# Manage alert notifications

StorageGRID

NetApp
July 18, 2022

# Table of Contents

# Manage alert notifications

## Set up SNMP notifications for alerts

If you want StorageGRID to send SNMP notifications when alerts occur, you must enable the StorageGRID SNMP agent and configure one or more trap destinations.

You can use the **CONFIGURATION** > **Monitoring** > **SNMP agent** option in the Grid Manager or the SNMP endpoints for the Grid Management API to enable and configure the StorageGRID SNMP agent. The SNMP agent supports all three versions of the SNMP protocol.

To learn how to configure the SNMP agent, see Use SNMP monitoring.

After you configure the StorageGRID SNMP agent, two types of event-driven notifications can be sent:

- Traps are notifications sent by the SNMP agent that do not require acknowledgment by the management system. Traps serve to notify the management system that something has happened within StorageGRID, such as an alert being triggered. Traps are supported in all three versions of SNMP.
- Informs are similar to traps, but they require acknowledgment by the management system. If the SNMP agent does not receive an acknowledgment within a certain amount of time, it resends the inform until an acknowledgment is received or the maximum retry value has been reached. Informs are supported in SNMPv2c and SNMPv3.

Trap and inform notifications are sent when a default or custom alert is triggered at any severity level. To suppress SNMP notifications for an alert, you must configure a silence for the alert. See Silence alert notifications.

Alert notifications are sent by whichever Admin Node is configured to be the preferred sender. By default, the primary Admin Node is selected. See the instructions for administering StorageGRID.

> Trap and inform notifications are also sent when certain alarms (legacy system) are triggered at specified severity levels or higher; however, SNMP notifications are not sent for every alarm or every alarm severity. See Alarms that generate SNMP notifications (legacy system).

## Set up email notifications for alerts

If you want email notifications to be sent when alerts occur, you must provide information about your SMTP server. You must also enter email addresses for the recipients of alert notifications.

**What you'll need**

- You are signed in to the Grid Manager using a supported web browser.
- You have the Manage Alerts or Root Access permission.

**About this task**

Because alarms and alerts are independent systems, the email setup used for alert notifications is not used for alarm notifications and AutoSupport messages. However, you can use the same email server for all notifications.

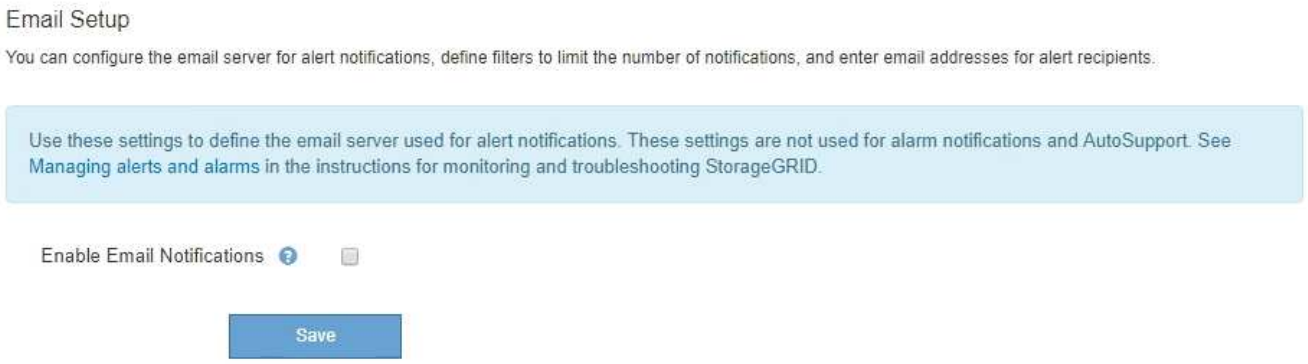
If your StorageGRID deployment includes multiple Admin Nodes, you can select which Admin Node should be

the preferred sender of alert notifications. The same “preferred sender” is also used for alarm notifications and AutoSupport messages. By default, the primary Admin Node is selected. For details, see the instructions for administering StorageGRID.

