Monitors and Alerts

Cloud Insights

NetApp
March 02, 2022

Table of Contents

Monitors and Alerts

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 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**

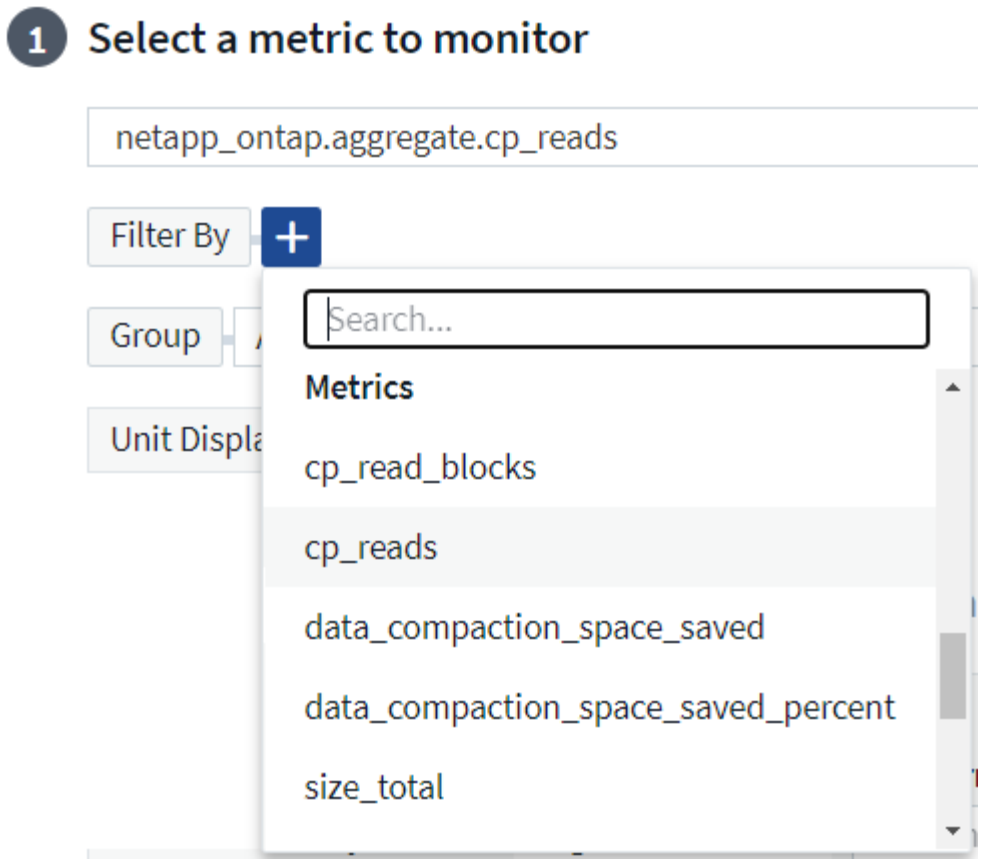
   The Monitors list page is displayed, showing currently configured monitors.

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.



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.

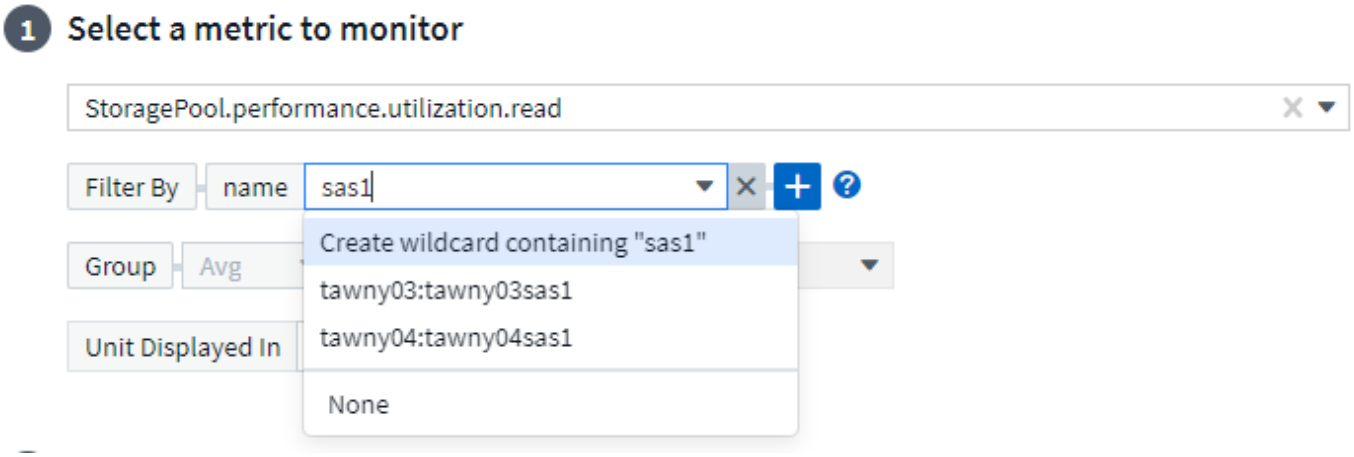
   The graph displays historical data. The Warning and Critical level lines on the graph are a visual representation of the Monitor, so you can easily see when the Monitor might trigger an alert in each case.

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

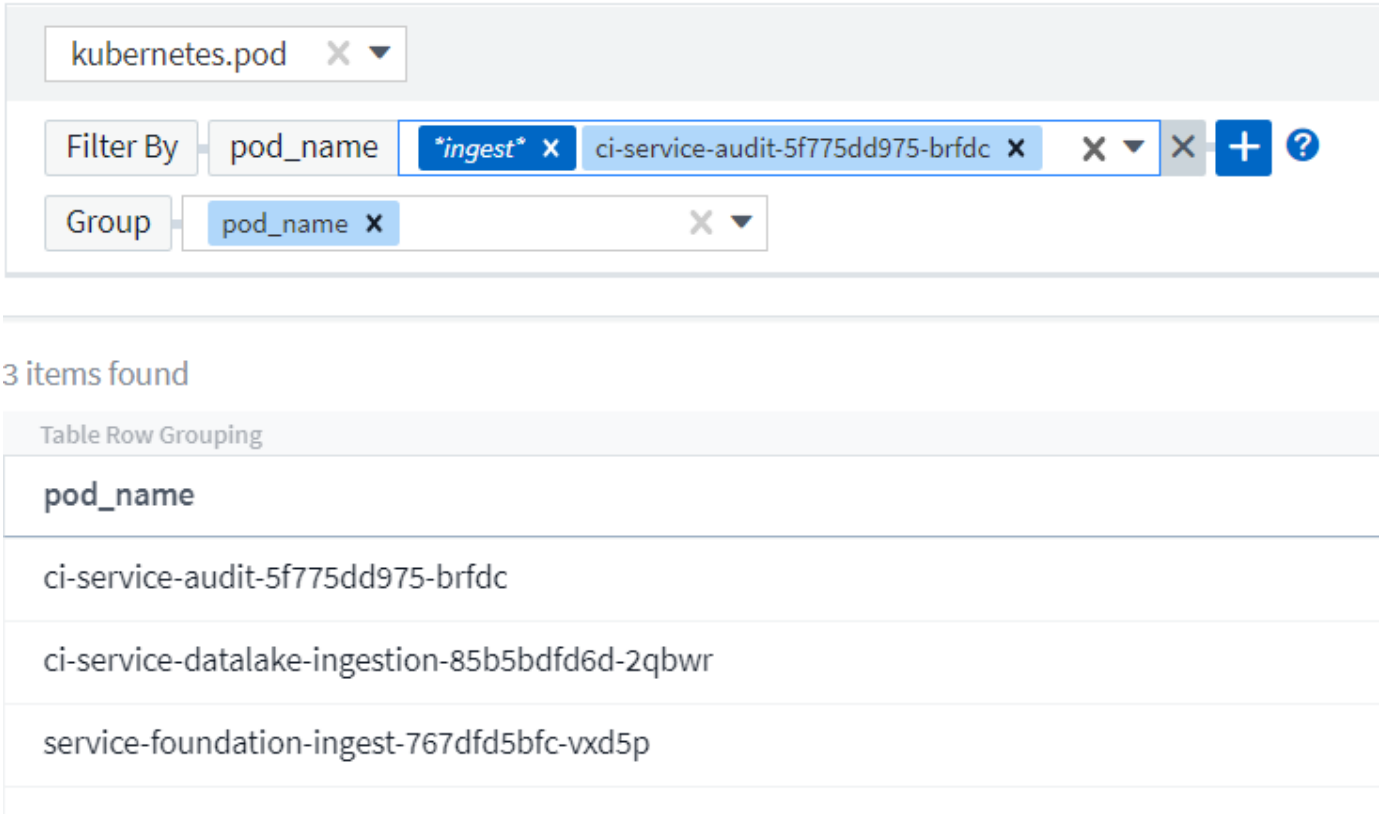
   You can choose to trigger an alert the moment a threshold is breached, or wait until the threshold has been in continuous breach for a period of time. In our example, we do not want to be alerted every time the Total IOPS peaks above the Warning or Critical level, but only when a monitored object continuously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

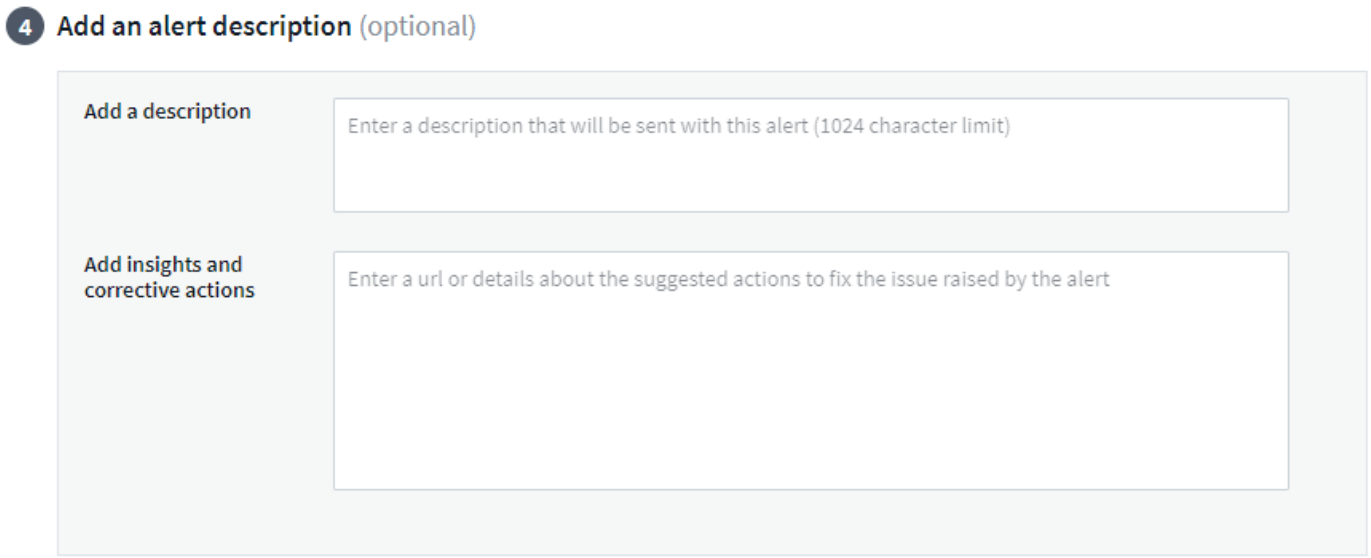


Note that Wildcard and Expression filtering works with text or lists but not with numerics, dates or booleans.

