



Webhook Notifications

Data Infrastructure Insights

NetApp

February 03, 2026

This PDF was generated from https://docs.netapp.com/us-en/data-infrastructure-insights/ws_notifications_using_webhooks.html on February 03, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Webhook Notifications	1
Workload Security notifications using webhooks	1
Creating a webhook	1
Parameters: What are they and how to use them?	2
Workload Security Webhooks List Page	3
Configure Webhook notification in alert policy	4
Workload Security Webhook Example for Discord	6
Discord Setup:	6
Create Workload Security Webhook:	6
Notifications via Webhook	8
Workload Security Webhook Example for PagerDuty	9
PagerDuty Setup:	10
Create Workload Security PagerDuty Webhook:	11
Notifications via Webhook	12
Workload Security Webhook Example for Slack	13
Workload Security Webhook Example for Microsoft Teams	16
Teams Setup:	16
Create Workload Security Teams Webhook:	17
Notifications via Webhook	18

Webhook Notifications

Workload Security notifications using webhooks

Webhooks allow users to send critical or warning alert notifications to various applications using a customized webhook channel.

Many commercial applications support webhooks as a standard input interface, for example: Slack, PagerDuty, Teams, and Discord. By supporting a generic, customizable webhook channel, Workload Security can support many of these delivery channels. Information about configuring the webhooks can be found on the respective application's websites. For example, Slack provides [this useful guide](#).

You can create multiple webhook channels, each channel targeted for a different purpose, separate applications, different recipients, etc.

The webhook channel instance is comprised of the following elements

Name	Description
URL	Webhook target URL, including the http:// or https:// prefix along with the url params
Method	GET/POST - Default is POST
Custom Header	Specify any custom headers here
Message Body	Put the body of your message here
Default Alert Parameters	Lists the default parameters for the webhook
Custom Parameters and Secrets	Custom parameters and secrets allows you to add unique parameters and secure elements such as passwords

Creating a webhook

To create a Workload Security Webhook, go to Admin > Notifications and select "Workload Security Webhooks" tab. The following image shows a sample slack webhook creation screen.

Note: User must be a Workload Security *Admin* in order to create and manage Workload Security Webhooks.

Add a Webhook

Name
Test-Webhook-1

Template Type
Slack

URL ?
https://hooks.slack.com/services/<id>

Validate SSL Certificate for secure communication

Method
POST

Custom Header
Content-type: application/json
Accept: application/json

Message Body

```
{  
  "blocks": [  
    {  
      "type": "section",  
      "text": {  
        "type": "mrkdwn",  
        "text": "*%severity% Alert: %%synopsis%*"  
      }  
    },  
    {  
      "type": "divider"  
    }  
  ]  
}
```

Buttons
Cancel Test Webhook Create Webhook

- Enter appropriate information for each of the fields, and click "Save".
- You can also click the "Test Webhook" button to test the connection. Note that this will send the "Message Body" (without substitutions) to the defined URL according to the selected Method.
- SWS webhooks comprise a number of default parameters. Additionally, you can create your own custom parameters or secrets.

Parameters: What are they and how to use them?

Alert Parameters are dynamic values populated per alert. For example, the %%severity%% parameter will be replaced with the severity type of the alert.

Note that substitutions are not performed when clicking the "Test Webhook" button; the test sends a payload that shows the parameter's placeholders (%%<param-name>%%) but does not replace them with data.

Custom Parameters and Secrets

In this section you can add any custom parameters and/or secrets you wish. A custom parameter or secret can be in the URL or message body. Secrets allow user to configure a secure custom parameter like password, apiKey etc.

The following sample image shows how custom parameters are used in webhook creation.

Custom Parameter	Description
%%alertDetailsPageUrl%%	https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%
%%alertTimestamp%%	Alert timestamp in Epoch format (milliseconds)
%%changePercentage%%	Change Percentage
%%detected%%	Alert timestamp in GMT (Tue, 27 Oct 2020 01:20:30 GMT)
%%id%%	Alert ID
%%note%%	Note
%%severity%%	Alert severity
%%status%%	Alert status
%%synopsis%%	Alert Synopsis
%%type%%	Alert type
%%userId%%	User id
%%userName%%	User name
%%filesDeleted%%	Files deleted
%%encryptedFilesSuffix%%	Encrypted files suffix
%%filesEncrypted%%	Files encrypted

Workload Security Webhooks List Page

On the Webhooks list page, displayed are the Name, Created By, Created On, Status, Secure, and Last Reported fields.