**Steps**

1. Select **ALERTS** > **Email setup**.

   The Email Setup page appears.




2. Select the **Enable Email Notifications** check box to indicate that you want notification emails to be sent when alerts reach configured thresholds.

   The Email (SMTP) Server, Transport Layer Security (TLS), Email Addresses, and Filters sections appear.

3. In the Email (SMTP) Server section, enter the information StorageGRID needs to access your SMTP server.

   If your SMTP server requires authentication, you must provide both a username and a password.

| Field | Enter |
|---|---|
| Mail Server | The fully qualified domain name (FQDN) or IP address of the SMTP server. |
| Port | The port used to access the SMTP server. Must be between 1 and 65535. |
| Username (optional) | If your SMTP server requires authentication, enter the username to authenticate with. |
| Password (optional) | If your SMTP server requires authentication, enter the password to authenticate with. |


4. In the Email Addresses section, enter email addresses for the sender and for each recipient.

   a. For the **Sender Email Address**, specify a valid email address to use as the From address for alert notifications.

      For example: `storagegrid-alerts@example.com`

   b. In the Recipients section, enter an email address for each email list or person who should receive an email when an alert occurs.

      Select the plus icon ✚ to add recipients.


5. If Transport Layer Security (TLS) is required for communications with the SMTP server, select **Require TLS** in the Transport Layer Security (TLS) section.

   a. In the **CA Certificate** field, provide the CA certificate that will be used to verify the identify of the SMTP server.

      You can copy and paste the contents into this field, or select **Browse** and select the file.

      You must provide a single file that contains the certificates from each intermediate issuing certificate authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.

   b. Select the **Send Client Certificate** check box if your SMTP email server requires email senders to provide client certificates for authentication.

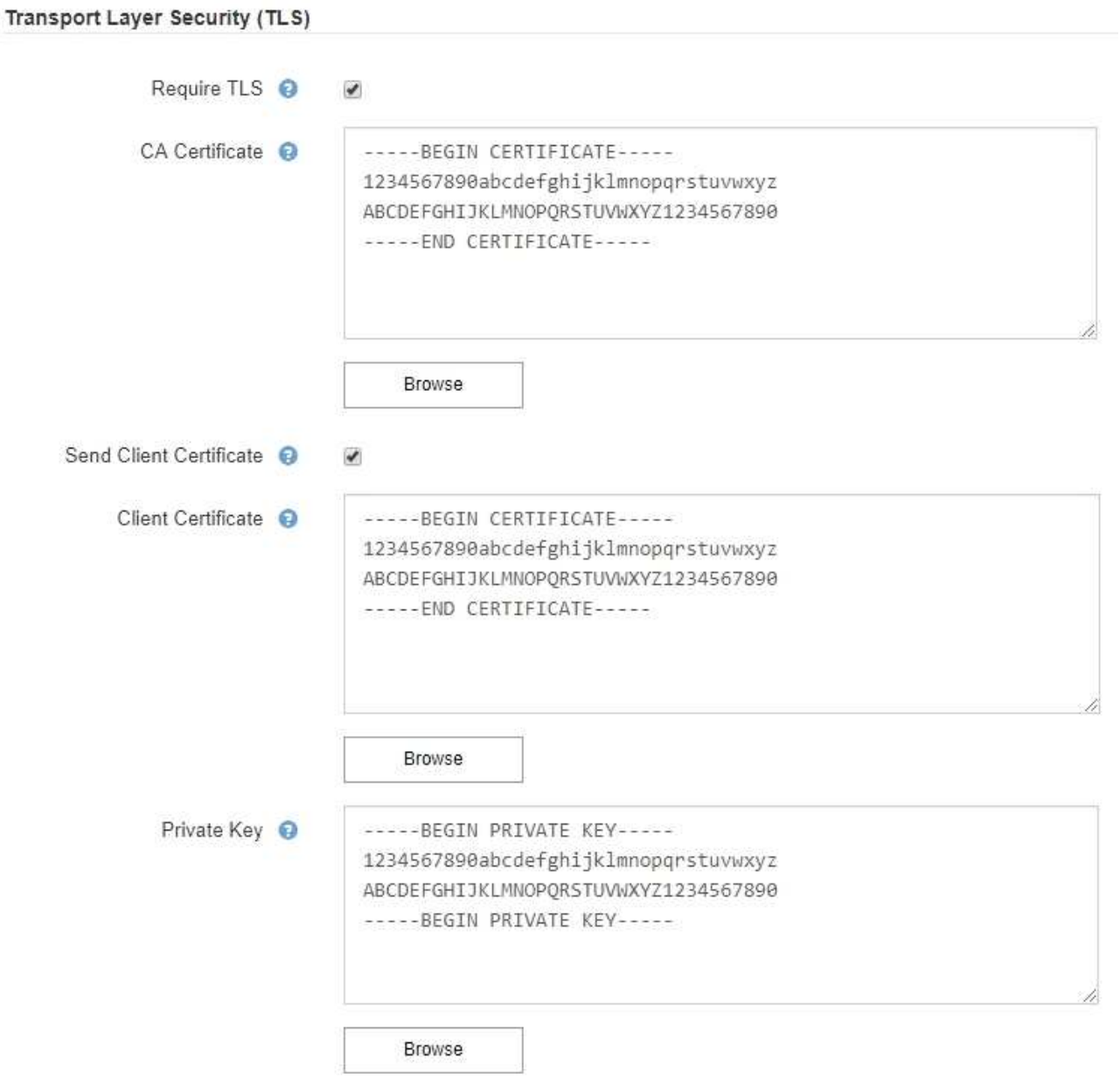
   c. In the **Client Certificate** field, provide the PEM-encoded client certificate to send to the SMTP server.

