_space_saved

data_compaction_space_saved_percent

size_total

When working with integration data (Kubernetes, ONTAP Advanced Data, etc.), metric filtering removes the individual/unmatched data points from the plotted data series, unlike infrastructure data (storage, VM, ports etc.) where filters work on the aggregated value of the data series and potentially remove the entire object from the chart.

> To create a multi-condition monitor (e.g., IOPS > X and latency > Y), define the first condition as a threshold and the second condition as a filter.

Define the Conditions of the Monitor.

1. After choosing the object and metric to monitor, set the Warning-level and/or Critical-level thresholds.
2. For the *Warning* level, enter 200. The dashed line indicating this Warning level displays in the example graph.
3. For the *Critical* level, enter 400. The dashed line indicating this Critical level displays in the example graph.

   The graph displays historical data. The Warning and Critical level lines on the graph are a visual representation of the Monitor, so you can easily see when the Monitor might trigger an alert in each case.

4. For the occurence interval, choose *Continuously* for a period of *15 Minutes*.

   You can choose to trigger an alert the moment a threshold is breached, or wait until the threshold has been in continuous breach for a period of time. In our example, we do not want to be alerted every time the Total IOPS peaks above the Warning or Critical level, but only when a monitored object continuously exceeds one of these levels for at least 15 minutes.

Refining the Filter

When you are filtering, as you begin typing you are presented with the option to create a **wildcard filter** based on the current text. Selecting this option will return all results that match the wildcard expression. You can also create **expressions** using NOT or OR, or you can select the "None" option to filter for null values in the field.

Filters based on wildcards or expressions (e.g. NOT, OR, "None", etc.) display in dark blue in the filter field. Items that you select directly from the list are displayed in light blue.

Note that Wildcard and Expression filtering works with text or lists but not with numerics, dates or booleans.

Setting Corrective Actions or Additional Information

You can add an optional description as well as additional insights and/or corrective actions by filling in the **Add an Alert Description** section. The description can be up to 1024 characters and will be sent with the alert. The insights/corrective action field can be up to 67,000 characters and will be displayed in the summary section of the alert landing page.

In these fields you can provide notes, links, or steps to take to correct or otherwise address the alert.

Select notification type and recipients

In the *Set up team notification(s)* section, you can choose whether to alert your team via email or Webhook.

Alerting via Email:

Specify the email recipients for alert notifications. If desired, you can choose different recipients for warning or critical alerts.

Alerting via Webhook:

Specify the webhook(s) for alert notifications. If desired, you can choose different webhooks for warning or critical alerts.

Save your Monitor

1. If desired, you can add a description of the monitor.

2. Give the Monitor a meaningful name and click **Save**.

   Your new monitor is added to the list of active Monitors.

Monitor List

The Monitor page lists the currently configured monitors, showing the following:

- Monitor Name
- Status
- Object/metric being monitored
- Conditions of the Monitor

You can view any active alerts associated with a monitor by clicking rthe "bell" icon next to the Monitor name.

You can choose to temporarily suspend monitoring of an object type by clicking the menu to the right of the monitor and selecting **Pause**. When you are ready to resume monitoring, click **Resume**.

You can copy a monitor by selecting **Duplicate** from the menu. You can then modify the new monitor and change the object/metric, filter, conditions, email recipients, etc.

If a monitor is no longer needed, you can delete it by selecting **Delete** from the menu.

Monitor Groups

Grouping allows you to view and manage related monitors. For example, you can have a monitor group dedicated to the storage in your environment, or monitors relevant to a certain recipient list.

The number of monitors contained in a group is shown next to the group name.

To create a new group, click the **"+" Create New Monitor Group** button. Enter a name for the group and click **Create Group**. An empty group is created with that name.

To add monitors to the group, go to the *All Monitors* group (recommended) and do one of the following:

- To add a single monitor, click the menu to the right of the monitor and select *Add to Group*. Choose the group to which to add the monitor.
- Click on the monitor name to open the monitor's edit view, and select a group in the *Associate to a monitor group* section.

Remove monitors by clicking on a group and selecting *Remove from Group* from the menu. You can not remove monitors from the *All Monitors* or *Custom Monitors* group. To delete a monitor from these groups, you must delete the monitor itself.

> (i) Removing a monitor from a group does not delete the monitor from Cloud Insights. To completely remove a monitor, select the monitor and click *Delete*. This also removes it from the group to which it belonged and it is no longer available to any user.