Setting Corrective Actions or Additional Information

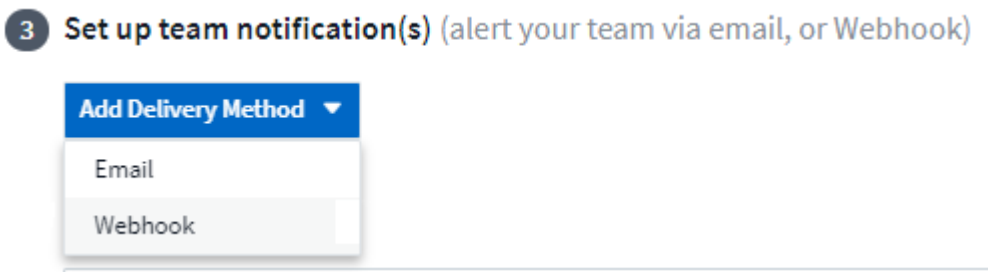
You can add an optional description as well as additional insights and/or corrective actions by filling in the **Add an Alert Description** section. The description can be up to 1024 characters and will be sent with the alert. The insights/corrective action field can be up to 67,000 characters and will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



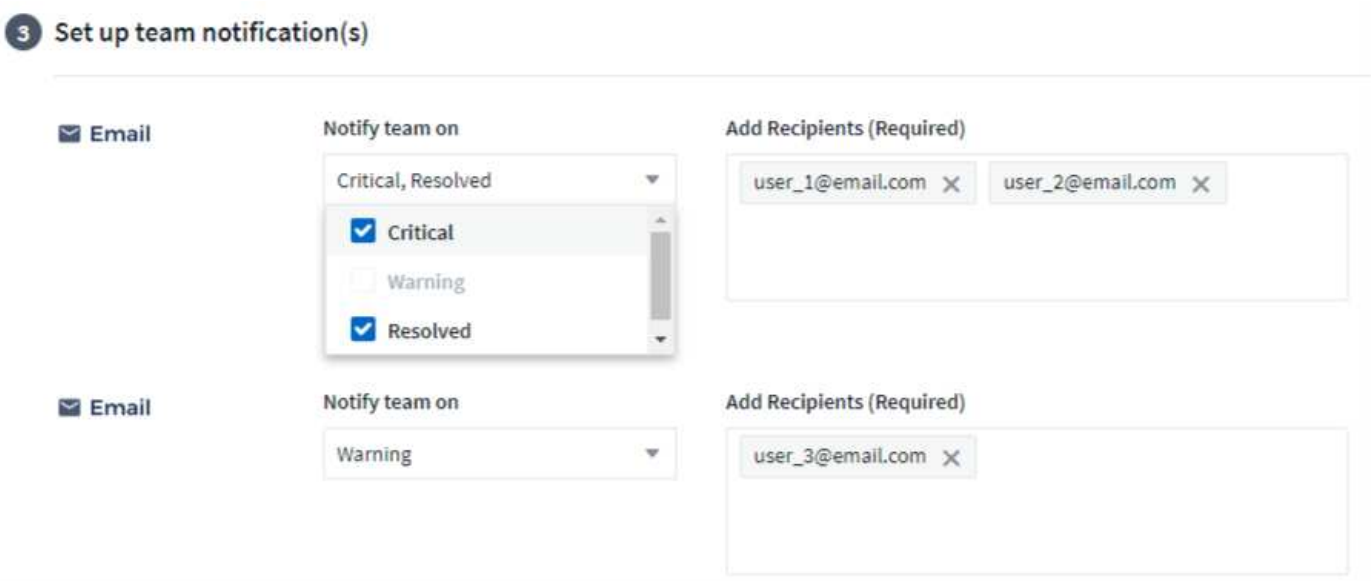
Select notification type and recipients

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



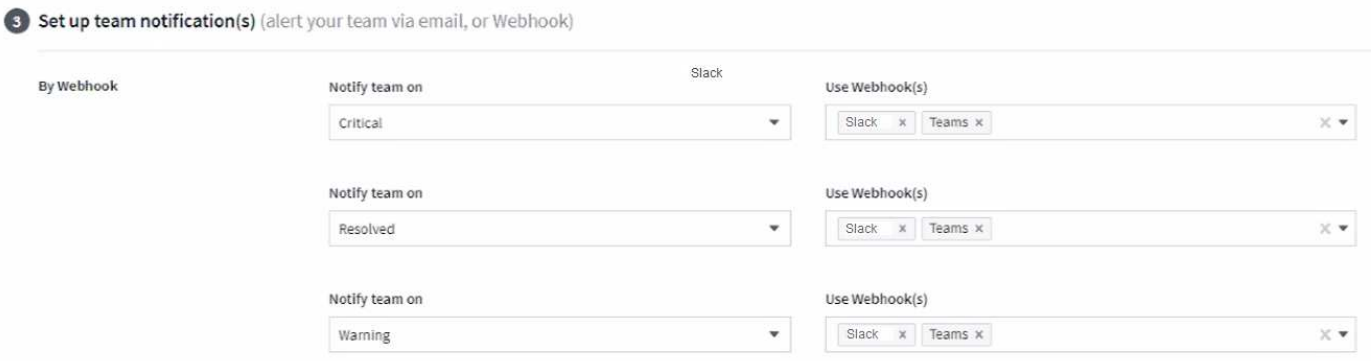
Alerting via Email:

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.



Warning vs. Critical vs. Resolved alerting

Whether a monitor sends a Warning, Critical, or Resolved alert notification depends on which threshold is crossed:

- Crossing from non-triggered to WARNING - Send Warning Alert
- Crossing from non-triggered to CRITICAL - Send Critical Alert
- Crossing from WARNING to CRITICAL - Send Critical Alert
- Crossing from CRITICAL to WARNING - Send Warning Alert
- Crossing from WARNING to Non-Triggered - Send RESOLVED Alert
- Crossing from CRITICAL to Non-Triggered - Send RESOLVED 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 view any active alerts associated with a monitor by clicking rthe "bell" icon next to the Monitor name.

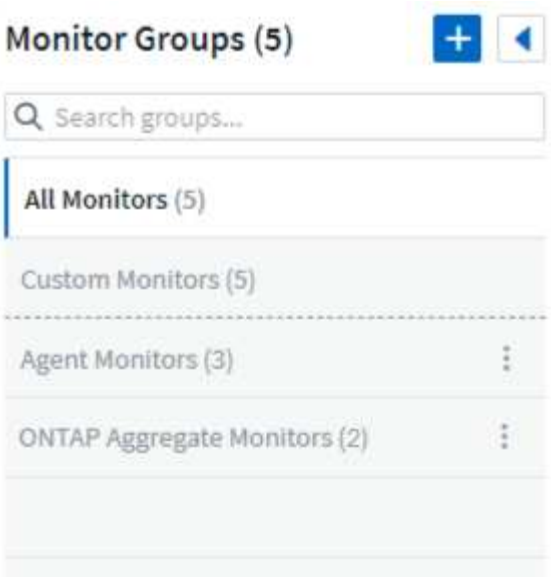
You can choose to temporarily suspend monitoring of an object type by clicking the menu to the right of the monitor and selecting **Pause**. When you are ready to resume monitoring, click **Resume**.

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.

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.

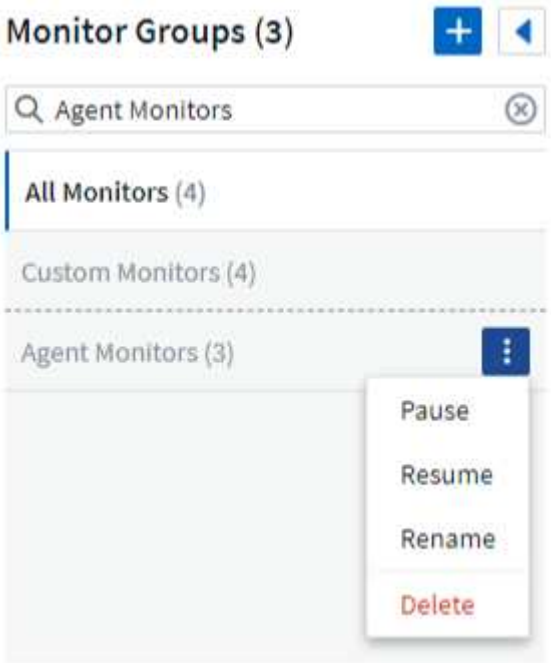
You can also move a monitor to a different group in the same manner, selecting *Move to Group*.

Each monitor can belong to only a single group at any given time.

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

Beginning in October 2021, Cloud Insights includes a number of system-defined monitors for both metrics and logs.

Read more about System-Defined Monitors, including descriptions of the monitors included with Cloud Insights.

More Information

- Viewing and Dismissing Alerts

Viewing and Managing Alerts from Monitors

Cloud Insights displays alerts when monitored thresholds are exceeded.

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

Viewing and Managing Alerts

To view and manage alerts, do the following.

1. Navigate to the **Alerts > All Alerts** page.
2. A list of up to the most recent 1,000 alerts is displayed. You can sort this list on any field by clicking the column header for the field. The list displays the following information. Note that not all of these columns are displayed by default. You can select columns to display by clicking on the "gear" icon :
   - **Alert ID**: System-generated unique alert ID
   - **Triggered Time**: The time at which the relevant Monitor triggered the alert

- **Current Severity** (Active alerts tab): The current severity of the active alert
- **Top Severity** (Resolved alerts tab); The maximum severity of the alert before it was resolved
- **Monitor**: The monitor configured to trigger the alert
- **Triggered On**: The object on which the monitored threshold was breached
- **Status**: Current alert status, *New* or *In Process*
- **Active Status**: *Active* or *Resolved*
- **Condition**: The threshold condition that triggered the alert
- **Metric**: The object's metric on which the monitored threshold was breached
- **Monitor Status**: Current status of the monitor that triggered the alert
- **Has Corrective Action**: The alert has suggested corrective actions. Open the alert page to view these.