      You can copy and paste the contents into this field, or select **Browse** and select the file.

   d. In the **Private Key** field, enter the private key for the client certificate in unencrypted PEM encoding.

      You can copy and paste the contents into this field, or select **Browse** and select the file.

If you need to edit the email setup, select the pencil icon to update this field.




6. In the Filters section, select which alert severity levels should result in email notifications, unless the rule for a specific alert has been silenced.

| Severity | Description |
|---|---|
| Minor, major, critical | An email notification is sent when the minor, major, or critical condition for an alert rule is met. |
| Major, critical | An email notification is sent when the major or critical condition for an alert rule is met. Notifications are not sent for minor alerts. |
| Critical only | An email notification is sent only when the critical condition for an alert rule is met. Notifications are not sent for minor or major alerts. |


7. When you are ready to test your email settings, perform these steps:
   a. Select **Send Test Email**.

      A confirmation message appears, indicating that a test email was sent.

   b. Check the inboxes of all email recipients and confirm that a test email was received.

      If the email is not received within a few minutes or if the **Email notification failure** alert is triggered, check your settings and try again.

   c. Sign in to any other Admin Nodes and send a test email to verify connectivity from all sites.

      When you test alert notifications, you must sign in to every Admin Node to verify connectivity. This is in contrast to testing alarm notifications and AutoSupport messages, where all Admin Nodes send the test email.