You can also move a monitor to a different group in the same manner, selecting *Move to Group*.

> (i) Each monitor can belong to only a single group at any given time.

To pause or resume all monitors in a group at once, select the menu for the group and click *Pause* or *Resume*.

Use the same menu to rename or delete a group. Deleting a group does not delete the monitors from Cloud

Insights; they are still available in *All Monitors*.

System-Defined Monitors (Preview)

Beginning in October 2021, Cloud Insights will be previewing a number of system-definied monitors for both metrics and logs. The Monitors interface will include a number of changes to accomodate these system monitors. These are described in this section.

> ℹ️   Since System-Defined monitors are a Preview feature, they are subject to change.

Create the Monitor

1. From the Cloud Insights menu, click **Alerts > Manage Monitors**

   The Monitors list page is displayed, showing currently configured monitors.

2. To modify an existing monitor, click the monitor name in the list.
3. To add a monitor, Click **+ Monitor**.

When you add a new monitor, you are prompted to create a Metric Monitor or a Log Monitor.

- *Metric* monitors alert on infrastructure- or performance-related triggers
- *Log* monitors alert on log-related activity

After you choose your monitor type, the Monitor Configuration dialog is displayed.

Metric Monitor

1. In the drop-down, search for and choose an object type and metric to monitor.

You can set filters to narrow down which object attributes or metrics to monitor.

1 Select a metric to monitor

netapp_ontap.aggregate.cp_reads

Filter By [+]

Group

Unit Displa

Search...

Metrics

cp_read_blocks

cp_reads

data_compaction_space_saved

data_compaction_space_saved_percent

size_total

When working with integration data (Kubernetes, ONTAP Advanced Data, etc.), metric filtering removes the individual/unmatched data points from the plotted data series, unlike infrastructure data (storage, VM, ports etc.) where filters work on the aggregated value of the data series and potentially remove the entire object from the chart.

> To create a multi-condition monitor (e.g., IOPS > X and latency > Y), define the first condition as a threshold and the second condition as a filter.
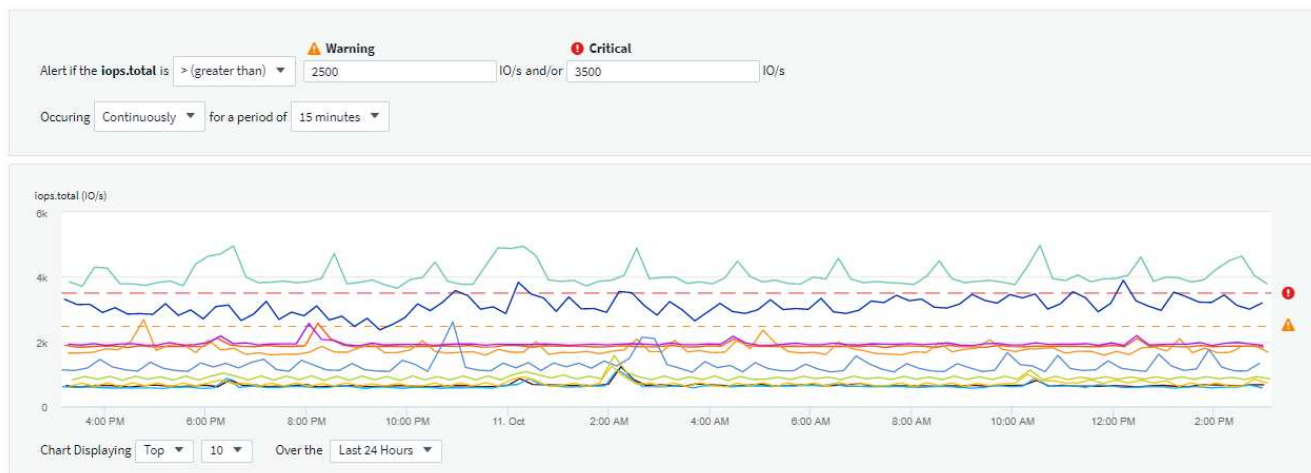
Define the Conditions of the Monitor.

1. After choosing the object and metric to monitor, set the Warning-level and/or Critical-level thresholds.

2. For the *Warning* level, enter 200 for our example. The dashed line indicating this Warning level displays in the example graph.

3. For the *Critical* level, enter 400. The dashed line indicating this Critical level displays in the example graph.

   The graph displays historical data. The Warning and Critical level lines on the graph are a visual representation of the Monitor, so you can easily see when the Monitor might trigger an alert in each case.

