



Monitors and Alerts

Cloud Insights

NetApp
April 18, 2022

Table of Contents

- Monitors and Alerts 1
 - Alerting with Monitors 1
 - Viewing and Managing Alerts from Monitors 8
 - Configuring Email Notifications 10
 - System Monitors 12

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.

Monitors allow you to set thresholds on metrics generated by "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. These *metric* monitors alert you when warning-level or critical-level thresholds are crossed.

You can also create monitors to trigger warning-, critical-, or informational-level alerts when specified *log events* are detected.

Cloud Insights provides a number of [System-Defined Monitors](#) as well, based on your environment.

Metric or Log 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. Configuration varies depending on which type of monitor you are creating.

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



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 occurrence 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.

Create an alert at severity Critical when the conditions above occur Once

Associate this alert with Storage Node objects identified internally by uuid whose value found in the log in the column ems.node_uuid is an exact match

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" x x ▼ x +

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

Critical, Resolved ▼

☒ Critical

☐ Warning

☒ Resolved

Add Recipients (Required)

user_1@email.com x

user_2@email.com x

Email

Notify team on

Warning ▼

Add Recipients (Required)

user_3@email.com x

Alerting via Webhook:

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

critical alerts.

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

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

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.

4 Add an alert description (optional)

Add a description	<div>Enter a description that will be sent with this alert (1024 character limit)</div>
Add insights and corrective actions	<div>Enter a url or details about the suggested actions to fix the issue raised by the alert</div>

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.

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 following monitor groups are shown. The number of monitors contained in a group is shown next to the group name.

- **All Monitors** lists all monitors.
- **Custom Monitors** lists all user-created monitors.
- **Suspended Monitors** will list any system monitors that have been suspended by Cloud Insights.
- Cloud Insights will also show a number of **System Monitor Groups**, which will list one or more groups of [system-defined monitors](#), including ONTAP Infrastructure and Workload monitors.



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.

Suspended Monitors

This group will only be shown if Cloud Insights has suspended one or more monitors. A monitor may be suspended if it is generating excessive or continuous alerts. If the monitor is a custom monitor, modify the conditions to prevent the continuous alerting, and then resume the monitor. The monitor will be removed from

the Suspended Monitors group when the issue causing the suspension is resolved.

System-Defined Monitors

These groups will show monitors provided by Cloud Insights, as long as your environment contains the devices and/or log availability required by the monitors.

System-Defined monitors cannot be modified, moved to another group, or deleted. However, you can duplicate a system monitor and modify or move the duplicate.

System monitors may include monitors for ONTAP Infrastructure (storage, volume, etc.) or Workloads (i.e. log monitors), or other groups. NetApp is constantly evaluating customer need and product functionality, and will update or add to system monitors and groups as needed.

Custom Monitor Groups

You can create your own groups to contain monitors based on your needs. For example, you may want a group for all of your storage-related monitors.

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)

A screenshot of a web interface showing a dropdown menu. The dropdown is open, displaying the text 'ONTAP Monitors' with a small downward arrow on the right side of the menu box.

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*.

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*.



Two groups are shown by default:

- **All Monitors** lists all monitors.
- **Custom Monitors** lists only user-created monitors.
- **Suspended Monitors** will be shown only if a monitor has been suspended by the system.

System-Defined Monitors

Cloud Insights includes a number of system-defined monitors for both metrics and logs. The system monitors available are dependent on the data collectors present in your environment. Because of that, the monitors available in Cloud Insights may change as data collectors are added or their configurations changed.

View the [System-Defined Monitors](#) page for descriptions of 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.

Alert Summary

Monitor:

Volume Total Data

Triggered On:

cluster_name: tawny
aggr_name: Multiple_Values

Duration / Time Triggered:

1d 6h / Jun 9, 2020 2:22 AM

Top Severity:

❗ Critical

Metric:

① netapp_ontap.workload_volume.total_data

Condition:

Average total_data is > (greater than) 0m and/or 0m all the time in 2-hour window.

Filters Applied:

cluster_name: Any

Status:

New

Expert View

Display Metrics ▾



Related Alerts

1 item found

Alert ID	Active Status	Triggered Time ↓	Top Severity	Monitor	Triggered On	Status
AL-46769	Resolved	a day ago Jun 9, 2020 2:22 AM	❗ Critical	Volume Total Data	cluster_name: tawny aggr_name: Multiple_Values	New

Comments

There are no comments yet on this alert.

[+ Comment](#)

"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

Subscription Notification Recipients

Send subscription related notifications to the following:

☒ All Account Owners

☒ All Administrators

☒ Additional Email Addresses

Enter email addresses separated by commas.

Save

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.

Global Monitor Notification Recipients

Default email recipients for monitor related notifications:

- ☒ All Account Owners
- ☒ All Administrators
- ☐ Additional Email Addresses

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

Global Performance Policy Recipients

Default email recipients for Performance Policy related notifications:

Recipients	Email Signature
<div>Enter email addresses separated by commas.</div>	<div>Email signature added to messages sent by Cloud Insights</div>

Save

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 system monitors available are dependent on the data collectors present in your environment. Because of that, the monitors available in Cloud Insights may change as data collectors are added or their configurations changed.



Most 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*:

- ☒ Enable ONTAP EMS log collection
- ☒ Opt in for Advanced Counter Data Collection rollout.

Two groups are shown by default:

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

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 *Move to Group*. Choose the group to which to add the monitor.
- To add multiple monitors, select the ones you want to move, and click *Bulk Actions*. Choose *Move to group*. You cannot move system-defined monitors.
- 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, or from any of the system-defined monitor groups. 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 any 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*. You cannot move monitors from the system-defined monitor groups; to move a monitor from one of these groups, you must first *Duplicate* the monitor, and then move the duplicated monitor to the desired group.

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*. You cannot delete system-defined monitor groups.