8. Select **Save**.

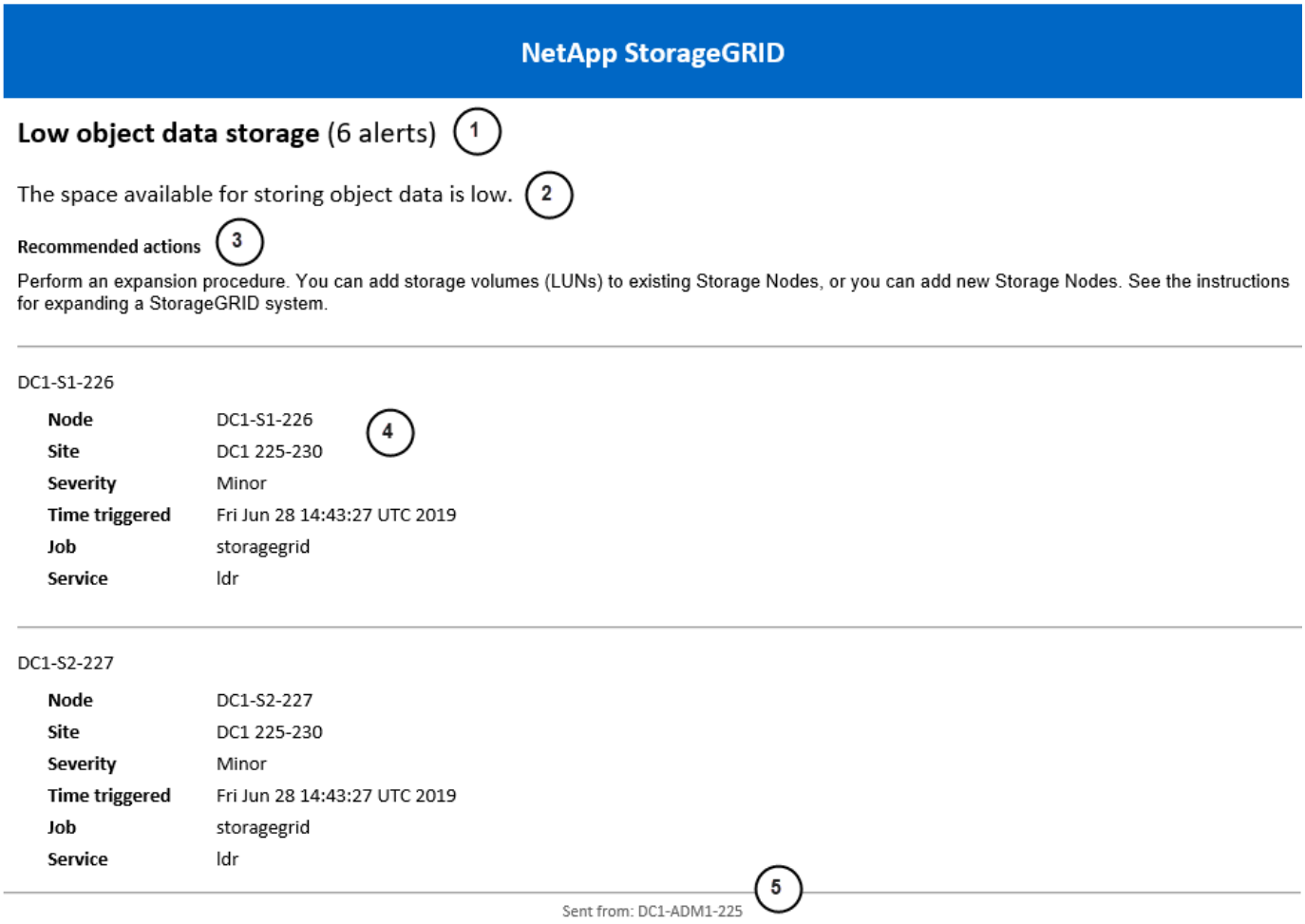
   Sending a test email does not save your settings. You must select **Save**.

   The email settings are saved.

## Information included in alert email notifications

After you configure the SMTP email server, email notifications are sent to the designated recipients when an alert is triggered, unless the alert rule is suppressed by a silence. See Silence alert notifications.

Email notifications include the following information:




| Callout | Description |
|---|---|
| 1 | The name of the alert, followed by the number of active instances of this alert. |
| 2 | The description of the alert. |
| 3 | Any recommended actions for the alert. |
| 4 | Details about each active instance of the alert, including the node and site affected, the alert severity, the UTC time when the alert rule was triggered, and the name of the affected job and service. |
| 5 | The hostname of the Admin Node that sent the notification. |

## How alerts are grouped

To prevent an excessive number of email notifications from being sent when alerts are triggered, StorageGRID attempts to group multiple alerts in the same notification.