4. For the occurence interval, choose *Continuously* for a period of *15 Minutes*.

   You can choose to trigger an alert the moment a threshold is breached, or wait until the threshold has been in continuous breach for a period of time. In our example, we do not want to be alerted every time the Total IOPS peaks above the Warning or Critical level, but only when a monitored object continuously exceeds one of these levels for at least 15 minutes.

Log Monitor

In a **Log monitor**, first choose which log to monitor from the available log list. You can then filter based on the available attributes as above.

For example, you might choose to filter for "object.store.unavailabe" message type in the logs.netapp.ems source:

(i) The Log Monitor filter cannot be empty.

Define the alert behavior

Choose how you want to alert when a log alert is triggered. You can set the monitor to alert with *Warning*, *Critical*, or *Informational* severity, based on the filter conditions you set above.

Define the alert resolution behavior

You can choose how an log monitor alert is resolved. You are presented with three choices:

- **Resolve instantly**: The alert is immediately resolved with no further action needed
- **Resolve based on time**: The alert is resolved after the specified time has passed
- **Resolve based on log entry**: The alert is resolved when a subsequent log activity has occurred. For example, when an object is logged as "available".

- ○ Resolve instantly
- ○ Resolve based on time
- ● Resolve based on log entry

| Log Source | logs.netapp.ems ▼ |

| Filter By | ems.ems_message_type | *"object.store.available"* ✕ | ✕ ▼ | ✕ | + |

Select notification type and recipients

In the *Set up team notification(s)* section, you can choose whether to alert your team via email or Webhook.

③ **Set up team notification(s)** (alert your team via email, or Webhook)

Add Delivery Method ▼
- Email
- Webhook

Alerting via Email:

Specify the email recipients for alert notifications. If desired, you can choose different recipients for warning or critical alerts.

③ **Set up team notification(s)**

✉ **Email**

Notify team on	Add Recipients (Required)
Critical, Resolved ▼	user_1@email.com ✕ user_2@email.com ✕
☑ Critical	
☐ Warning	
☑ Resolved	

✉ **Email**

Notify team on	Add Recipients (Required)
Warning ▼	user_3@email.com ✕

Alerting via Webhook:

Specify the webhook(s) for alert notifications. If desired, you can choose different webhooks for warning or critical alerts.

By Webhook	Notify team on		Slack	Use Webhook(s)	
	Critical	▼		Slack × Teams ×	× ▼
	Notify team on			Use Webhook(s)	
	Resolved	▼		Slack × Teams ×	× ▼
	Notify team on			Use Webhook(s)	
	Warning	▼		Slack × Teams ×	× ▼

ⓘ Webhooks is considered a Preview feature and is therefore subject to change.

Setting Corrective Actions or Additional Information

You can add an optional description as well as additional insights and/or corrective actions by filling in the **Add an Alert Description** section. The description can be up to 1024 characters and will be sent with the alert. The insights/corrective action field can be up to 67,000 characters and will be displayed in the summary section of the alert landing page.

In these fields you can provide notes, links, or steps to take to correct or otherwise address the alert.

Save your Monitor

1. If desired, you can add a description of the monitor.
2. Give the Monitor a meaningful name and click **Save**.

   Your new monitor is added to the list of active Monitors.

Monitor List

The Monitor page lists the currently configured monitors, showing the following:

- Monitor Name

- Status

- Object/metric being monitored

- Conditions of the Monitor

You can choose to temporarily suspend monitoring of an object type by clicking the menu to the right of the monitor and selecting **Pause**. When you are ready to resume monitoring, click **Resume**.

You can copy a monitor by selecting **Duplicate** from the menu. You can then modify the new monitor and change the object/metric, filter, conditions, email recipients, etc.

If a monitor is no longer needed, you can delete it by selecting **Delete** from the menu.