You can manage an alert by clicking the menu to the right of the alert and choosing one of the following:

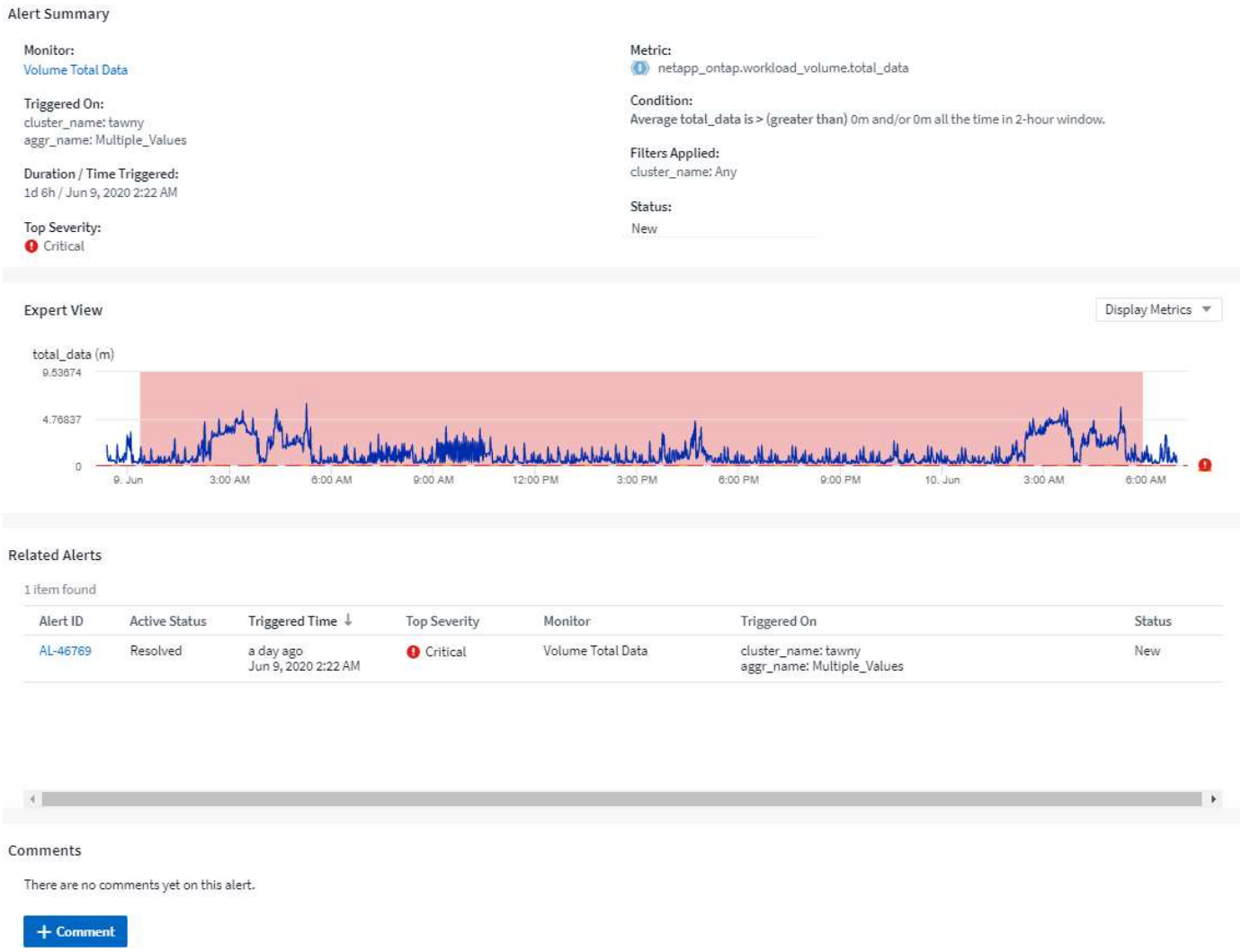
- **In Process** to indicate that the alert is under investigation or otherwise needs to be kept open
- **Dismiss** to remove the alert from the list of active alerts.

You can manage multiple alerts by selecting the checkbox to the left of each Alert and clicking *Change Selected Alerts Status*.

Clicking on an Alert ID opens the Alert Detail Page.

Alert Detail Page

The Alert Detail Page provides additional detail about the alert, including a *Summary*, an *Expert View* showing graphs related to the object's data, any *Related Assets*, and *Comments* entered by alert investigators.



"Permanently Active" Alerts

It is possible to configure a monitor in such a way for the condition to **always** exist on the monitored object—for example, IOPS > 1 or latency > 0. These are often created as 'test' monitors and then forgotten. Such monitors create alerts that stay permanently open on the constituent objects, which can cause system stress and stability issues over time.

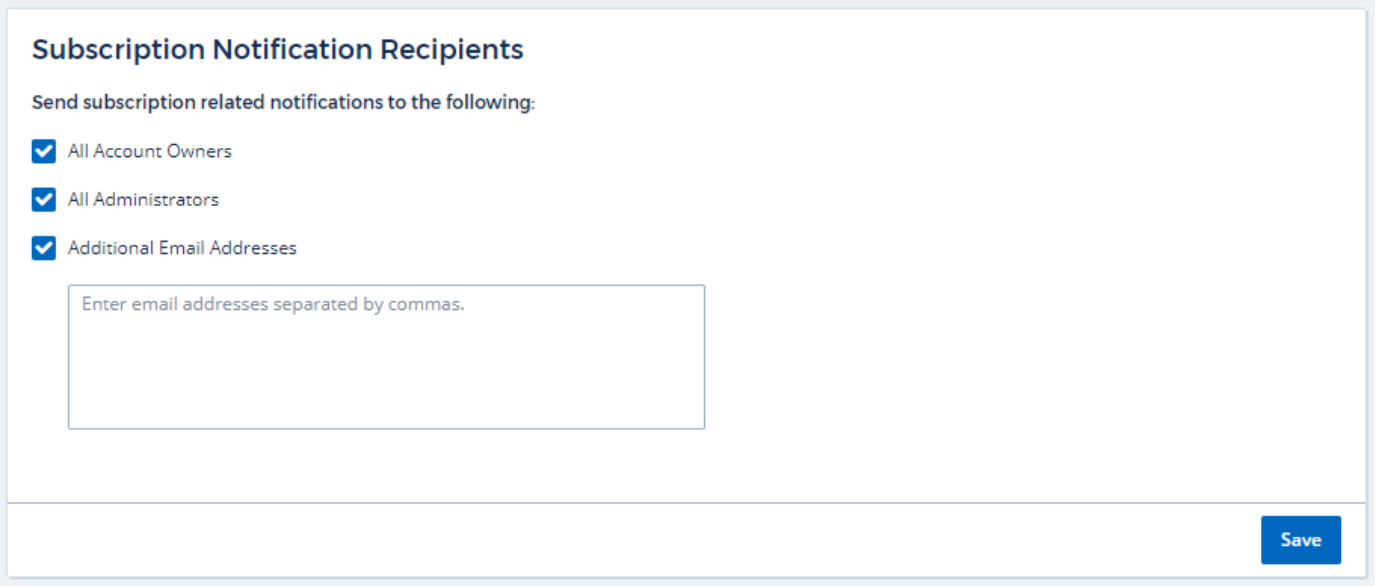
To prevent this, Cloud Insights will automatically close any "permanently active" alert after 7 days. Note that the underlying monitor conditions may (probably will) continue to exist, causing a new alert to be issued almost immediately, but this closing of "always active" alerts alleviates some of the system stress that can otherwise occur.

Configuring Email Notifications

You can configure an email list for subscription-related notifications, as well as a global email list of recipients for notification of performance policy threshold violations.

To configure notification email recipient settings, go to the **Admin > Notifications** page.

Subscription Notification Recipients



To configure recipients for subscription-related event notifications, go to the "Subscription Notification Recipients" section.
You can choose to have email notifications sent for subscription-related events to any or all of the following recipients:

- All Account Owners
- All Administrators
- Additional Email Addresses that you specify

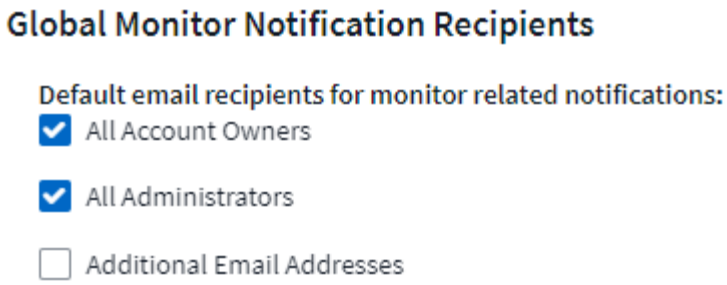
The following are examples of the types of notifications that might be sent, and user actions you can take.

Notification:	**User Action:**
Trial or subscription has been updated	Review subscription details on the Subscription page
Subscription will expire in 90 days Subscription will expire in 30 days	No action needed if “Auto Renewal” is enabled Contact NetApp sales to renew the subscription
Trial ends in 2 days	Renew trial from the Subscription page. You can renew a trial one time. Contact NetApp sales to purchase a subscription
Trial or subscription has expired Account will stop collecting data in 48 hours Account will be deleted after 48 hours	Contact NetApp sales to purchase a subscription

Global Recipient List for Alerts

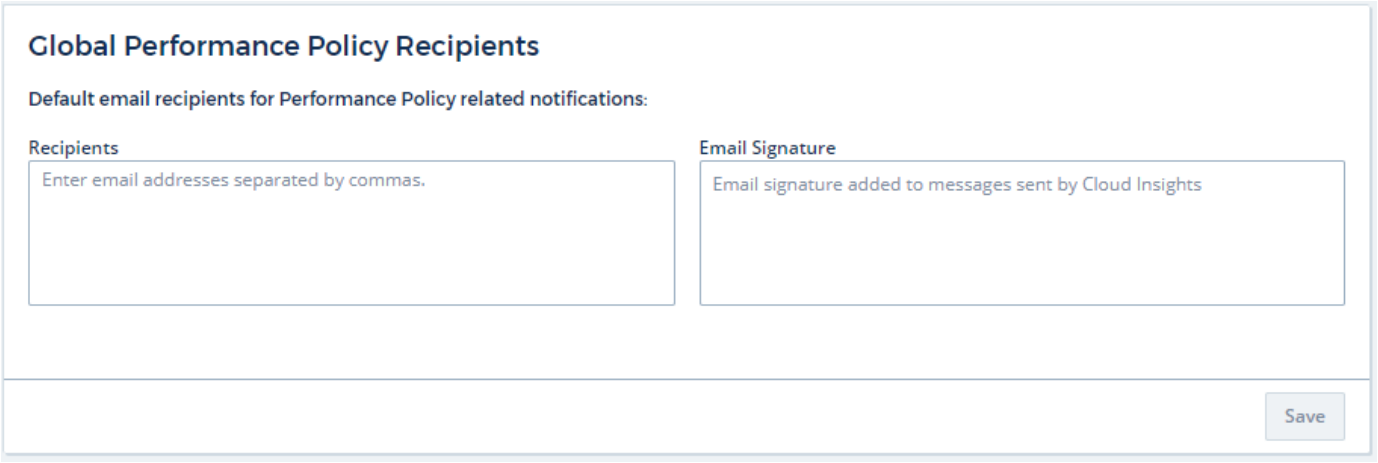
Email notifications of alerts are sent to the alert recipient list for every action on the alert. You can choose to send alert notifications to a global recipient list.

