Manage alerts

Active IQ Unified Manager

NetApp
October 07, 2026

This PDF was generated from https://docs.netapp.com/us-en/active-iq-unified-manager/events/concept_what_alerts_are.html on October 07, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Manage alerts . . . 1
- Learn about alerts in Active IQ Unified Manager . . . 1
- Information contained in an Active IQ Unified Manager alert email . . . 1
- Add alerts . . . 2
  - Add alerts in Active IQ Unified Manager . . . 2
  - Guidelines for adding alerts in Active IQ Unified Manager . . . 4
- Add alerts for performance events in Active IQ Unified Manager . . . 5
- Test alerts in Active IQ Unified Manager . . . 6
- Disable alerts for Resolved and Obsolete events in Active IQ Unified Manager . . . 6
- Exclude disaster recovery destination volumes from generating alerts in Active IQ Unified Manager . . . 7
- View alerts in Active IQ Unified Manager . . . 7
- Edit alerts in Active IQ Unified Manager . . . 8
- Delete alerts in Active IQ Unified Manager . . . 8
- Description of alert windows and dialog boxes . . . 8
  - Learn about the Alert Setup page in Active IQ Unified Manager . . . 8
  - Learn about the Add Alert dialog box in Active IQ Unified Manager . . . 10
  - Edit alert properties in Active IQ Unified Manager . . . 13

Manage alerts

Learn about alerts in Active IQ Unified Manager

While events occur continuously, the Unified Manager generates an alert only when an event meets specified filter criteria. You can choose the events for which alerts should be generated—for example, when a space threshold is exceeded or an object goes offline. You can also associate an alert with a script that is executed when an alert is triggered.

Filter criteria include object class, name, or event severity.

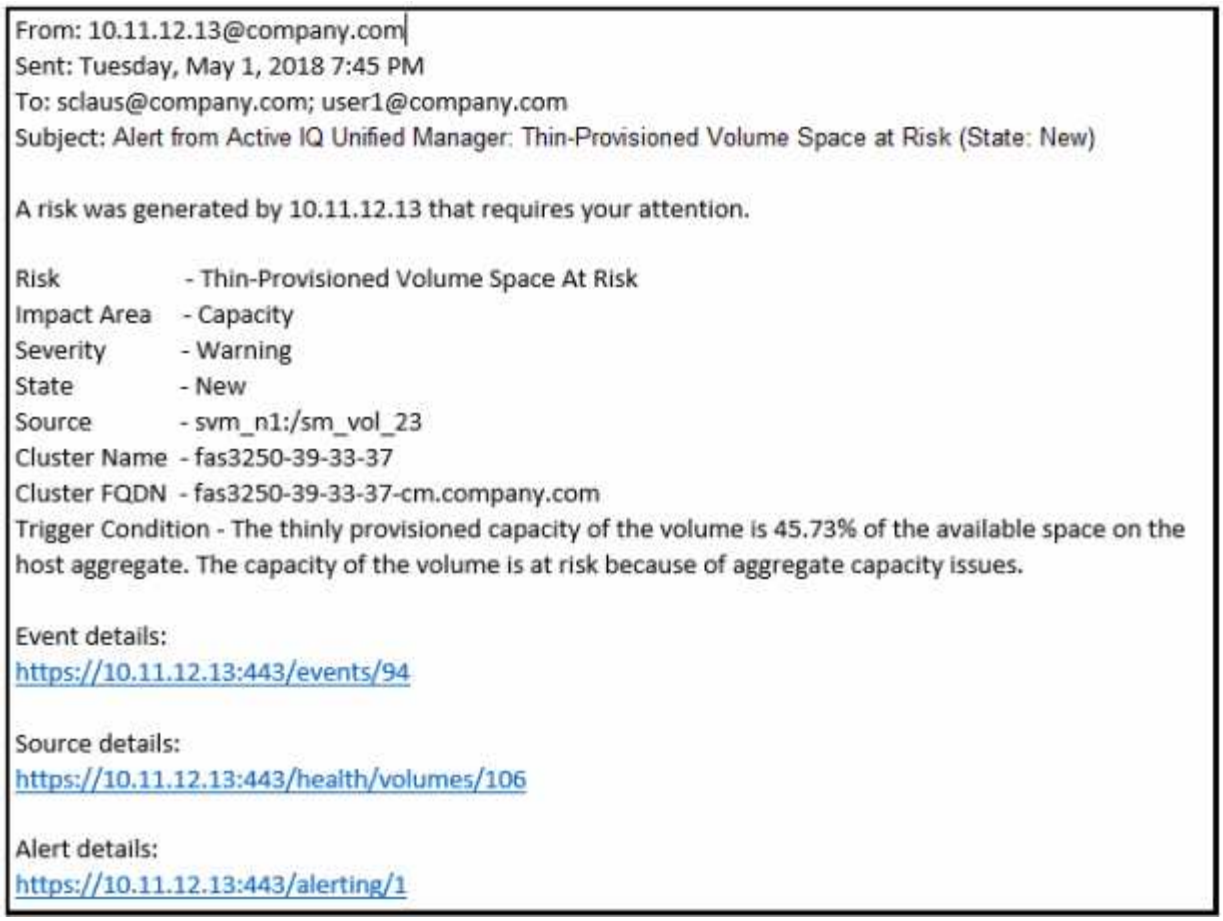
Information contained in an Active IQ Unified Manager alert email