Refer to the following table for examples of how StorageGRID groups multiple alerts in email notifications.

| Behavior | Example |
| --- | --- |
| Each alert notification applies only to alerts that have the same name. If two alerts with different names are triggered at the same time, two email notifications are sent. | • Alert A is triggered on two nodes at the same time. Only one notification is sent.<br>• Alert A is triggered on node 1, and Alert B is triggered on node 2 at the same time. Two notifications are sent—one for each alert. |
| For a specific alert on a specific node, if the thresholds are reached for more than one severity, a notification is sent only for the most severe alert. | • Alert A is triggered and the minor, major, and critical alert thresholds are reached. One notification is sent for the critical alert. |
| The first time an alert is triggered, StorageGRID waits 2 minutes before sending a notification. If other alerts with the same name are triggered during that time, StorageGRID groups all of the alerts in the initial notification. | 1. Alert A is triggered on node 1 at 08:00. No notification is sent.<br>2. Alert A is triggered on node 2 at 08:01. No notification is sent.<br>3. At 08:02, a notification is sent to report both instances of the alert. |
| If an another alert with the same name is triggered, StorageGRID waits 10 minutes before sending a new notification. The new notification reports all active alerts (current alerts that have not been silenced), even if they were reported previously. | 1. Alert A is triggered on node 1 at 08:00. A notification is sent at 08:02.<br>2. Alert A is triggered on node 2 at 08:05. A second notification is sent at 08:15 (10 minutes later). Both nodes are reported. |
| If there are multiple current alerts with the same name and one of those alerts is resolved, a new notification is not sent if the alert reoccurs on the node for which the alert was resolved. | 1. Alert A is triggered for node 1. A notification is sent.<br>2. Alert A is triggered for node 2. A second notification is sent.<br>3. Alert A is resolved for node 2, but it remains active for node 1.<br>4. Alert A is triggered again for node 2. No new notification is sent because the alert is still active for node 1. |
| StorageGRID continues to send email notifications once every 7 days until all instances of the alert are resolved or the alert rule is silenced. | 1. Alert A is triggered for node 1 on March 8. A notification is sent.<br>2. Alert A is not resolved or silenced. Additional notifications are sent on March 15, March 22, March 29, and so on. |

## Troubleshoot alert email notifications

If the **Email notification failure** alert is triggered or you are unable to receive the test alert email notification, follow these steps to resolve the issue.

**What you'll need**

- You are signed in to the Grid Manager using a supported web browser.
- You have the Manage Alerts or Root Access permission.

**Steps**

1. Verify your settings.
   a. Select **ALERTS** > **Email setup**.
   b. Verify that the Email (SMTP) Server settings are correct.
   c. Verify that you have specified valid email addresses for the recipients.
2. Check your spam filter, and make sure that the email was not sent to a junk folder.
3. Ask your email administrator to confirm that emails from the sender address are not being blocked.
4. Collect a log file for the Admin Node, and then contact technical support.

   Technical support can use the information in the logs to help determine what went wrong. For example, the prometheus.log file might show an error when connecting to the server you specified.

   See Collect log files and system data.

# Silence alert notifications

Optionally, you can configure silences to temporarily suppress alert notifications.

**What you'll need**

- You are signed in to the Grid Manager using a supported web browser.
- You have the Manage Alerts or Root Access permission.

**About this task**

You can silence alert rules on the entire grid, a single site, or a single node and for one or more severities. Each silence suppresses all notifications for a single alert rule or for all alert rules.

If you have enabled the SNMP agent, silences also suppress SNMP traps and informs.