To configure global alert recipients, click on **Admin > Notifications** and choose the desired recipients in the **Global Monitor Notification Recipients** section.



You can always override the global recipients list for an individual monitor when creating or modifying the monitor.

Global Recipient List for Performance Policy Notifications



To add recipients to the global performance policy notification email list, go to the "Global Performance Policy Recipients" section and enter email addresses separated by commas. Emails sent as alerts from performance policy threshold violations will be sent to all recipients on the list.

If you make a mistake, you can click on [x] to remove a recipient from the list.

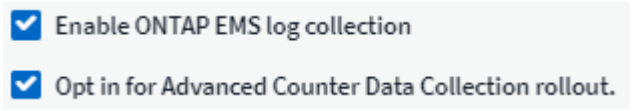
You can also add an optional signature block that will be attached to the email notifications sent.

ⓘ You can override the global list for a specific policy when you configure that policy.

System Monitors

Cloud Insights includes a number of system-defined 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.

System Monitors are in *Paused* state by default. Before resuming the monitor, you must ensure that *Advanced Counter Data Collection* and *Enable ONTAP EMS log collection* are enabled in the Data Collector. These options can be found in the ONTAP Data Collector under *Advanced Configuration*:



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.

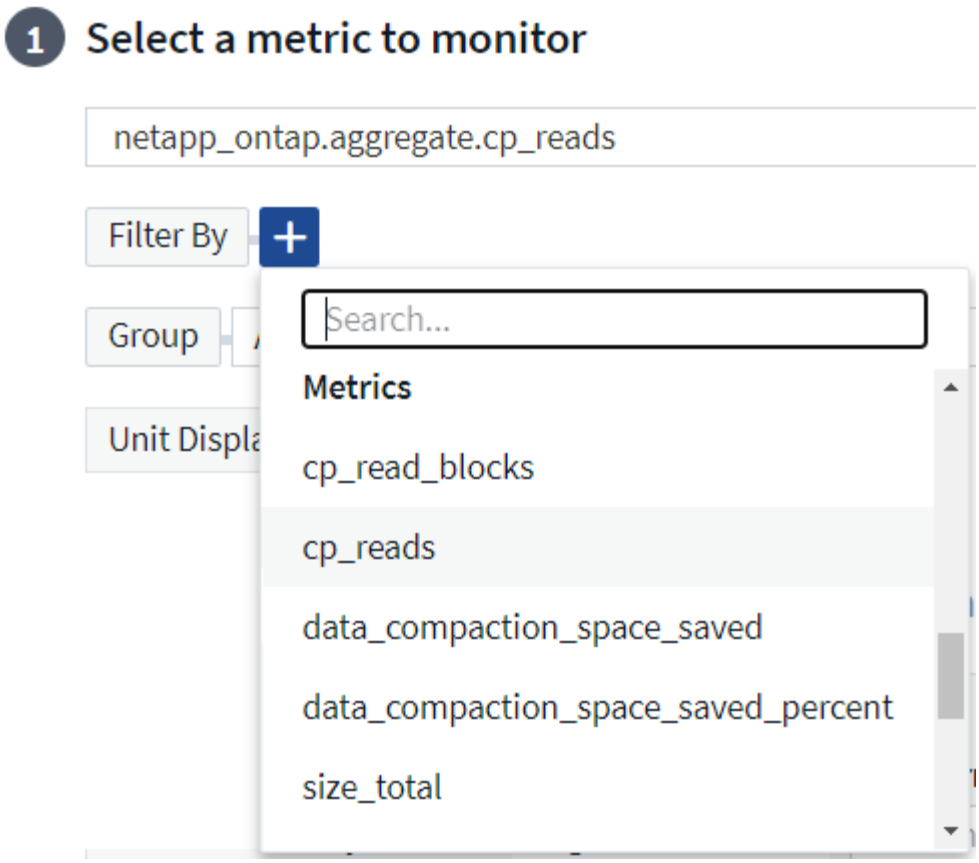
- *Metric* monitors alert on infrastructure- or performance-related triggers
- *Log* monitors alert on log-related activity

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.



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.

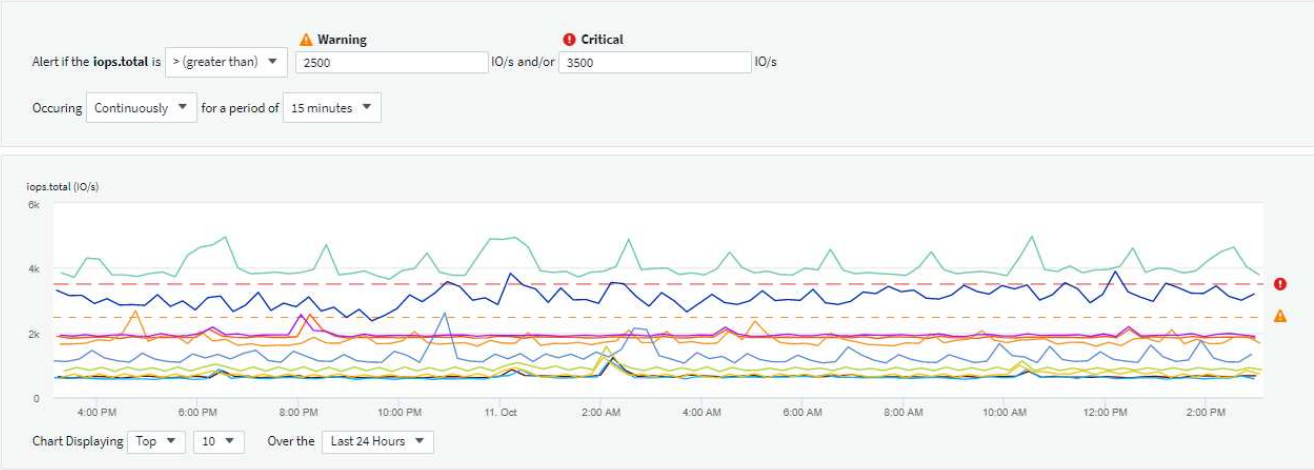
Define the Conditions of the Monitor.

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

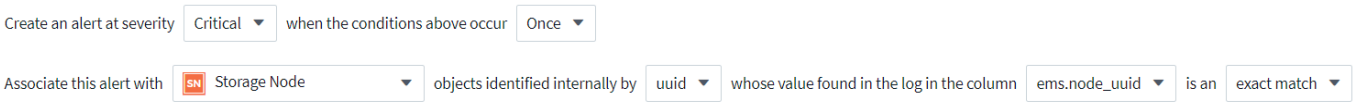
When creating a **Log monitor**, first choose which log to monitor from the available log list. You can then filter based on the available attributes as above.

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

The Log Monitor filter cannot be empty.

Define the alert behavior

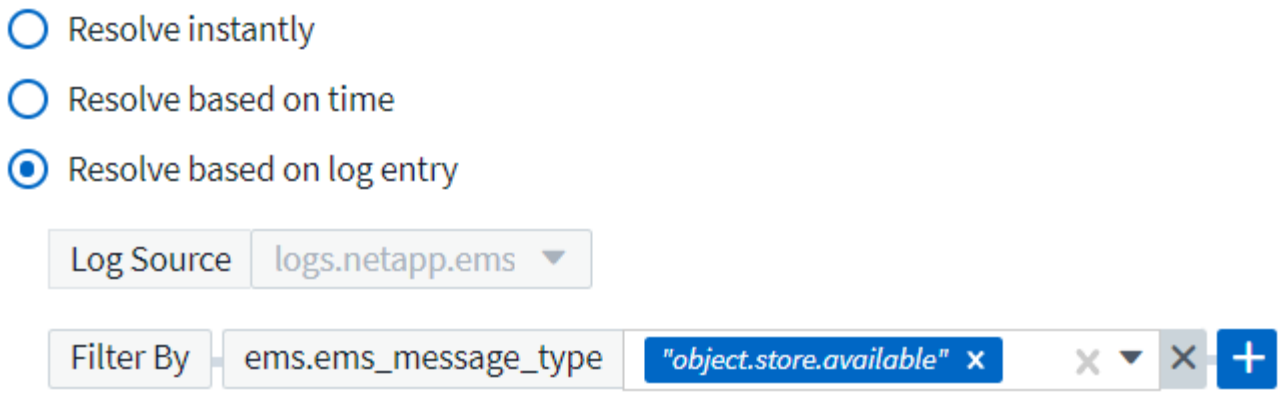
Choose how you want to alert when a log alert is triggered. You can set the monitor to alert with *Warning*, *Critical*, or *Informational* severity, based on the filter conditions you set above.



Define the alert resolution behavior

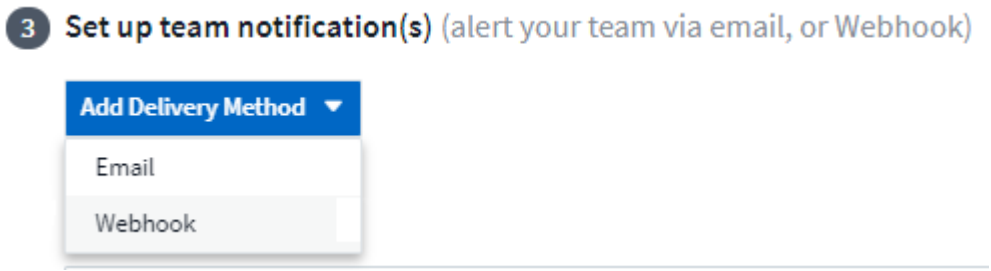
You can choose how an log monitor alert is resolved. You are presented with three choices:

- **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".