Unified Manager alert emails provide the type of event, the severity of the event, the name of the policy or threshold that was breached to cause the event, and a description of the event. The email message also provides a hyperlink for each event that enables you to view the details page for the event in the UI.

Alert emails are sent to all users who have subscribed to receive alerts.

If a performance counter or capacity value has a large change during a collection period, it could cause both a critical and a warning event to be triggered at the same time for the same threshold policy. In this case, you may receive one email for the warning event and one for the critical event. This is because Unified Manager enables you to subscribe separately to receive alerts for warning and critical threshold breaches.

A sample alert email is shown below:


From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from Active IQ Unified Manager: Thin-Provisioned Volume Space at Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1

Add alerts

Add alerts in Active IQ Unified Manager

You can configure alerts to notify you when a particular event is generated. You can configure alerts for a single resource, for a group of resources, or for events of a particular severity type. You can specify the frequency with which you want to be notified and associate a script to the alert.

Before you begin

- You must have configured notification settings such as the user email address, SMTP server, and SNMP trap host to enable the Active IQ Unified Manager server to use these settings to send notifications to users when an event is generated.
- You must know the resources and events for which you want to trigger the alert, and the user names or email addresses of the users that you want to notify.
- If you want to have a script execute based on the event, you must have added the script to Unified Manager by using the Scripts page.
- You must have the Application Administrator or Storage Administrator role.

You can create an alert directly from the Event details page after receiving an event in addition to creating an alert from the Alert Setup page, as described here.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. In the **Alert Setup** page, click **Add**.
3. In the **Add Alert** dialog box, click **Name**, and enter a name and description for the alert.
4. Click **Resources**, and select the resources to be included in or excluded from the alert.

   You can set a filter by specifying a text string in the **Name contains** field to select a group of resources. Based on the text string that you specify, the list of available resources displays only those resources that match the filter rule. The text string that you specify is case-sensitive.

   If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule, and the alert is not generated for events related to the excluded resource.

5. Click **Events**, and select the events based on the event name or event severity type for which you want to trigger an alert.

   To select more than one event, press the Ctrl key while you make your selections.

6. Click **Actions**, and select the users that you want to notify, choose the notification frequency, choose whether an SNMP trap will be sent to the trap receiver, and assign a script to be executed when an alert is generated.

   If you modify the email address that is specified for the user and reopen the alert for editing, the Name field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you modified the email address of the selected user from the Users page, the modified email address is not updated for the selected user.

   You can also choose to notify users through SNMP traps.