Monitor Groups

Grouping allows you to view and manage related monitors. For example, you can have a monitor group dedicated to the storage in your environment, or monitors relevant to a certain recipient list.
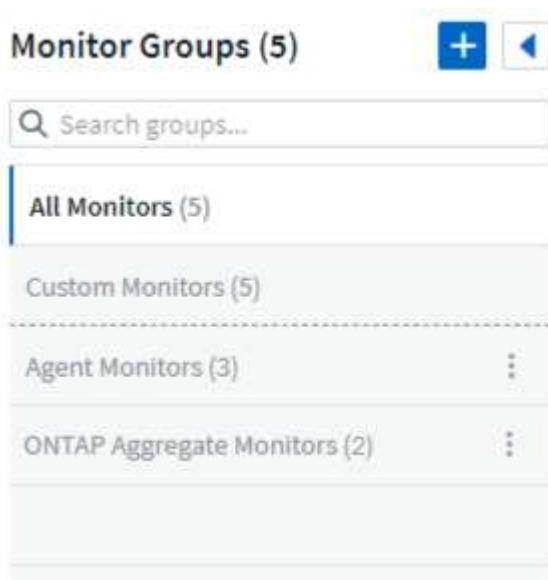
The number of monitors contained in a group is shown next to the group name.

> ⓘ Custom monitors can be paused, resumed, deleted, or moved to another group. System-defined monitors can be paused and resumed but can not be deleted or moved.

Custom Monitor Groups

To create a new custom monitor group, click the **"+" Create New Monitor Group** button. Enter a name for the group and click **Create Group**. An empty group is created with that name.

To add monitors to the group, go to the *All Monitors* group (recommended) and do one of the following:

- To add a single monitor, click the menu to the right of the monitor and select *Add to Group*. Choose the group to which to add the monitor.

- Click on the monitor name to open the monitor's edit view, and select a group in the *Associate to a monitor group* section.

5 **Associate to a monitor group** (optional)

ONTAP Monitors ▼

Remove monitors by clicking on a group and selecting *Remove from Group* from the menu. You can not remove monitors from the *All Monitors* or *Custom Monitors* group. To delete a monitor from these groups, you must delete the monitor itself.

> ⓘ Removing a monitor from a group does not delete the monitor from Cloud Insights. To completely remove a monitor, select the monitor and click *Delete*. This also removes it from the group to which it belonged and it is no longer available to any user.

You can also move a monitor to a different group in the same manner, selecting *Move to Group*.

> ⓘ Each monitor can belong to only a single group at any given time (in addition to belonging to "All Monitors" and "Custom Monitors").

To pause or resume all monitors in a group at once, select the menu for the group and click *Pause* or *Resume*.

Use the same menu to rename or delete a group. Deleting a group does not delete the monitors from Cloud Insights; they are still available in *All Monitors*.

Monitor Groups (3)   ＋ ◀

🔍 Agent Monitors   ⊗

All Monitors (4)

Custom Monitors (4)

- -

Agent Monitors (3)   ⋮

Pause

Resume

Rename

Delete

System-Defined Monitors

System-defined monitors are comprised of pre-defined metrics and conditions, as well as default descriptions and corrective actions, which can not be modified. You *can* modify the notification recipient list for system-defined monitors. To view the metrics, conditions, description and corrective actions, or to modify the recipient list, open a system-defined monitor group and click the monitor name in the list.

System-defined monitor groups cannot be modified or removed.

The following system-defined monitors are available, in the noted groups.

- **ONTAP Infrastructure** includes monitors for infrastructure-related issues in ONTAP clusters.
- **ONTAP Workload Examples** includes monitors for workload-related issues.
- Monitors in both group default to *Paused* state.

Monitor Name	Severity	Monitor Description	Corrective Action
WAFL Quota Qtree Exceeded	INFO	This event occurs when a tree quota has exceeded on a volume. This event is not repeated for this tree for a set amount of time or until a "quota resize" is performed. The amount of time is specified by the "quota logmsg" command.	Reduce the usage in this tree or increase the quota and run the "quota resize" command.
Volume Automatic Resizing Succeeded	INFO	"This event occurs when the automatic resizing of a volume is successful. It happens when the 'autosize grow' option is enabled, and the volume reaches the grow threshold percentage."	None.
Volume Automatic Resizing Failed	WARNING	The automatic resizing of the volume has failed. The volume might run out of space if you do not take corrective actions.	Analyze why automatic resize failed: Did the volume reach its maximum capacity? Is the storage pool (aggregate) out of space? Increase the maximum capacity of the volume when you automatically resize it.
SnapMirror Relationship Out of Sync	CRITICAL	This event occurs when a SnapMirror® Sync relationship status changes from 'in-sync' to 'out-of-sync'. I/O restrictions are imposed on the source volume based on the mode of replication. Client read or write access to the volume is not allowed for relationships of the 'strict-sync-mirror' policy type. Data protection is affected.	Check the network connection between the source and destination volumes. Monitor the SnapMirror Sync relationship status using the 'snapmirror show' command. 'Auto-resync' attempts to bring the relationship back to the 'in-sync' status.