Note: The value of 'status' column will keep changing based on the result of last webhook trigger result. The following are examples of status results.

Status	Description
OK	Successfully sent notification.
403	Forbidden.
404	URL not found.

400	Bad Request. You might see this status if there is any error in the message body, for example: <ul style="list-style-type: none"> • Badly formatted json. • Providing invalid value for reserved keys. For example, PagerDuty accepts only critical/warning/error/info for “Severity”. Any other result may yield a 400 status. • Application specific validation errors. For example, Slack allows a maximum of 10 fields inside a section. Including more than 10 may result in a 400 status.
410	Resource is no longer available

“Last Reported” column indicates the time when the webhook was last triggered.

From the webhooks listing page users can also Edit/Duplicate/Delete webhooks.

Configure Webhook notification in alert policy

To add a webhook notification to an alert policy, go to -Workload Security > Policies- and select an existing policy or add a new policy. In the *Actions* section > *Webhook Notifications* dropdown, select the required webhooks.

Edit Attack Policy

X

Policy Name*

For Attack Type(s) *

Ransomware Attack
 Data Destruction - File Deletion

On Device

+ Another Device

Actions

Take Snapshot ?
 Block User File Access ?

Time Period

▼

Webhooks Notifications

Test-Webhook-1

Cancel
Save

Webhook notifications are tied to policies. When the attack (RW/DD/WARN) happens, the action configured (Take snapshot / user blocking) will be taken and then the associated webhook notification will be triggered.

Note: Email notifications are independent of policies, they will be triggered as usual.

- If a policy is paused, webhook notifications will not be triggered.
- Multiple webhooks can be attached to a single policy but it is recommended to attach no more than 5 webhooks to a policy.

Workload Security Webhook Examples

Webhooks for [Slack](#)

Webhooks for [PagerDuty](#)

Webhooks for [Teams](#)

Webhooks for [Discord](#)

Workload Security Webhook Example for Discord

Webhooks allow users to send alert notifications to various applications using a customized webhook channel. This page provides an example for setting up webhooks for Discord.



This page refers to third-party instructions, which are subject to change. Refer to the [Discord documentation](#) for the most up-to-date information.

Discord Setup:

- In Discord, select the Server, under Text Channels, select Edit Channel (gear icon)
- Select **Integrations > View Webhooks** and click **New Webhook**
- Copy the Webhook URL. You will need to paste this into the Workload Security webhook configuration.

Create Workload Security Webhook:

1. Navigate to Admin > Notifications and select the *Workload Security Webhooks* tab. Click '+ Webhook' to create a new webhook.
2. Give the webhook a meaningful Name.
3. In the *Template Type* drop-down, select **Discord**.
4. Paste the Discord URL from above into the *URL* field.

Add a Webhook

Name

Template Type

URL

Validate SSL Certificate for secure communication

Method

Custom Header

```
Content-Type: application/json
Accept: application/json
```

Message Body

```
{
  "content": null,
  "embeds": [
    {
      "title": "%%severity%% | %%id%%",
      "description": "%%synopsis%%",
      "url": "https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%",
      "color": 3244733,
      "fields": [
        {
          "name": "%%",
          "value": "%%"
        }
      ]
    }
  ]
}
```

In order to test the webhook, temporarily replace the URL value in the message body with any valid URL (such as <https://netapp.com>) then click the *Test Webhook* button. Discord requires that a valid URL be supplied in order for Test Webhook functionality to work.

Be sure to set the message body back once the test completes.

Notifications via Webhook

To notify on events via webhook, navigate to *Workload Security > Policies*. Click on *+Attack Policy* or *+Warning Policy*.

- Enter a meaningful policy name.
- Select the required Attack Type(s), Devices to which policy should be attached, and required Actions.
- Under the *Webhooks Notifications* dropdown, select the required Discord webhooks and save.

Note: Webhooks can also be attached to existing policies by editing them.

Add Attack Policy



Policy Name*

For Attack Type(s) *

- Ransomware Attack
- Data Destruction - File Deletion

On Device

[+ Another Device](#)

Actions

- Take Snapshot [?](#)
- Block User File Access [?](#)

Time Period

Webhooks Notifications

Test-Webhook-1

[Cancel](#)[Save](#)

Workload Security Webhook Example for PagerDuty

Webhooks allow users to send alert notifications to various applications using a

customized webhook channel. This page provides an example for setting up webhooks for PagerDuty.