7. Click **Save**.

Example of adding an alert

This example shows how to create an alert that meets the following requirements:

- Alert name: HealthTest
- Resources: includes all volumes whose name contains "abc" and excludes all volumes whose name contains "xyz"
- Events: includes all critical health events
- Actions: includes "sample@domain.com", a "Test" script, and the user has to be notified every 15 minutes

Perform the following steps in the Add Alert dialog box:

1. Click **Name**, and enter **`HealthTest`** in the **Alert Name** field.
2. Click **Resources**, and in the Include tab, select **Volumes** from the drop-down list.
   a. Enter **`abc`** in the **Name contains** field to display the volumes whose name contains "abc".
   b. Select **<<All Volumes whose name contains 'abc'>>** from the Available Resources area, and move it to the Selected Resources area.
   c. Click **Exclude**, and enter **`xyz`** in the **Name contains** field, and then click **Add**.

3. Click **Events**, and select **Critical** from the Event Severity field.
4. Select **All Critical Events** from the Matching Events area, and move it to the Selected Events area.
5. Click **Actions**, and enter **`sample@domain.com`** in the Alert these users field.
6. Select **Remind every 15 minutes** to notify the user every 15 minutes.

   You can configure an alert to repeatedly send notifications to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.

7. In the Select Script to Execute menu, select **Test** script.
8. Click **Save**.

Guidelines for adding alerts in Active IQ Unified Manager

You can add alerts based on a resource, such as a cluster, node, aggregate, or volume, and events of a particular severity type. As a best practice, you can add an alert for any of your critical objects after you have added the cluster to which the object belongs.

You can use the following guidelines and considerations to create alerts to manage your systems effectively:

- Alert description

  You should provide a description for the alert so that it helps you track your alerts effectively.

- Resources

  You should decide which physical or logical resource requires an alert. You can include and exclude resources, as required. For example, if you want to closely monitor your aggregates by configuring an alert, you must select the required aggregates from the list of resources.

  If you select a category of resources, for example, **<<All User or Group Quotas>>**, then you will receive alerts for all objects in that category.

  > Selecting a cluster as the resource does not automatically select the storage objects within that cluster. For example, if you create an alert for all critical events for all clusters you will receive alerts only for cluster critical events. You will not receive alerts for critical events on nodes, aggregates, and so forth.

- Event severity

  You should decide if an event of a specified severity type (Critical, Error, Warning) should trigger the alert and, if so, which severity type.

- Selected Events

  If you add an alert based on the type of event generated, you should decide which events require an alert.

  If you select an event severity, but do not select any individual events (if you leave the "Selected Events" column empty) then you will receive alerts for all events in the category.

- Actions

  You must provide the user names and email addresses of the users who receive the notification. You can

also specify an SNMP trap as a mode of notification. You can associate your scripts to an alert so that they are executed when an alert is generated.

- Notification frequency

  You can configure an alert to repeatedly send notification to the recipients for a specified time. You should determine the time from which the event notification is active for the alert. If you want the event notification to be repeated until the event is acknowledged, you should determine how often you want the notification to be repeated.

- Execute Script

  You can associate your script with an alert. Your script is executed when the alert is generated.

Add alerts for performance events in Active IQ Unified Manager

You can configure alerts for individual performance events just like any other events received by Unified Manager. Additionally, if you want to treat all performance events alike and have email sent to the same person, you can create a single alert to notify you when any critical or warning performance events are triggered.

Before you begin

You must have the Application Administrator or Storage Administrator role.

The example below shows how to create an event for all critical latency, IOPS, and MBps events. You can use this same methodology to select events from all performance counters, and for all warning events.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. In the **Alert Setup** page, click **Add**.
3. In the **Add Alert** dialog box, click **Name**, and enter a name and description for the alert.
4. Do not select any resources on the **Resources** page.

   Because no resources are selected, the alert is applied to all clusters, aggregates, volumes, and so on, for which these events are received.

5. Click **Events** and perform the following actions:
   a. In the Event Severity list, select **Critical**.
   b. In the Event Name Contains field, enter `latency` and then click the arrow to select all the matching events.
   c. In the Event Name Contains field, enter `iops` and then click the arrow to select all the matching events.
   d. In the Event Name Contains field, enter `mbps` and then click the arrow to select all the matching events.
6. Click **Actions** and then select the name of the user who will receive the alert email in the **Alert these users** field.
7. Configure any other options on this page for issuing SNMP traps and executing a script.

