



# **Monitors and Alerts**

## **Cloud Insights**

NetApp  
November 30, 2021

# Table of Contents

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

# 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](#) preview documentation.

### Creating a Monitor

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

#### Requirements

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

#### Create the Monitor

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

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

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

The Monitor Configuration dialog is displayed.

3. In the drop-down, search for and choose an object type and metric to monitor, for example *netapp\_ontap\_volume\_node\_nfs\_write\_latency*.

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

## 1 Select a metric to monitor



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 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.

## 2 Define the monitor's conditions (set at least one threshold condition)



### 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.

## 1 Select a metric to monitor

The screenshot shows the filter configuration interface. The metric being monitored is `StoragePool.performance.utilization.read`. The filter is set to `name` with the value `sas1`. A dropdown menu is open, showing the option `Create wildcard containing "sas1"` (highlighted in light blue), followed by `tawny03:tawny03sas1` and `tawny04:tawny04sas1`. The `Unit Displayed In` is set to `Avg`. The `Unit Displayed In` dropdown is also open, showing the option `None`.

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.

kubernetes.pod

Filter By
pod\_name
\*ingest\*
ci-service-audit-5f775dd975-brfdc
+
?

Group
pod\_name

3 items found

pod_name
ci-service-audit-5f775dd975-brfdc
ci-service-datalake-ingestion-85b5bdfd6d-2qbwr
service-foundation-ingest-767dfd5bfc-vxd5p

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.

#### 4 Add an alert description (optional)

Add a description

Enter a description that will be sent with this alert (1024 character limit)

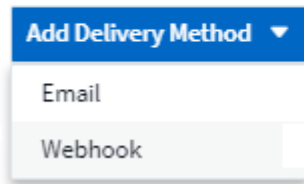
Add insights and corrective actions

Enter a url or details about the suggested actions to fix the issue raised by 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.

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



A dropdown menu titled "Add Delivery Method" with a blue header. The menu is open, showing two options: "Email" and "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)



The form shows two sections for email notifications. Each section has a "Notify team on" dropdown and an "Add Recipients (Required)" input field.

**Section 1:**

- Notify team on:** A dropdown menu with "Critical, Resolved" selected. Below it, a list of options: ☒ Critical, ☐ Warning, and ☒ Resolved.
- Add Recipients (Required):** Two email addresses are listed: user\_1@email.com and user\_2@email.com.

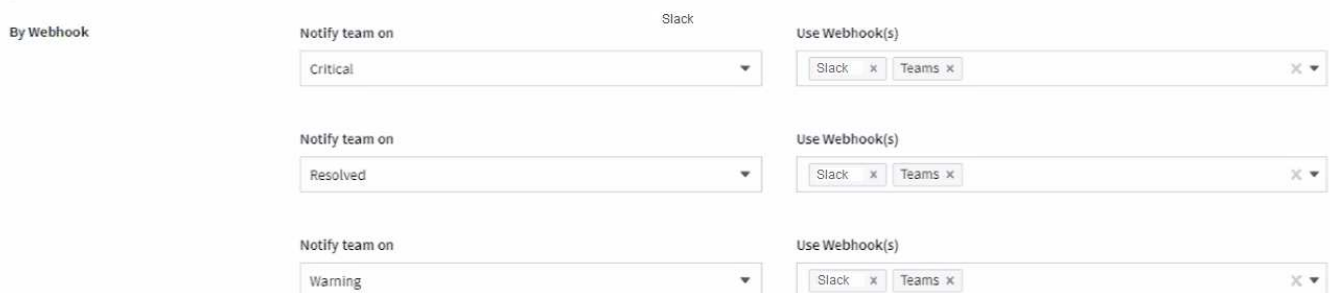
**Section 2:**

- Notify team on:** A dropdown menu with "Warning" selected.
- Add Recipients (Required):** One email address is listed: user\_3@email.com.

#### Alerting via Webhook:

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

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



The form shows three sections for webhook notifications. Each section has a "Notify team on" dropdown and a "Use Webhook(s)" input field.

**Section 1:**

- Notify team on:** A dropdown menu with "Critical" selected.
- Use Webhook(s):** Two webhooks are listed: Slack and Teams.

**Section 2:**

- Notify team on:** A dropdown menu with "Resolved" selected.
- Use Webhook(s):** Two webhooks are listed: Slack and Teams.

**Section 3:**

- Notify team on:** A dropdown menu with "Warning" selected.
- Use Webhook(s):** Two webhooks are listed: Slack and Teams.

## 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 the "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.



## Monitor Groups (5)



Search groups...

- All Monitors (5)
- Custom Monitors (5)
- Agent Monitors (3)
- ONTAP Aggregate Monitors (2)

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.

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

ONTAP Monitors

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



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

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

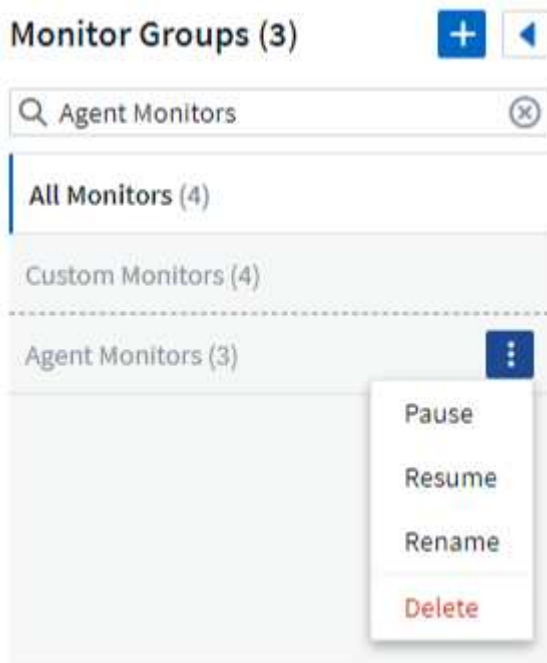


Each monitor can belong to only a single group at any given time.

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

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

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



## System-Defined Monitors (Preview)

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



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

Read more about [System-Defined Monitors](#)

Two groups are shown by default:

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

### 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	<span style="color: red;">❗</span> 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 <a href="#">Subscription</a> page
Subscription will expire in 90 days Subscription will expire in 30 days	No action needed if "Auto Renewal" is enabled Contact <a href="#">NetApp sales</a> to renew the subscription
Trial ends in 2 days	Renew trial from the <a href="#">Subscription</a> page. You can renew a trial one time. Contact <a href="#">NetApp sales</a> 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 <a href="#">NetApp sales</a> 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.

## Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

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