SAN 'active-active' State Changed	WARNING	"The SAN pathing is no longer symmetric. Pathing should be asymmetric only on ASA, because AFF and FAS are both asymmetric."	"Try and enable the ""active-active"" state. Contact customer support if the problem persists."
QoS Monitor Memory Maxed Out	CRITICAL	The QoS subsystem's dynamic memory has reached its limit for the current platform hardware. Some QoS features might operate in a limited capacity.	"Delete some active workloads or streams to free up memory. Use the 'statistics show -object workload -counter ops' command to determine which workloads are active. Active workloads show non-zero ops. Then use the 'workload delete <workload_name>' command multiple times to remove specific workloads. Alternatively, use the 'stream delete -workload <workload name> *' command to delete the associated streams from the active workload."
NVMe Namespace Online	INFO	This event occurs when an NVMe namespace is brought online manually.	None.
NVMe Namespace Offline	INFO	This event occurs when an NVMe namespace is brought offline manually.	None.
NVMe Namespace Destroyed	INFO	This event occurs when an NVMe namespace is destroyed.	None.
Non-responsive Antivirus Server	INFO	This event occurs when ONTAP® detects a non-responsive antivirus (AV) server and forcibly closes its Vscan connection.	Ensure that the AV server installed on the AV connector can connect to the Storage Virtual Machine (SVM) and receive the scan requests.
LUN Destroyed	INFO	This event occurs when a LUN is destroyed.	None.

FC Target Port Commands Exceeded	WARNING	The number of outstanding commands on the physical FC target port exceeds the supported limit. The port does not have sufficient buffers for the outstanding commands. It is overrun or the fan-in is too steep because too many initiator I/Os are using it.	Perform the following corrective actions: "1. Evaluate the host fan-in on the port, and perform one of the following actions:" a. Reduce the number of hosts that log in to this port. b. Reduce the number of LUNs accessed by the hosts that log in to this port. c. Reduce the host command queue depth. "2. Monitor the ""queue_full"" counter on the ""fcp_port"" CM object, and ensure that it does not increase. For example: " statistics show -object fcp_port -counter queue_full -instance port.portname -raw 3. Monitor the threshold counter and ensure that it does not increase. For example: statistics show -object fcp_port -counter threshold_full -instance port.portname -raw
LUN Offline	INFO	This event occurs when a LUN is brought offline manually.	Bring the LUN back online.
AWS Credentials Not Initialized	INFO	This event occurs when a module attempts to access Amazon Web Services (AWS) Identity and Access Management (IAM) role-based credentials from the cloud credentials thread before they are initialized.	"Wait for the cloud credentials thread, as well as the system, to complete initialization. "

Cloud Tier Unreachable	CRITICAL	A storage node cannot connect to Cloud Tier object store API. Some data will be inaccessible.	"If you use on-premises products, perform the following corrective actions: " "1. Verify that your intercluster LIF is online and functional by using the ""network interface show"" command." "2. Check the network connectivity to the object store server by using the ""ping"" command over the destination node intercluster LIF." 3. Ensure the following: a. The configuration of your object store has not changed. b. The login and connectivity information is still valid. Contact NetApp technical support if the issue persists. "If you use Cloud Volumes ONTAP, perform the following corrective actions: " 1. Ensure that the configuration of your object store has not changed. 2. Ensure that the login and connectivity information is still valid. Contact NetApp technical support if the issue persists.
FlexGroup Constituent Out of Inodes	CRITICAL	"A constituent of a FlexGroup volume has run out of inodes, which might cause a potential disruption of service. You cannot create new files on this constituent. This might lead to an overall imbalanced distribution of content across the FlexGroup volume."	"It is recommended that you add capacity to the FlexGroup volume by using the ""volume modify -files +X"" command." "Alternatively, delete files from the FlexGroup volume. However, it is difficult to determine which files have landed on the constituent."