8. Click **Save**.

Test alerts in Active IQ Unified Manager

You can test an alert to verify that you have configured it correctly. When an event is triggered, an alert is generated, and an alert email is sent to the configured recipients. You can verify whether the notification is sent and whether your script is executed by using the test alert.

Before you begin

- You must have configured notification settings such as the email address of the recipients, SMTP server, and SNMP trap.

  The Unified Manager server can use these settings to send notifications to users when an event is generated.

- You must have assigned a script and configured the script to run when the alert is generated.
- You must have the Application Administrator role.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. In the **Alert Setup** page, select the alert that you want to test, and then click **Test**.

   A test alert email is sent to the email addresses that you specified while creating the alert.

Disable alerts for Resolved and Obsolete events in Active IQ Unified Manager

For all events that you have configured to send alerts, an alert message is sent when those events transition through all available states: New, Resolved, and Obsolete. If you do not want to receive alerts for events as they move into the Resolved and Obsolete states, you can configure a global setting to suppress those alerts.

Before you begin

You must have the Application Administrator or Storage Administrator role.

By default, alerts are not sent for events as they move into the Resolved and Obsolete states.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. In the **Alert Setup** page, perform one of the following actions using the slider control next to the item **Alerts for Resolved and Obsolete events**:

To…	Do this…
Stop sending alerts as events are resolved or obsoleted	Move the slider control to the left

To…	Do this…
Start sending alerts as events are resolved or obsoleted	Move the slider control to the right

Exclude disaster recovery destination volumes from generating alerts in Active IQ Unified Manager

When configuring volume alerts you can specify a string in the Alert dialog box that identifies a volume or group of volumes. If you have configured disaster recovery for SVMs, however, the source and destination volumes have the same name, so you will receive alerts for both volumes.

Before you begin

You must have the Application Administrator or Storage Administrator role.

You can disable alerts for disaster recovery destination volumes by excluding volumes that have the name of the destination SVM. This is possible because the identifier for volume events contains both the SVM name and volume name in the format "<svm_name>:/<volume_name>".

The example below shows how to create alerts for volume "vol1" on the primary SVM "vs1", but exclude the alert from being generated on a volume with the same name on SVM "vs1-dr".

Perform the following steps in the Add Alert dialog box:

Steps

1. Click **Name** and enter a name and description for the alert.
2. Click **Resources**, and then select the **Include** tab.
   a. Select **Volume** from the drop-down list, and then enter **`vol1`** in the **Name contains** field to display the volumes whose name contains "vol1".
   b. Select **<<All Volumes whose name contains 'vol1'>>** from the **Available Resources** area, and move it to the **Selected Resources** area.
3. Select the **Exclude** tab, select **Volume**, enter **`vs1-dr`** in the **Name contains** field, and then click **Add**.

   This excludes the alert from being generated for volume "vol1" on SVM "vs1-dr".
4. Click **Events** and select the event or events that you want to apply to the volume or volumes.
5. Click **Actions** and then select the name of the user who will receive the alert email in the **Alert these users** field.
6. Configure any other options on this page for issuing SNMP traps and executing a script, and then click **Save**.

View alerts in Active IQ Unified Manager

You can view the list of alerts that is created for various events from the Alert Setup page. You can also view alert properties such as the alert description, notification method and frequency, events that trigger the alert, email recipients of the alerts, and affected resources such as clusters, aggregates, and volumes.

Before you begin

You must have the Operator, Application Administrator, or Storage Administrator role.

Step

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.

   The list of alerts is displayed in the Alert Setup page.

Edit alerts in Active IQ Unified Manager

You can edit alert properties such as the resource with which the alert is associated, events, recipients, notification options, notification frequency, and associated scripts.

Before you begin

You must have the Application Administrator role.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. In the **Alert Setup** page, select the alert that you want to edit, and click **Edit**.
3. In the **Edit Alert** dialog box, edit the name, resources, events, and actions sections, as required.