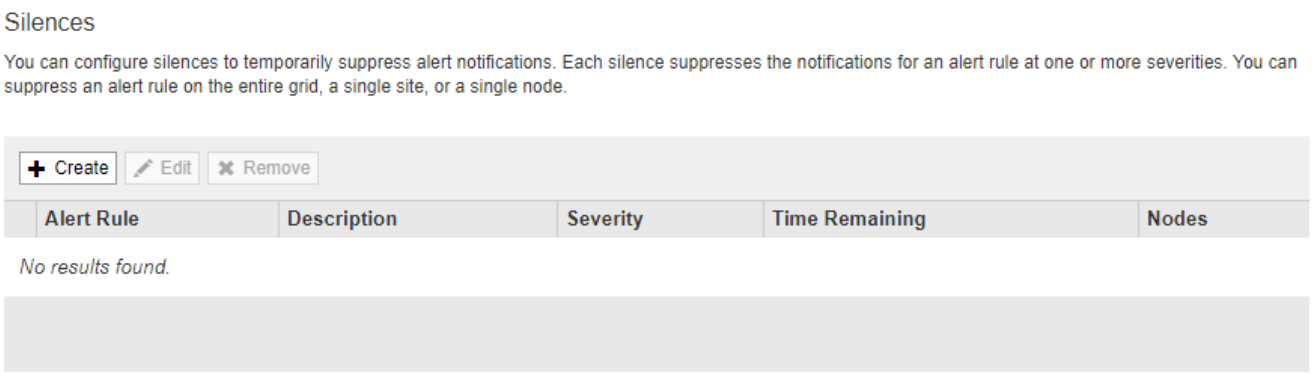
> Be careful when deciding to silence an alert rule. If you silence an alert, you might not detect an underlying problem until it prevents a critical operation from completing.

> Because alarms and alerts are independent systems, you cannot use this functionality to suppress alarm notifications.

**Steps**

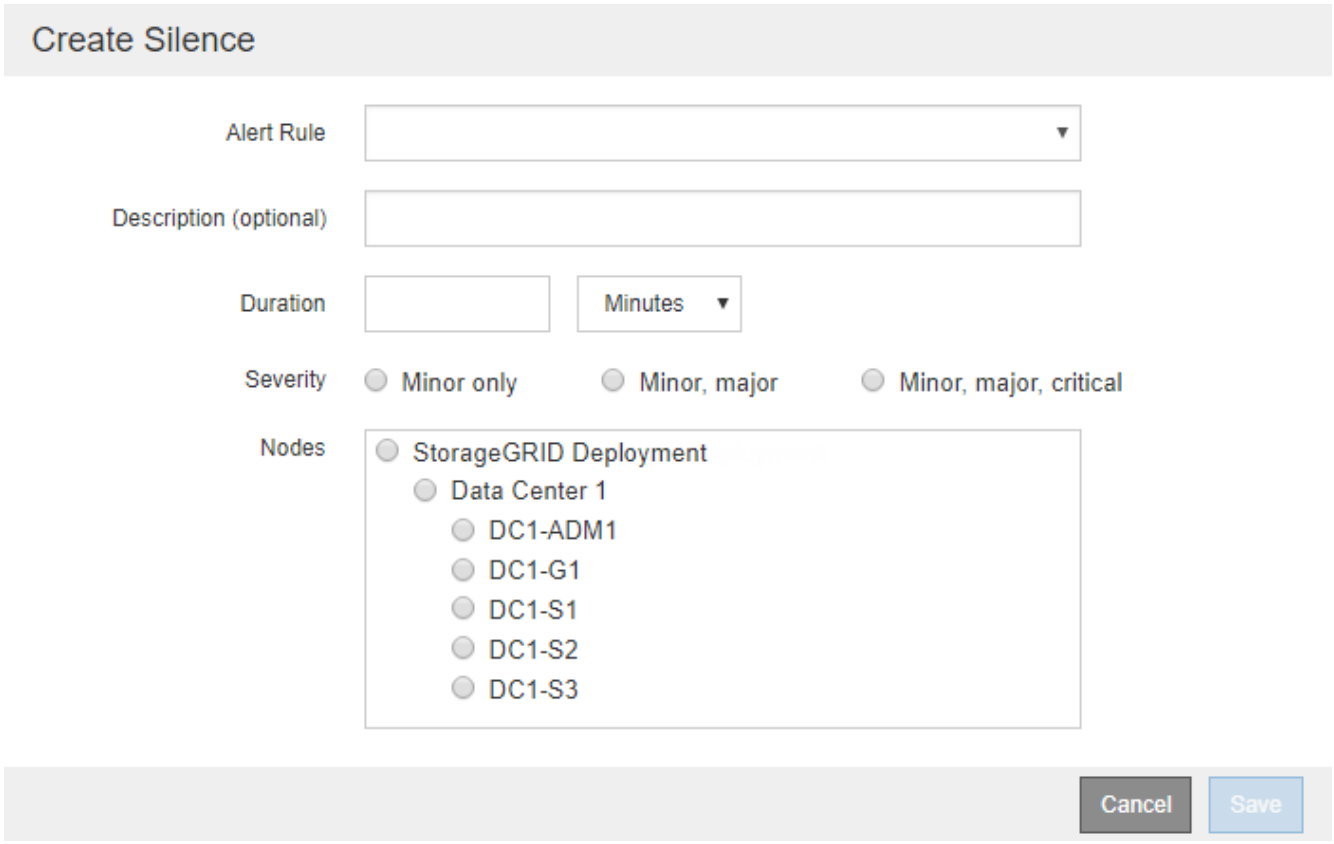
1. Select **ALERTS** > **Silences**.