This page refers to third-party instructions, which are subject to change. Refer to the [PagerDuty documentation](#) for the most up-to-date information.

PagerDuty Setup:

1. In PagerDuty, navigate to **Services > Service Directory** and click on the **+New Service** button.
2. Enter a *Name* and select *Use our API directly*. Select *Add Service*.

Add a Service

A service may represent an application, component or team you wish to open incidents against.

General Settings

Name:

Description:

Integration Settings

Connect with one of PagerDuty's supported integrations, or create a custom integration through email or API. Alerts from a service from a supported integration or through the Events V2 API.

You can add more than one integration to a service, for example, one for monitoring alerts and one for change events.

Integration Type Select a tool

PagerDuty integrates with hundreds of tools, including monitoring tools, ticketing systems, code repositories, and deploy pipelines. This may involve configuration steps in the tool you are integrating with PagerDuty.

Integrate via email
If your monitoring tool can send email, it can integrate with PagerDuty using a custom email address.

Use our API directly
If you're writing your own integration, use our Events API. More information is in our developer documentation.

Events API v2

Don't use an integration
If you only want incidents to be manually created, You can always add additional integrations later.

3. Select the **Integrations** tab to see the **Integration Key**. You will need this key when you create the Workload Security webhook below.
1. Go to **Incidents** or **Services** to view Alerts.

Open Incidents (5)

					All statuses	Go to incident #	25 per page	1 - 5 of 5
Status	Priority	Urgency	Alerts	Title	Assigned To	Created		
<input type="checkbox"/> Acknowledged	High	1	Critical Alert: Ransomware attack from user account #403982 + SHOW DETAILS (1 triggered alert)	Chandan SS	Today at 4:11 AM			
<input type="checkbox"/> Acknowledged	High	1	Critical Alert: Data Destruction - File Deletion attack from user account #403996 + SHOW DETAILS (1 triggered alert)	Chandan SS	Today at 5:41 AM			

Create Workload Security PagerDuty Webhook:

- Navigate to Admin > Notifications and select the *Workload Security Webhooks* tab. Select '+ Webhook' to create a new webhook.
- Give the webhook a meaningful name.
- In the *Template Type* dropdown, select *PagerDuty Trigger*.
- Create a custom parameter secret named *routingKey* and set the value to the PagerDuty *Integration Key* created above.

Custom Parameters and Secrets ?

Name	Value ↑	Description
%%routingKey%%	*****	:

+ Parameter

Name ?	Value
routingKey	*****
Type	Description
Secret	

Cancel Save Parameter

Add a Webhook

Name
Test PagerDuty

Template Type
PagerDuty Trigger

URL 
https://events.pagerduty.com/%%pagerDutyId%%

Validate SSL Certificate for secure communication

Method
POST

Custom Header
Content-Type: application/json
Accept: application/json

Message Body

```
{
  "dedup_key": "%%id%%",
  "event_action": "trigger",
  "links": [
    {
      "href": "https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%",
      "text": "%%severity%% | %%id%% | %%detected%%"
    }
  ],
  "payload": {
    "severity": "%%severity%%"
  }
}
```

Buttons

[Cancel](#) [Test Webhook](#) [Create Webhook](#)

Notifications via Webhook

- To notify on events via webhook, navigate to *Workload Security > Policies*. Select *+Attack Policy* or *+Warning Policy*.
- Enter a meaningful policy name.
- Select required Attack Type(s), Devices to which the policy should be attached, and the required Actions.
- Under *Webhooks Notifications* dropdown, select the required PagerDuty webhooks. Save the policy.

Note: Webhooks can also be attached to existing policies by editing them.

Add Attack Policy

Policy Name*
Test policy 1

For Attack Type(s) *
 Ransomware Attack
 Data Destruction - File Deletion

On Device
All Devices

+ Another Device

Actions
 Take Snapshot ?
 Block User File Access ?