   You can change or remove the script that is associated with the alert.

4. Click **Save**.

Delete alerts in Active IQ Unified Manager

You can delete an alert when it is no longer required. For example, you can delete an alert that was created for a particular resource when that resource is no longer monitored by Unified Manager.

Before you begin

You must have the Application Administrator role.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. On the **Alert Setup** page, select the alerts that you want to delete, and click **Delete**.
3. Click **Yes** to confirm the delete request.

Description of alert windows and dialog boxes

Learn about the Alert Setup page in Active IQ Unified Manager

The Alert Setup page displays a list of alerts and provides information about the alert name, status, notification method, and notification frequency. You can also add, edit, remove, enable, or disable alerts from this page.

You must have the Application Administrator or Storage Administrator role.

Command buttons

- **Add**

  Displays the Add Alert dialog box, which enables you to add new alerts.

- **Edit**

  Displays the Edit Alert dialog box, which enables you to edit selected alerts.

- **Delete**

  Deletes the selected alerts.

- **Enable**

  Enables the selected alerts to send notifications.

- **Disable**

  Disables the selected alerts when you want to temporarily stop sending notifications.

- **Test**

  Tests the selected alerts to verify their configuration after being added or edited.

- **Alerts for Resolved and Obsolete Events**

  Allows you to enable or disable the sending of alerts when events are moved to the Resolved or Obsolete states. This can help users from receiving unnecessary notifications.

List view

The list view displays, in tabular format, information about the alerts that are created. You can use the column filters to customize the data that is displayed. You can also select an alert to view more information about it in the details area.

- **Status**

  Specifies whether an alert is enabled ( ) or disabled ( ).

- **Alert**

  Displays the name of the alert.

- **Description**

  Displays a description for the alert.

- **Notification Method**

  Displays the notification method that is selected for the alert. You can notify users through email or SNMP traps.

- **Notification Frequency**

  Specifies the frequency (in minutes) with which the management server continues to send notifications until the event is acknowledged, resolved, or moved to the Obsolete state.

Details area

The details area provides more information about the selected alert.

- **Alert Name**

  Displays the name of the alert.

- **Alert Description**

  Displays a description for the alert.

- **Events**

  Displays the events for which you want to trigger the alert.

- **Resources**

  Displays the resources for which you want to trigger the alert.

- **Includes**

  Displays the group of resources for which you want to trigger the alert.

- **Excludes**

  Displays the group of resources for which you do not want to trigger the alert.

- **Notification Method**

  Displays the notification method for the alert.

- **Notification Frequency**

  Displays the frequency with which the management server continues to send alert notifications until the event is acknowledged, resolved, or moved to the Obsolete state.

- **Script Name**

  Displays the name of the script associated with the selected alert. This script is executed when an alert is generated.

- **Email Recipients**

  Displays the email addresses of users who receive the alert notification.

Learn about the Add Alert dialog box in Active IQ Unified Manager

You can create alerts to notify you when a particular event is generated, so that you can address the issue quickly and thereby minimize impact to your environment. You can

create alerts for a single resource or a set of resources, and for events of a particular severity type. You can also specify the notification method and frequency of the alerts.

You must have the Application Administrator or Storage Administrator role.

Name

This area enables you to specify a name and description for the alert:

- **Alert Name**

  Enables you to specify an alert name.

- **Alert Description**

  Enables you to specify a description for the alert.

Resources

This area enables you to select an individual resource or group the resources based on a dynamic rule for which you want to trigger the alert. A *dynamic rule* is the set of resources filtered based on the text string you specify. You can search for resources by selecting a resource type from the drop-down list or you can specify the exact resource name to display a specific resource.

If you are creating an alert from any of the storage object details pages, the storage object is automatically included in the alert.

- **Include**

  Enables you to include the resources for which you want to trigger alerts. You can specify a text string to group resources that match the string and select this group to be included in the alert. For example, you can group all volumes whose name contains the "abc" string.