   The Silences page appears.




2. Select **Create**.

   The Create Silence dialog box appears.




3. Select or enter the following information:

| Field | Description |
|---|---|
| Alert Rule | The name of the alert rule you want to silence. You can select any default or custom alert rule, even if the alert rule is disabled.<br><br>**Note:** Select **All rules** if you want to silence all alert rules using the criteria specified in this dialog box. |
| Description | Optionally, a description of the silence. For example, describe the purpose of this silence. |

| Field | Description |
| --- | --- |
| Duration | How long you want this silence to remain in effect, in minutes, hours, or days. A silence can be in effect from 5 minutes to 1,825 days (5 years).<br><br>**Note:** You should not silence an alert rule for an extended amount of time. If an alert rule is silenced, you might not detect an underlying problem until it prevents a critical operation from completing. However, you might need to use an extended silence if an alert is triggered by a specific, intentional configuration, such as might be the case for the **Services appliance link down** alerts and the **Storage appliance link down** alerts. |
| Severity | Which alert severity or severities should be silenced. If the alert is triggered at one of the selected severities, no notifications are sent. |
| Nodes | Which node or nodes you want this silence to apply to. You can suppress an alert rule or all rules on the entire grid, a single site, or a single node. If you select the entire grid, the silence applies to all sites and all nodes. If you select a site, the silence applies only to the nodes at that site.<br><br>**Note:** You cannot select more than one node or more than one site for each silence. You must create additional silences if you want to suppress the same alert rule on more than one node or more than one site at one time. |

4. Select **Save**.
5. If you want to modify or end a silence before it expires, you can edit or remove it.

| Option | Description |
| --- | --- |
| Edit a silence | a. Select **ALERTS** > **Silences**.<br>b. From the table, select the radio button for the silence you want to edit.<br>c. Select **Edit**.<br>d. Change the description, the amount of time remaining, the selected severities, or the affected node.<br>e. Select **Save**. |
| Remove a silence | a. Select **ALERTS** > **Silences**.<br>b. From the table, select the radio button for the silence you want to remove.<br>c. Select **Remove**.<br>d. Select **OK** to confirm you want to remove this silence.<br><br>**Note**: Notifications will now be sent when this alert is triggered (unless suppressed by another silence). If this alert is currently triggered, it might take few minutes for email or SNMP notifications to be sent and for the Alerts page to update. |

**Related information**

- Configure the SNMP agent