Time Period
12 hours

Webhooks Notifications
Please Select
Test-Webhook-1

Cancel Save

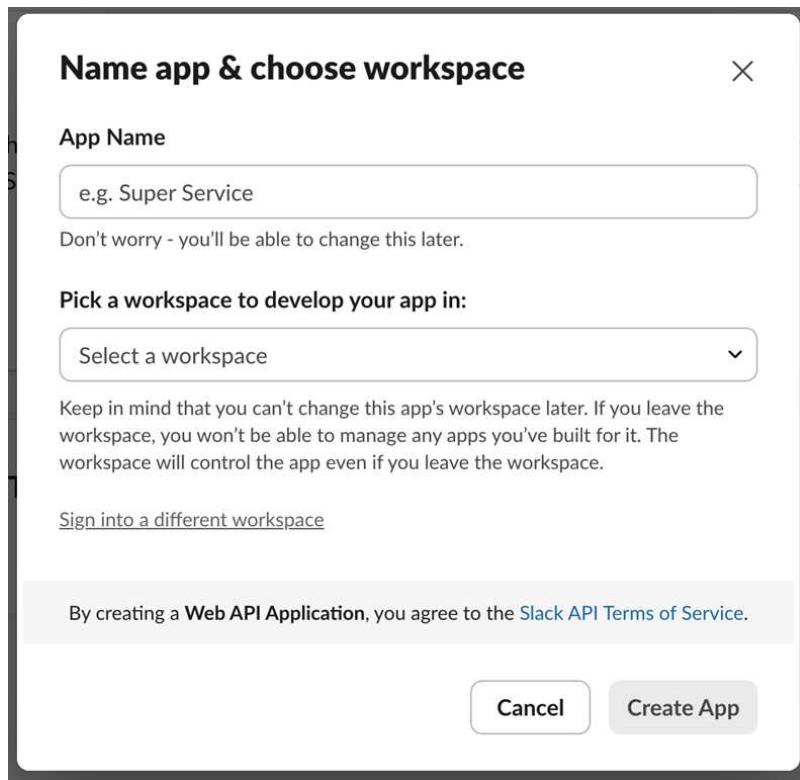
Workload Security Webhook Example for Slack

Webhooks allow users to send alert notifications to various applications using a customized webhook channel. This page provides an example for setting up webhooks for Slack.

This page refers to third-party instructions, which are subject to change. Refer to the Slack documentation for the most up-to-date information.

Slack Example

- Go to <https://api.slack.com/apps> and Create a new App. Give it a meaningful name and select a Workspace.



- Go to Incoming Webhooks, click on *Activate Incoming Webhooks*, select *Add New Webhook*, and select the Channel on which to Post.
- Copy the Webhook URL. This URL will be given when creating a Workload Security webhook.

Create Workload Security Slack Webhook

1. Navigate to Admin > Notifications and select the *Workload Security Webhooks* tab. Select *+ Webhook* to create a new webhook.
2. Give the webhook a meaningful name.
3. In the *Template Type* dropdown, select *Slack*.
4. Paste the URL copied from above.

Add a Webhook

Name
Test-Webhook-1

Template Type
Slack

URL 
https://hooks.slack.com/services/<id>

Validate SSL Certificate for secure communication

Method
POST

Custom Header
Content-type: application/json
Accept: application/json

Message Body

```
{  
  "blocks": [  
    {  
      "type": "section",  
      "text": {  
        "type": "mrkdwn",  
        "text": "*%severity%% Alert: %%synopsis%%*"  
      }  
    },  
    {  
      "type": "divider"  
    }  
  ]  
}
```

Buttons
Cancel **Test Webhook** **Create Webhook**

Notifications via webhook

- To notify on events via webhook, navigate to *Workload Security > Policies*. Click on *+Attack Policy* or *+Warning Policy*.
- Enter a meaningful policy name.
- Select required Attack Type(s), Devices to which the policy should be attached, and required Actions.
- Under the *Webhooks Notifications* dropdown, select the required webhooks. Save the policy.

Note: Webhooks can also be attached to existing policies by editing them.

Add Attack Policy

Policy Name*
Test policy 1

For Attack Type(s) *

Ransomware Attack
 Data Destruction - File Deletion

On Device

All Devices

+ Another Device

Actions

Take Snapshot [?](#)
 Block User File Access [?](#)