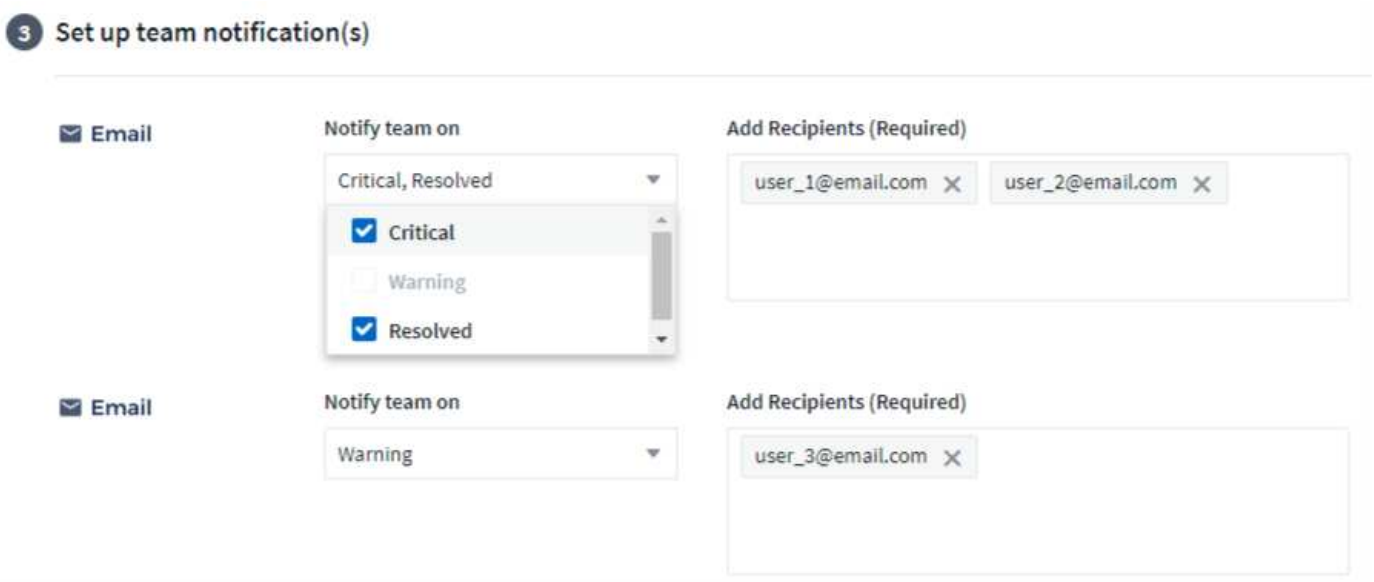
Select notification type and recipients

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



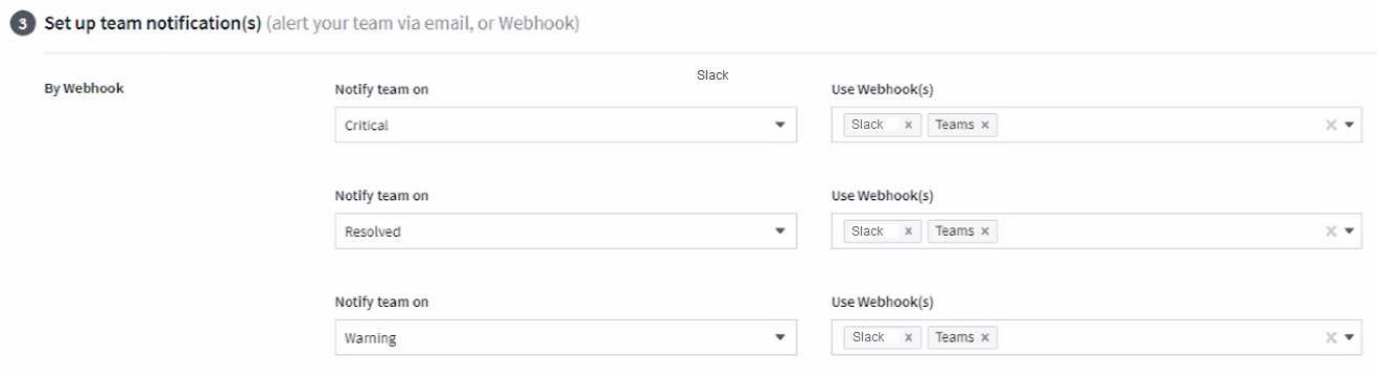
Alerting via Email:

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



Alerting via Webhook:

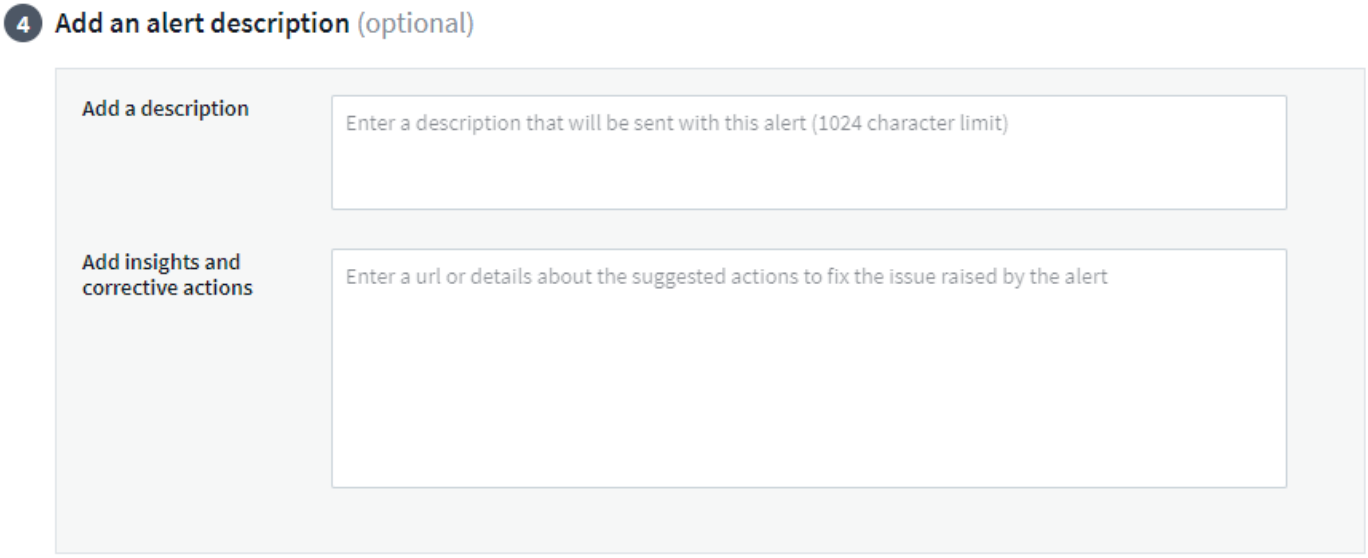
Specify the webhook(s) for alert notifications. If desired, you can choose different webhooks for warning or critical alerts.



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 pause 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.

Two groups are shown by default:

- **All Monitors** lists all monitors.
- **Custom Monitors** lists only user-created monitors.

Monitor Descriptions

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.

Below are the system monitors currently included with Cloud Insights:

Metric Monitors

Monitor Name	Severity	Description	Corrective Action

Fiber Channel Port High Utilization	CRITICAL	Fiber Channel Protocol ports are used to receive and transfer the SAN traffic between the customer host system and the ONTAP LUNs. If the port utilization is high, then it will become a bottleneck and it will ultimately affect the performance of sensitive of Fiber Channel Protocol workloads. A warning alert indicates that planned action should be taken to balance network traffic. A critical alert indicates that service disruption is imminent and emergency measures should be taken to balance network traffic to ensure service continuity.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. Move workloads to another lower utilized FCP port 2. Limit the traffic of certain LUNs to essential work only either via QoS policies in ONTAP or host-side configuration to lighten the utilization of the FCP ports… Plan to take the following actions soon if warning threshold is breached: 1. Consider configuring more FCP ports to handle the data traffic so that the port utilization gets distributed among more ports 2. Move workloads to another lower utilized FCP port 3. Limit the traffic of certain LUNs to essential work only either via QoS policies in ONTAP or host-side configuration to lighten the utilization of the FCP ports

Lun High Latency	CRITICAL	LUNs are objects that serve the IO traffic often driven by performance sensitive applications such as databases. High LUN latencies means that the applications themselves may suffer and be unable to accomplish their tasks. A warning alert indicates that planned action should be taken to move the LUN to appropriate Node or Aggregate. A critical alert indicates that service disruption is imminent and emergency measures should be taken to ensure service continuity. The following are expected latencies based on media type - SSD up to 1-2 milliseconds; SAS up to 8-10 milliseconds and SATA HDD 17-20 milliseconds	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. If the LUN or its volume has a QoS policy associated with it, evaluate its threshold limits and validate if they are causing the LUN workload to get throttled… Plan to take the following actions soon if warning threshold is breached: 1. If aggregate is also experiencing high utilization, move the LUN to another aggregate 2. If the node is also experiencing high utilization, move the volume to another node or reduce the total workload of the node 3. If the LUN or its volume has a QoS policy associated with it, evaluate its threshold limits and validate if they are causing the LUN workload to get throttled

Network Port High Utilization	CRITICAL	Network ports are used to receive and transfer the NFS, CIFS and iSCSI protocol traffic between the customer host systems and the ONTAP volumes. If the port utilization is high then it will become a bottleneck and it will ultimately affect the performance of NFS, CIFS and iSCSI workloads. A warning alert indicates that planned action should be taken to balance network traffic. A critical alert indicates that service disruption is imminent and emergency measures should be taken to balance network traffic to ensure service continuity.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. Limit the traffic of certain volumes to essential work only either via QoS policies in ONTAP or host-side analysis to lighten the utilization of the network ports 2. Configure one or more volumes to use another lower utilized network port… Plan to take the following actions soon if warning threshold is breached: 1. Consider configuring more network ports to handle the data traffic so that the port utilization gets distributed among more ports 2. Configure one or more volumes to use another lower utilized network port

NVMe Namespace High Latency	CRITICAL	NVMe Namespaces are objects that serve the IO traffic often driven by performance sensitive applications such as databases. High NVMe Namespaces latencies means that the applications themselves may suffer and be unable to accomplish their tasks. A warning alert indicates that planned action should be taken to move the LUN to appropriate Node or Aggregate. A critical alert indicates that service disruption is imminent and emergency measures should be taken to ensure service continuity.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. If the NVMe namespace or its volume has a QoS policy assigned to them, evaluate its limit thresholds in case they are causing the NVMe namespace workload to get throttled… Plan to take the following actions soon if warning threshold is breached: 1. If aggregate is also experiencing high utilization, move the LUN to another aggregate 2. If the node is also experiencing high utilization, move the volume to another node or reduce the total workload of the node 3. If the NVMe namespace or its volume has a QoS policy assigned to them, evaluate its limit thresholds in case they are causing the NVMe namespace workload to get throttled