FlexGroup Constituent Nearly Out of Inodes	WARNING	"A constituent within a FlexGroup volume is almost out of inodes, which might cause a potential disruption of service. The constituent receives lesser create requests than average. This might impact the overall performance of the FlexGroup volume, because the requests are routed to constituents with more inodes."	"It is recommended that you add capacity to the FlexGroup volume by using the ""volume modify -files +X"" command." "Alternatively, delete files from the FlexGroup volume. However, it is difficult to determine which files have landed on the constituent."
FlexGroup Constituent Full	CRITICAL	"A constituent within a FlexGroup volume is full, which might cause a potential disruption of service. You can still create or expand files on the FlexGroup volume. However, none of the files that are stored on the constituent can be modified. As a result, you might see random out-of-space errors when you try to perform write operations on the FlexGroup volume."	"It is recommended that you add capacity to the FlexGroup volume by using the ""volume modify -files +X"" command." "Alternatively, delete files from the FlexGroup volume. However, it is difficult to determine which files have landed on the constituent."
Flexgroup Constituent Nearly Full	WARNING	"A constituent within a FlexGroup volume is nearly out of space, which might cause a potential disruption of service. Files can be created and expanded. However, if the constituent runs out of space, you might not be able to append to or modify the files on the constituent. "	"It is recommended that you add capacity to the FlexGroup volume by using the ""volume modify -files +X"" command." "Alternatively, delete files from the FlexGroup volume. However, it is difficult to determine which files have landed on the constituent."

Service Processor Not Configured	WARNING	"This event occurs on a weekly basis, to remind you to configure the Service Processor (SP). The SP is a physical device that is incorporated into your system to provide remote access and remote management capabilities. You should configure the SP to use its full functionality. "	Perform the following corrective actions: "1. Configure the SP by using the ""system service-processor network modify"" command." "2. Optionally, obtain the MAC address of the SP by using the ""system service-processor network show"" command." "3. Verify the SP network configuration by using the ""system service-processor network show"" command." "4. Verify that the SP can send an AutoSupport email by using the ""system service-processor autosupport invoke"" command." NOTE: AutoSupport email hosts and recipients should be configured in ONTAP before you issue this command.
Service Processor Offline	CRITICAL	"ONTAP is no longer receiving heartbeats from the Service Processor (SP), even though all the SP recovery actions have been taken. ONTAP cannot monitor the health of the hardware without the SP."	Power-cycle the system by performing the following actions: The system will shut down to prevent hardware damage and data loss. Set up a panic alert to be notified immediately if the SP goes offline. 1. Pull the controller out from the chassis. 2. Push the controller back in. 3. Turn the controller back on. "If the problem persists, replace the controller module."

Unassigned Disks	INFO	System has unassigned disks - capacity is being wasted and your system may have some misconfiguration or partial configuration change applied.	Perform the following corrective actions: "1. Determine which disks are unassigned by using the ""disk show -n"" command." "2. Assign the disks to a system by using the ""disk assign"" command."
System Cannot Operate Due to Fan Failure	CRITICAL	"One or more main unit fans have failed, disrupting system operation. This might lead to a potential data loss. "	Replace the failed fans.
Fan Failed	WARNING	One or more main unit fans have failed. The system remains operational.	"Reseat the failed fans. If the error persists, replace them." "However, if the condition persists for too long, the overtemperature might trigger an automatic shutdown."
Fan in Warning State	INFO	This event occurs when one or more fans are in a warning state.	Replace the indicated fans to avoid overheating.

NVRAM Battery Low	WARNING	The NVRAM battery capacity is critically low. There might be a potential data loss if the battery runs out of power.	Perform the following corrective actions: "Your system generates and transmits an AutoSupport or ""call home"" message to NetApp technical support and the configured destinations if it is configured to do so. The successful delivery of an AutoSupport message significantly improves problem determination and resolution." "1. View the battery's current status, capacity, and charging state by using the ""system node environment sensors show"" command." "2. If the battery was replaced recently or the system was non-operational for an extended period of time, monitor the battery to verify that it is charging properly." "3. Contact NetApp technical support if the battery runtime continues to decrease below critical levels, and the storage system shuts down automatically."
Disk Out of Service	INFO	"This event occurs when a disk is removed from service because it has been marked failed, is being sanitized, or has entered the Maintenance Center."	None.

| Storage Switch Fans Failed | CRITICAL | "The indicated cooling fan or fan module of the shelf has failed. The disks in the shelf might not receive enough cooling airflow, which might result in disk failure." | Perform the following corrective actions:
1. Verify that the fan module is fully seated and secured.
NOTE: The fan is integrated into the power supply module in some disk shelves.
"2. If the issue persists, replace the fan module."
"3. If the issue still persists, contact NetApp technical support for assistance." |

More Information

- Viewing and Dismissing Alerts