- **Exclude**

  Enables you to exclude resources for which you do not want to trigger alerts. For example, you can exclude all volumes whose name contains the "xyz" string.

  The Exclude tab is displayed only when you select all resources of a particular resource type: for example, <<All Volumes>> or <<All Volumes whose name contains 'xyz'>>.

  If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule and the alert is not generated for the event.

Events

This area enables you to select the events for which you want to create the alerts. You can create alerts for events based on a particular severity or for a set of events.

To select more than one event, you should hold down the Ctrl key while you make your selections.

- **Event Severity**

  Enables you to select events based on the severity type, which can be Critical, Error, or Warning.

- **Event Name Contains**

  Enables you to select events whose name contains specified characters.

Actions

This area enables you to specify the users that you want to notify when an alert is triggered. You can also specify the notification method and the frequency of notification.

- **Alert these users**

  Enables you to specify the email address or user name of the user to receive notifications.

  If you modify the email address that is specified for the user and reopen the alert for editing, the Name field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you have modified the email address of the selected user from the Users page, the modified email address is not updated for the selected user.

- **Notification Frequency**

  Enables you to specify the frequency with which the management server sends notifications until the event is acknowledged, resolved, or moved to the obsolete state.

  You can choose the following notification methods:

  - Notify only once
  - Notify at a specified frequency
  - Notify at a specified frequency within the specified time range

- **Issue SNMP trap**

  Selecting this box enables you to specify whether SNMP traps should be sent to the globally configured SNMP host.

- **Execute Script**

  Enables you to add your custom script to the alert. This script is executed when an alert is generated.

  If you do not see this capability available in the user interface it is because the functionality has been disabled by your administrator. If required, you can enable this functionality from **Storage Management** > **Feature Settings**.

Command buttons

- **Save**

  Creates an alert and closes the dialog box.

- **Cancel**

  Discards the changes and closes the dialog box.

Edit alert properties in Active IQ Unified Manager

You can edit alert properties such as the resource with which the alert is associated, events, script, and notification options.

Name

This area enables you to edit the name and description for the alert.

- **Alert Name**

  Enables you to edit the alert name.

- **Alert Description**

  Enables you to specify a description for the alert.

- **Alert State**

  Enables you to enable or disable the alert.

Resources

This area enables you to select an individual resource or group the resources based on a dynamic rule for which you want to trigger the alert. You can search for resources by selecting a resource type from the drop-down list or you can specify the exact resource name to display a specific resource.

- **Include**

  Enables you to include the resources for which you want to trigger alerts. You can specify a text string to group resources that match the string and select this group to be included in the alert. For example, you can group all volumes whose name contains the “vol0” string.

- **Exclude**

  Enables you to exclude resources for which you do not want to trigger alerts. For example, you can exclude all volumes whose name contains the “xyz” string.

  The Exclude tab is displayed only when you select all resources of a particular resource type—for example, <<All Volumes>> or <<All Volumes whose name contains 'xyz'>>.

Events

This area enables you to select the events for which you want to trigger the alerts. You can trigger an alert for events based on a particular severity or for a set of events.

- **Event Severity**

  Enables you to select events based on the severity type, which can be Critical, Error, or Warning.

- **Event Name Contains**

  Enables you to select events whose name contains the specified characters.

Actions

This area enables you to specify the notification method and the frequency of notification.

- **Alert these users**

  Enables you to edit the email address or user name, or specify a new email address or user name to receive notifications.

- **Notification Frequency**

  Enables you to edit the frequency with which the management server sends notifications until the event is acknowledged, resolved, or moved to the obsolete state.

  You can choose the following notification methods:

  - Notify only once
  - Notify at a specified frequency
  - Notify at a specified frequency within the specified time range

- **Issue SNMP trap**

  Enables you to specify whether SNMP traps should be sent to the globally configured SNMP host.

- **Execute Script**

  Enables you to associate a script with the alert. This script is executed when an alert is generated.

Command buttons

- **Save**

  Saves the changes and closes the dialog box.

- **Cancel**

  Discards the changes and closes the dialog box.

Copyright information

Copyright © 2026 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.