QTree Capacity Hard Limit	CRITICAL	A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a volume. Each qtree has a space quota measured in KBytes that it can use to store data in order to control the growth of user data in volume and not exceed its total capacity. A qtree maintains a soft storage capacity quota in order to be able to alert the user proactively before reaching the total capacity quota limit in the qtree and being unable to store data anymore. Monitoring the amount of data stored within a qtree ensures that the user receives uninterrupted data service.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. Consider increasing the tree space quota in order to accommodate the growth 2. Consider instructing the user to delete unwanted data in the tree that is not needed anymore in order to free up space
QTree Capacity is Full	CRITICAL	A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a volume. Each qtree has a default space quota or a quota defined by a quota policy to limit amount of data stored in the tree within the volume capacity. A warning alert indicates that planned action should be taken to increase the space. A critical alert indicates that service disruption is imminent and emergency measures should be taken to free up space to ensure service continuity.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. Consider increasing the space of the qtree in order to accommodate the growth 2. Consider deleting data that is not needed anymore to free up space… Plan to take the following actions soon if warning threshold is breached: 1. Consider increasing the space of the qtree in order to accommodate the growth 2. Consider deleting data that is not needed anymore to free up space

QTree Capacity Soft Limit	WARNING	A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a volume. Each qtree has a space quota measured in KBytes that it can use to store data in order to control the growth of user data in volume and not exceed its total capacity. A qtree maintains a soft storage capacity quota in order to be able to alert the user proactively before reaching the total capacity quota limit in the qtree and being unable to store data anymore. Monitoring the amount of data stored within a qtree ensures that the user receives uninterrupted data service.	Plan to take the following actions soon if warning threshold is breached: 1. Consider increasing the tree space quota in order to accommodate the growth 2. Consider instructing the user to delete unwanted data in the tree that is not needed anymore in order to free up space
QTree Files Hard Limit	CRITICAL	A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a volume. Each qtree has a quota of the number of files that it can contain in order to maintain a manageable file system size within the volume. A qtree maintains a hard file number quota beyond which new files in the tree are denied. Monitoring the number of files within a qtree ensures that the user receives uninterrupted data service.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. Consider increasing the file count quota for the qtree 2. Delete files that are not used any more from the qtree file system.

QTree Files Soft Limit	WARNING	A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a volume. Each qtree has a quota of the number of files that it can contain in order to maintain a manageable file system size within the volume. A qtree maintains a soft file number quota in order to be able to alert the user proactively before reaching the limit of files in the qtree and being unable to store any additional files. Monitoring the number of files within a qtree ensures that the user receives uninterrupted data service.	Plan to take the following actions soon if warning threshold is breached: 1. Consider increasing the file count quota for the qtree 2. Delete files that are not used any more from the qtree file system
Snapshot Reserve Space is Full	CRITICAL	Storage capacity of a volume is necessary to store application and customer data. A portion of that space, called snapshot reserved space, is used to store snapshots which allow data to be protected locally. The more new and updated data stored in the ONTAP volume the more snapshot capacity is used and less snapshot storage capacity will be available for future new or updated data. If the snapshot data capacity within a volume reaches the total snapshot reserve space it may lead to the customer being unable to store new snapshot data and reduction in the level of protection for the data in the volume. Monitoring the volume used snapshot capacity ensures data services continuity.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. Consider configuring snapshots to use data space in the volume when the snapshot reserve is full 2. Consider deleting some older snapshots that may not be needed anymore to free up space… Plan to take the following actions soon if warning threshold is breached: 1. Consider increasing the snapshot reserve space within the volume to accommodate the growth 2. Consider configuring snapshots to use data space in the volume when the snapshot reserve is full

Storage Capacity Limit	CRITICAL	When a storage pool (aggregate) fills up, I/O operations slow down and finally cease causing a storage outage incident. A warning alert indicates that planned action should be taken soon to restore minimum free space. A critical alert indicates that service disruption is imminent and emergency measures should be taken to free up space to ensure service continuity.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. Delete Snapshots on non-critical volumes 2. Delete Volumes or LUNs that are non-essential workloads and that may be restored from off storage copies… Plan to take the following actions soon if warning threshold is breached: 1. Move one or more volumes to a different storage location 2. Add more storage capacity 3. Change storage efficiency settings or tier inactive data to cloud storage
Storage Performance Limit	CRITICAL	When a storage system reaches its performance limit, operations slow down, latency goes up and workloads and applications may start failing. ONTAP evaluates the storage pool utilization due to workloads and estimates what percent of performance has been consumed. A warning alert indicates that planned action should be taken to reduce storage pool load to as there may not be enough storage pool performance left to service workload peaks. A critical alert indicates that a performance brownout is imminent and emergency measures should be taken to reduce storage pool load to ensure service continuity.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. Suspend scheduled tasks such as Snapshots or SnapMirror replication 2. Idle non-essential workloads… Plan to take the following actions soon if warning threshold is breached: 1. Move one or more workloads to a different storage location 2. Add more storage nodes (AFF) or disk shelves (FAS)and redistribute workloads 3. Change workload characteristics(block size, application caching etc)

User Quota Capacity Hard Limit	CRITICAL	ONTAP recognize the users of Unix or Windows systems that have the rights to access volumes, files or directories within a volume. As a result ONTAP allows the customers to configure storage capacity for their users or groups of users of their Linux or Windows systems. The user or group policy quota limits the amount of space the user can utilize for their own data. A hard limit of this quota allows notification of the user when the amount of capacity used within the volume is right before reaching the total capacity quota. Monitoring the amount of data stored within a user or group quota ensures that the user receives uninterrupted data service.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. Consider increasing the space of the user or group quota in order to accommodate the growth 2. Consider instructing the user or group to delete data that is not needed anymore to free up space.

User Quota Capacity Soft Limit	WARNING	ONTAP recognize the users of Unix or Windows systems that have the rights to access volumes, files or directories within a volume. As a result ONTAP allows the customers to configure storage capacity for their users or groups of users of their Linux or Windows systems. The user or group policy quota limits the amount of space the user can utilize for their own data. A soft limit of this quota allows proactive notification of the user when the amount of capacity used within the volume is reaching the total capacity quota. Monitoring the amount of data stored within a user or group quota ensures that the user receives uninterrupted data service.	Plan to take the following actions soon if warning threshold is breached: 1. Consider increasing the space of the user or group quota in order to accommodate the growth 2. Consider deleting data that is not needed anymore to free up space.
Volume Capacity is Full	CRITICAL	Storage capacity of a volume is necessary to store application and customer data. The more data stored in the ONTAP volume the less storage availability for future data. If the data storage capacity within a volume reaches the total storage capacity may lead to the customer being unable to store data due to lack of storage capacity. Monitoring the volume used storage capacity ensures data services continuity.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. Consider increasing the space of the volume in order to accommodate the growth 2. Consider deleting data that is not needed anymore to free up space… Plan to take the following actions soon if warning threshold is breached: 1. Consider increasing the space of the volume in order to accommodate the growth

Volume High Latency	CRITICAL	Volumes are objects that serve the IO traffic often driven by performance sensitive applications including devOps applications, home directories, and databases. High volume latencies means that the applications themselves may suffer and be unable to accomplish their tasks. Monitoring volume latencies is critical to maintain application consistent performance. The following are expected latencies based on media type - SSD up to 1-2 milliseconds; SAS up to 8-10 milliseconds and SATA HDD 17-20 milliseconds.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. If the volume has a QoS policy assigned to it, evaluate its limit thresholds in case they are causing the volume workload to get throttled… Plan to take the following actions soon if warning threshold is breached: 1. If aggregate is also experiencing high utilization, move the volume to another aggregate. 2. If the volume has a QoS policy assigned to it, evaluate its limit thresholds in case they are causing the volume workload to get throttled. 3. If the node is also experiencing high utilization, move the volume to another node or reduce the total workload of the node

Volume Inodes Limit	CRITICAL	Volumes that store files use index nodes (inode) to store file metadata. When a volume exhausts its inode allocation no more files can be added to it. A warning alert indicates that planned action should be taken to increase the number of available inodes. A critical alert indicates that file limit exhaustion is imminent and emergency measures should be taken to free up inodes to ensure service continuity.	Immediate actions are required to minimize service disruption if critical threshold is breached: 1. Consider increasing the inodes value for the volume. If the inodes value is already at the max, then consider splitting the volume into two or more volumes because the file system has grown beyond the maximum size 2. Consider using FlexGroup as it helps to accommodate large file systems… Plan to take the following actions soon if warning threshold is breached: 1. Consider increasing the inodes value for the volume. If the inodes value is already at the max, then consider splitting the volume into two or more volumes because the file system has grown beyond the maximum size 2. Consider using FlexGroup as it helps to accommodate large file systems

Monitor Name	CI Severity	Monitor Description	Corrective Action

Node High Latency	WARNING / CRITICAL	Node latency has reached the levels where it might affect the performance of the applications on the node. Lower node latency ensures consistent performance of the applications. The expected latencies based on media type are: SSD up to 1-2 milliseconds; SAS up to 8-10 milliseconds and SATA HDD 17-20 milliseconds.	If critical threshold is breached, then immediate actions should be taken to minimize service disruption: 1. Suspend scheduled tasks, Snapshots or SnapMirror replication 2. Lower the demand of lower priority workloads via QoS limits 3. Inactivate non-essential workloads Consider immediate actions when warning threshold is breached: 1. Move one or more workloads to a different storage location 2. Lower the demand of lower priority workloads via QoS limits 3. Add more storage nodes (AFF) or disk shelves (FAS) and redistribute workloads 4. Change workload characteristics (block size, application caching etc)

Node Performance Limit	WARNING / CRITICAL	Node performance utilization has reached the levels where it might affect the performance of the IOs and the applications supported by the node. Low node performance utilization ensures consistent performance of the applications.	Immediate actions should be taken to minimize service disruption if critical threshold is breached: 1. Suspend scheduled tasks, Snapshots or SnapMirror replication 2. Lower the demand of lower priority workloads via QoS limits 3. Inactivate non-essential workloads Consider the following actions if warning threshold is breached: 1. Move one or more workloads to a different storage location 2. Lower the demand of lower priority workloads via QoS limits 3. Add more storage nodes (AFF) or disk shelves (FAS)and redistribute workloads 4. Change workload characteristics (block size, application caching etc)

Storage VM High Latency	WARNING / CRITICAL	Storage VM (SVM) latency has reached the levels where it might affect the performance of the applications on the storage VM. Lower storage VM latency ensures consistent performance of the applications. The expected latencies based on media type are: SSD up to 1-2 milliseconds; SAS up to 8-10 milliseconds and SATA HDD 17-20 milliseconds.	If critical threshold is breached, then immediately evaluate the threshold limits for volumes of the storage VM with a QoS policy assigned, to verify whether they are causing the volume workloads to get throttled Consider following immediate actions when warning threshold is breached: 1. If aggregate is also experiencing high utilization, move some volumes of the storage VM to another aggregate. 2. For volumes of the storage VM with a QoS policy assigned, evaluate the threshold limits if they are causing the volume workloads to get throttled 3. If the node is experiencing high utilization, move some volumes of the storage VM to another node or reduce the total workload of the node
User Quota Files Hard Limit	CRITICAL	The number of files created within the volume has reached the critical limit and additional files cannot be created. Monitoring the number of files stored ensures that the user receives uninterrupted data service.	Immediate actions are required to minimize service disruption if critical threshold is breached….Consider taking following actions: 1. Increase the file count quota for the specific user 2. Delete unwanted files to reduce the pressure on the files quota for the specific user

User Quota Files Soft Limit	WARNING	The number of files created within the volume has reached the threshold limit of the quota and is near to the critical limit. You cannot create additional files if quota reaches the critical limit. Monitoring the number of files stored by a user ensures that the user receives uninterrupted data service.	Consider immediate actions if warning threshold is breached: 1. Increase the file count quota for the specific user quota 2. Delete unwanted files to reduce the pressure on the files quota for the specific user
Volume Cache Miss Ratio	WARNING / CRITICAL	Volume Cache Miss Ratio is the percentage of read requests from the client applications that are returned from the disk instead of being returned from the cache. This means that the volume has reached the set threshold.	If critical threshold is breached, then immediate actions should be taken to minimize service disruption: 1. Move some workloads off of the node of the volume to reduce the IO load 2. If not already on the node of the volume, increase the WAFL cache by purchasing and adding a Flash Cache 3. Lower the demand of lower priority workloads on the same node via QoS limits Consider immediate actions when warning threshold is breached: 1. Move some workloads off of the node of the volume to reduce the IO load 2. If not already on the node of the volume, increase the WAFL cache by purchasing and adding a Flash Cache 3. Lower the demand of lower priority workloads on the same node via QoS limits 4. Change workload characteristics (block size, application caching etc)

Volume Qtree Quota Overcommit	WARNING / CRITICAL	Volume Qtree Quota Overcommit specifies the percentage at which a volume is considered to be overcommitted by the qtree quotas. The set threshold for the qtree quota is reached for the volume. Monitoring the volume qtree quota overcommit ensures that the user receives uninterrupted data service.	If critical threshold is breached, then immediate actions should be taken to minimize service disruption: 1. Increase the space of the volume 2. Delete unwanted data When warning threshold is breached, then consider increasing the space of the volume.

Log Monitors (not time-resolved)

Monitor Name	Severity	Description	Corrective Action
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: …Verify that your intercluster LIF is online and functional by using the "network interface show" command.…Check the network connectivity to the object store server by using the "ping" command over the destination node intercluster LIF.…Ensure the following:…The configuration of your object store has not changed.…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: …Ensure that the configuration of your object store has not changed.… Ensure that the login and connectivity information is still valid.…Contact NetApp technical support if the issue persists.
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.

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.
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 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.
LUN Offline	INFO	This event occurs when a LUN is brought offline manually.	Bring the LUN back online.
Main Unit Fan Failed	WARNING	One or more main unit fans have failed. The system remains operational.…However, if the condition persists for too long, the overtemperature might trigger an automatic shutdown.	Reseat the failed fans. If the error persists, replace them.
Main Unit Fan in Warning State	INFO	This event occurs when one or more main unit 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.…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.	Perform the following corrective actions:…View the battery's current status, capacity, and charging state by using the "system node environment sensors show" command.…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.…Contact NetApp technical support if the battery runtime continues to decrease below critical levels, and the storage system shuts down automatically.

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:…Configure the SP by using the "system service-processor network modify" command.…Optionally, obtain the MAC address of the SP by using the "system service-processor network show" command.…Verify the SP network configuration by using the "system service-processor network show" command.…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.…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.	Power-cycle the system by performing the following actions:…Pull the controller out from the chassis.…Push the controller back in.…Turn the controller back on.…If the problem persists, replace the controller module.

Shelf 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:…Verify that the fan module is fully seated and secured. NOTE: The fan is integrated into the power supply module in some disk shelves.…If the issue persists, replace the fan module.…If the issue still persists, contact NetApp technical support for assistance.
System Cannot Operate Due to Main Unit 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.
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:…Determine which disks are unassigned by using the "disk show -n" command.…Assign the disks to a system by using the "disk assign" command.

Log Monitors Resolved by Time

Monitor Name	Severity	Description	Corrective Action
Antivirus Server Busy	WARNING	The antivirus server is too busy to accept any new scan requests.	If this message occurs frequently, ensure that there are enough antivirus servers to handle the virus scan load generated by the SVM.

AWS Credentials for IAM Role Expired	CRITICAL	Cloud Volume ONTAP has become inaccessible. The Identity and Access Management (IAM) role-based credentials have expired. The credentials are acquired from the Amazon Web Services (AWS) metadata server using the IAM role, and are used to sign API requests to Amazon Simple Storage Service (Amazon S3).	Perform the following:…Log in to the AWS EC2 Management Console.…Navigate to the Instances page.…Find the instance for the Cloud Volumes ONTAP deployment and check its health.…Verify that the AWS IAM role associated with the instance is valid and has been granted proper privileges to the instance.
AWS Credentials for IAM Role Not Found	CRITICAL	The cloud credentials thread cannot acquire the Amazon Web Services (AWS) Identity and Access Management (IAM) role-based credentials from the AWS metadata server. The credentials are used to sign API requests to Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP has become inaccessible.…	Perform the following:…Log in to the AWS EC2 Management Console.…Navigate to the Instances page.…Find the instance for the Cloud Volumes ONTAP deployment and check its health.…Verify that the AWS IAM role associated with the instance is valid and has been granted proper privileges to the instance.
AWS Credentials for IAM Role Not Valid	CRITICAL	The Identity and Access Management (IAM) role-based credentials are not valid. The credentials are acquired from the Amazon Web Services (AWS) metadata server using the IAM role, and are used to sign API requests to Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP has become inaccessible.	Perform the following:…Log in to the AWS EC2 Management Console.…Navigate to the Instances page.…Find the instance for the Cloud Volumes ONTAP deployment and check its health.…Verify that the AWS IAM role associated with the instance is valid and has been granted proper privileges to the instance.

AWS IAM Role Not Found	CRITICAL	The Identity and Access Management (IAM) roles thread cannot find an Amazon Web Services (AWS) IAM role on the AWS metadata server. The IAM role is required to acquire role-based credentials used to sign API requests to Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP has become inaccessible.…	Perform the following:…Log in to the AWS EC2 Management Console.…Navigate to the Instances page.…Find the instance for the Cloud Volumes ONTAP deployment and check its health.…Verify that the AWS IAM role associated with the instance is valid.
AWS IAM Role Not Valid	CRITICAL	The Amazon Web Services (AWS) Identity and Access Management (IAM) role on the AWS metadata server is not valid. The Cloud Volume ONTAP has become inaccessible.…	Perform the following:…Log in to the AWS EC2 Management Console.…Navigate to the Instances page.…Find the instance for the Cloud Volumes ONTAP deployment and check its health.…Verify that the AWS IAM role associated with the instance is valid and has been granted proper privileges to the instance.
AWS Metadata Server Connection Fail	CRITICAL	The Identity and Access Management (IAM) roles thread cannot establish a communication link with the Amazon Web Services (AWS) metadata server. Communication should be established to acquire the necessary AWS IAM role-based credentials used to sign API requests to Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP has become inaccessible.…	Perform the following:…Log in to the AWS EC2 Management Console.…Navigate to the Instances page.…Find the instance for the Cloud Volumes ONTAP deployment and check its health.…

FabricPool Space Usage Limit Nearly Reached	WARNING	The total cluster-wide FabricPool space usage of object stores from capacity-licensed providers has nearly reached the licensed limit.	Perform the following corrective actions:…Check the percentage of the licensed capacity used by each FabricPool storage tier by using the "storage aggregate object-store show-space" command.…Delete Snapshot copies from volumes with the tiering policy "snapshot" or "backup" by using the "volume snapshot delete" command to clear up space.…Install a new license on the cluster to increase the licensed capacity.
FabricPool Space Usage Limit Reached	CRITICAL	The total cluster-wide FabricPool space usage of object stores from capacity-licensed providers has reached the license limit.	Perform the following corrective actions:…Check the percentage of the licensed capacity used by each FabricPool storage tier by using the "storage aggregate object-store show-space" command.…Delete Snapshot copies from volumes with the tiering policy "snapshot" or "backup" by using the "volume snapshot delete" command to clear up space.…Install a new license on the cluster to increase the licensed capacity.

Giveback of Aggregate Failed	CRITICAL	This event occurs during the migration of an aggregate as part of a storage failover (SFO) giveback, when the destination node cannot reach the object stores.	Perform the following corrective actions:…Verify that your intercluster LIF is online and functional by using the "network interface show" command.…Check network connectivity to the object store server by using the"'ping" command over the destination node intercluster LIF. …Verify that the configuration of your object store has not changed and that login and connectivity information is still accurate by using the "aggregate object-store config show" command.…Alternatively, you can override the error by specifying false for the "require-partner-waiting" parameter of the giveback command.…Contact NetApp technical support for more information or assistance.

HA Interconnect Down	WARNING	The high-availability (HA) interconnect is down. Risk of service outage when failover is not available.	Corrective actions depend on the number and type of HA interconnect links supported by the platform, as well as the reason why the interconnect is down. …If the links are down:…Verify that both controllers in the HA pair are operational.…For externally connected links, make sure that the interconnect cables are connected properly and that the small form-factor pluggables (SFPs), if applicable, are seated properly on both controllers.…For internally connected links, disable and re-enable the links, one after the other, by using the "ic link off" and "ic link on" commands. …If links are disabled, enable the links by using the "ic link on" command. …If a peer is not connected, disable and re-enable the links, one after the other, by using the "ic link off" and "ic link on" commands.…Contact NetApp technical support if the issue persists.

Max Sessions Per User Exceeded	WARNING	You have exceeded the maximum number of sessions allowed per user over a TCP connection. Any request to establish a session will be denied until some sessions are released. …	Perform the following corrective actions: …Inspect all the applications that run on the client, and terminate any that are not operating properly.…Reboot the client.…Check if the issue is caused by a new or existing application:…If the application is new, set a higher threshold for the client by using the "cifs option modify -max-opens -same-file-per-tree" command. In some cases, clients operate as expected, but require a higher threshold. You should have advanced privilege to set a higher threshold for the client. …If the issue is caused by an existing application, there might be an issue with the client. Contact NetApp technical support for more information or assistance.

Max Times Open Per File Exceeded	WARNING	You have exceeded the maximum number of times that you can open the file over a TCP connection. Any request to open this file will be denied until you close some open instances of the file. This typically indicates abnormal application behavior.…	Perform the following corrective actions:…Inspect the applications that run on the client using this TCP connection. The client might be operating incorrectly because of the application running on it.…Reboot the client.…Check if the issue is caused by a new or existing application:…If the application is new, set a higher threshold for the client by using the "cifs option modify -max-opens -same-file-per-tree" command. In some cases, clients operate as expected, but require a higher threshold. You should have advanced privilege to set a higher threshold for the client. …If the issue is caused by an existing application, there might be an issue with the client. Contact NetApp technical support for more information or assistance.

NetBIOS Name Conflict	CRITICAL	The NetBIOS Name Service has received a negative response to a name registration request, from a remote machine. This is typically caused by a conflict in the NetBIOS name or an alias. As a result, clients might not be able to access data or connect to the right data-serving node in the cluster.	Perform any one of the following corrective actions:…If there is a conflict in the NetBIOS name or an alias, perform one of the following:…Delete the duplicate NetBIOS alias by using the "vserver cifs delete -aliases alias -vserver vserver" command.…Rename a NetBIOS alias by deleting the duplicate name and adding an alias with a new name by using the "vserver cifs create -aliases alias -vserver vserver" command. …If there are no aliases configured and there is a conflict in the NetBIOS name, then rename the CIFS server by using the "vserver cifs delete -vserver vserver" and "vserver cifs create -cifs -server netbiosname" commands. NOTE: Deleting a CIFS server can make data inaccessible. …Remove NetBIOS name or rename the NetBIOS on the remote machine.
NFSv4 Store Pool Exhausted	CRITICAL	A NFSv4 store pool has been exhausted.	If the NFS server is unresponsive for more than 10 minutes after this event, contact NetApp technical support.
No Registered Scan Engine	CRITICAL	The antivirus connector notified ONTAP that it does not have a registered scan engine. This might cause data unavailability if the "scan-mandatory" option is enabled.	Perform the following corrective actions:…Ensure that the scan engine software installed on the antivirus server is compatible with ONTAP.…Ensure that scan engine software is running and configured to connect to the antivirus connector over local loopback.

No Vscan Connection	CRITICAL	ONTAP has no Vscan connection to service virus scan requests. This might cause data unavailability if the "scan-mandatory" option is enabled.	Ensure that the scanner pool is properly configured and the antivirus servers are active and connected to ONTAP.
Node Root Volume Space Low	CRITICAL	The system has detected that the root volume is dangerously low on space. The node is not fully operational. Data LIFs might have failed over within the cluster, because of which NFS and CIFS access is limited on the node. Administrative capability is limited to local recovery procedures for the node to clear up space on the root volume.	Perform the following corrective actions:…Clear up space on the root volume by deleting old Snapshot copies, deleting files you no longer need from the /mroot directory, or expanding the root volume capacity.…Reboot the controller.…Contact NetApp technical support for more information or assistance.
Nonexistent Admin Share	CRITICAL	Vscan issue: a client has attempted to connect to a nonexistent ONTAP_ADMIN$ share.	Ensure that Vscan is enabled for the mentioned SVM ID. Enabling Vscan on a SVM causes the ONTAP_ADMIN$ share to be created for the SVM automatically.
NVMe Namespace Out of Space	CRITICAL	An NVMe namespace has been brought offline because of a write failure caused by lack of space.	Add space to the volume, and then bring the NVMe namespace online by using the "vserver nvme namespace modify" command.
NVMe-oF Grace Period Active	WARNING	This event occurs on a daily basis when the NVMe over Fabrics (NVMe-oF) protocol is in use and the grace period of the license is active. The NVMe-oF functionality requires a license after the license grace period expires. NVMe-oF functionality is disabled when the license grace period is over.	Contact your sales representative to obtain an NVMe-oF license, and add it to the cluster, or remove all instances of NVMe-oF configuration from the cluster.

NVMe-oF Grace Period Expired	WARNING	The NVMe over Fabrics (NVMe-oF) license grace period is over and the NVMe-oF functionality is disabled.	Contact your sales representative to obtain an NVMe-oF license, and add it to the cluster.
NVMe-oF Grace Period Start	WARNING	The NVMe over Fabrics (NVMe-oF) configuration was detected during the upgrade to ONTAP 9.5 software. NVMe-oF functionality requires a license after the license grace period expires.	Contact your sales representative to obtain an NVMe-oF license, and add it to the cluster.
Object Store Host Unresolvable	CRITICAL	The object store server host name cannot be resolved to an IP address. The object store client cannot communicate with the object-store server without resolving to an IP address. As a result, data might be inaccessible.	Check the DNS configuration to verify that the host name is configured correctly with an IP address.
Object Store Intercluster LIF Down	CRITICAL	The object-store client cannot find an operational LIF to communicate with the object store server. The node will not allow object store client traffic until the intercluster LIF is operational. As a result, data might be inaccessible.	Perform the following corrective actions:…Check the intercluster LIF status by using the "network interface show -role intercluster" command.…Verify that the intercluster LIF is configured correctly and operational.…If an intercluster LIF is not configured, add it by using the "network interface create -role intercluster" command.
Object Store Signature Mismatch	CRITICAL	The request signature sent to the object store server does not match the signature calculated by the client. As a result, data might be inaccessible.	Verify that the secret access key is configured correctly. If it is configured correctly, contact NetApp technical support for assistance.

READDIR Timeout	CRITICAL	A READDIR file operation has exceeded the timeout that it is allowed to run in WAFL. This can be because of very large or sparse directories. Corrective action is recommended.	Perform the following corrective actions:…Find information specific to recent directories that have had READDIR file operations expire by using the following 'diag' privilege nodeshell CLI command: wafl readdir notice show.…Check if directories are indicated as sparse or not:…If a directory is indicated as sparse, it is recommended that you copy the contents of the directory to a new directory to remove the sparseness of the directory file. …If a directory is not indicated as sparse and the directory is large, it is recommended that you reduce the size of the directory file by reducing the number of file entries in the directory.

Relocation of Aggregate Failed	CRITICAL	This event occurs during the relocation of an aggregate, when the destination node cannot reach the object stores.	Perform the following corrective actions:…Verify that your intercluster LIF is online and functional by using the "network interface show" command.…Check network connectivity to the object store server by using the"'ping" command over the destination node intercluster LIF. …Verify that the configuration of your object store has not changed and that login and connectivity information is still accurate by using the "aggregate object-store config show" command.…Alternatively, you can override the error by using the "override-destination-checks" parameter of the relocation command.…Contact NetApp technical support for more information or assistance.
Shadow Copy Failed	CRITICAL	A Volume Shadow Copy Service (VSS), a Microsoft Server backup and restore service operation, has failed.	Check the following using the information provided in the event message:…Is shadow copy configuration enabled?…Are the appropriate licenses installed? …On which shares is the shadow copy operation performed?…Is the share name correct?…Does the share path exist?…What are the states of the shadow copy set and its shadow copies?

Storage Switch Power Supplies Failed	WARNING	There is a missing power supply in the cluster switch. Redundancy is reduced, risk of outage with any further power failures.	Perform the following corrective actions:…Ensure that the power supply mains, which supplies power to the cluster switch, is turned on.…Ensure that the power cord is connected to the power supply.…Contact NetApp technical support if the issue persists.
Too Many CIFS Authentication	WARNING	Many authentication negotiations have occurred simultaneously. There are 256 incomplete new session requests from this client.	Investigate why the client has created 256 or more new connection requests. You might have to contact the vendor of the client or of the application to determine why the error occurred.
Unauthorized User Access to Admin Share	WARNING	A client has attempted to connect to the privileged ONTAP_ADMIN$ share even though their logged-in user is not an allowed user.	Perform the following corrective actions:…Ensure that the mentioned username and IP address is configured in one of the active Vscan scanner pools.…Check the scanner pool configuration that is currently active by using the "vserver vscan scanner pool show-active" command.
Virus Detected	WARNING	A Vscan server has reported an error to the storage system. This typically indicates that a virus has been found. However, other errors on the Vscan server can cause this event.…Client access to the file is denied. The Vscan server might, depending on its settings and configuration, clean the file, quarantine it, or delete it.	Check the log of the Vscan server reported in the "syslog" event to see if it was able to successfully clean, quarantine, or delete the infected file. If it was not able to do so, a system administrator might have to manually delete the file.

Anti-Ransomware Log Monitors

Monitor Name	Severity	Description	Corrective Action

Storage VM Anti-ransomware Monitoring Disabled	WARNING	The anti-ransomware monitoring for the storage VM is disabled. Enable anti-ransomware to protect the storage VM.	None
Storage VM Anti-ransomware Monitoring Enabled (Learning Mode)	INFO	The anti-ransomware monitoring for the storage VM is enabled in learning mode.	None
Volume Anti-ransomware Monitoring Enabled	INFO	The anti-ransomware monitoring for the volume is enabled.	None
Volume Anti-ransomware Monitoring Disabled	WARNING	The anti-ransomware monitoring for the volume is disabled. Enable anti-ransomware to protect the volume.	None
Volume Anti-ransomware Monitoring Enabled (Learning Mode)	INFO	The anti-ransomware monitoring for the volume is enabled in learning mode.	None
Volume Anti-ransomware Monitoring Paused (Learning Mode)	WARNING	The anti-ransomware monitoring for the volume is paused in learning mode.	None
Volume Anti-ransomware Monitoring Paused	WARNING	The anti-ransomware monitoring for the volume is paused.	None
Volume Anti-ransomware Monitoring Disabling	WARNING	The anti-ransomware monitoring for the volume is disabling.	None
Ransomware Activity Detected	CRITICAL	To protect the data from the detected ransomware, a Snapshot copy has been taken that can be used to restore original data. Your system generates and transmits an AutoSupport or "call home" message to NetApp technical support and any configured destinations. AutoSupport message improves problem determination and resolution.	Refer to the "FINAL-DOCUMENT-NAME" to take remedial measures for ransomware activity.

Astra Data Store (ADS) Monitors

Monitor Name	CI Severity	Monitor Description	Corrective Action
Cluster Capacity Full	Warning @ > 85 % Critical @ > 95 %	The Storage capacity of an ADS cluster is used to store application and customer data. The more data stored in the cluster the less storage availability for future data.…When the storage capacity within a cluster reaches the total cluster capacity, the cluster will be unable to store more data. Monitoring the cluster physical capacity ensures data services continuity.	Immediate actions are required to minimize service disruption if critical threshold is breached:…1. Consider increasing the space allocated to the cluster in order to accommodate the growth…2. Consider deleting data that is not needed anymore to free up space…Plan to take the following actions soon if warning threshold is breached:…1. Consider increasing the space allocated to the cluster in order to accommodate the growth.
Volume Capacity Full	Warning @ < 15% Critical @ < 5 %	The Storage capacity for a volume is used to store application and customer data. The more data stored on the cluster volume the less storage availability for future data.…When the data storage capacity used within a volume reaches the total storage capacity, the volume will be unable to store more data due to lack of available storage capacity.…Monitoring the volume used storage capacity ensures data services continuity.	Immediate actions are required to minimize service disruption if critical threshold is breached:…1. Consider increasing the space of the volume in order to accommodate the growth…2. Consider deleting data that is not needed anymore to free up space…Plan to take the following actions soon if warning threshold is breached:…1. Consider increasing the space of the volume in order to accommodate the growth.

More Information

- Viewing and Dismissing Alerts