Time Period

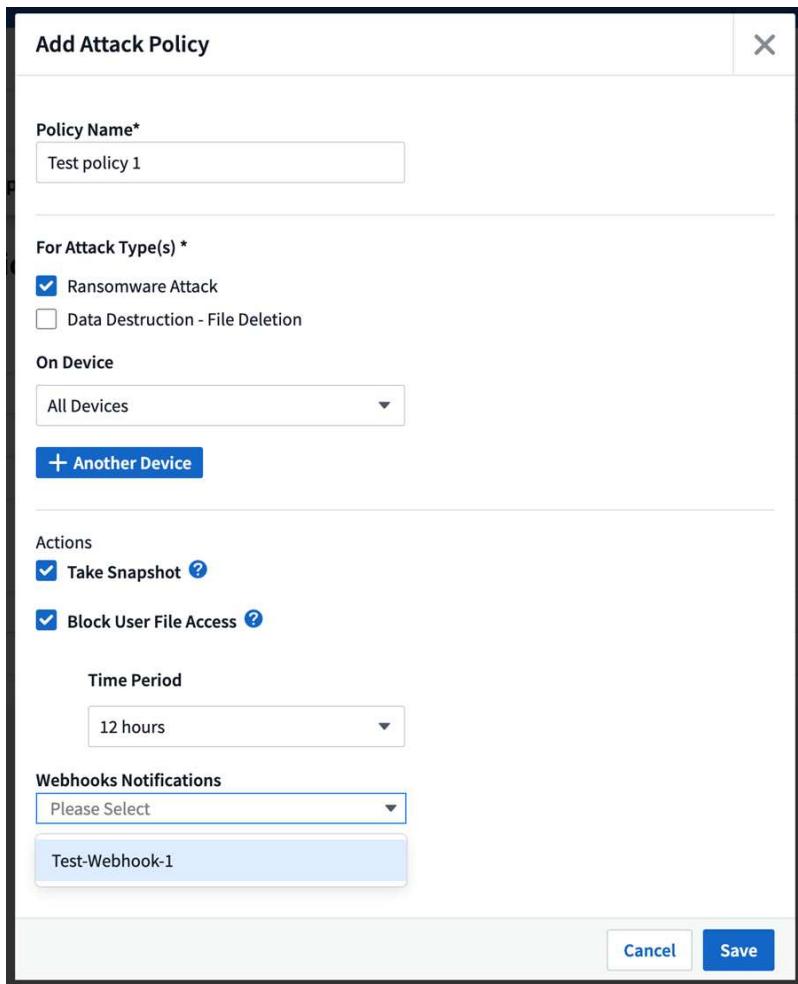
12 hours

Webhooks Notifications

Please Select

Test-Webhook-1

Cancel **Save**



Workload Security Webhook Example for Microsoft Teams

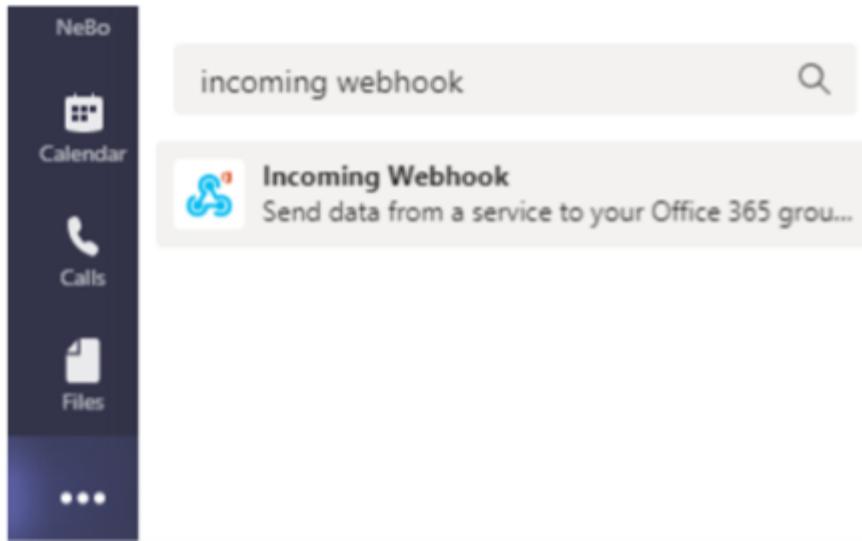
Webhooks allow users to send alert notifications to various applications using a customized webhook channel. This page provides an example for setting up webhooks for Teams.



This page refers to third-party instructions, which are subject to change. Refer to the [Teams documentation](#) for the most up-to-date information.

Teams Setup:

1. In Teams, select the kebab, and search for Incoming Webhook.



2. Select **Add to a Team > Select a Team > Setup a Connector**.
3. Copy the Webhook URL. You will need to paste this into the Workload Security webhook configuration.

Create Workload Security Teams Webhook:

1. Navigate to Admin > Notifications and select the "Workload Security Webhooks" tab. Select **+ Webhook** to create a new webhook.
2. Give the webhook a meaningful Name.
3. In the *Template Type* drop-down, select **Teams**.

Add a Webhook

Name

Template Type

URL

Validate SSL Certificate for secure communication

Method

Custom Header

```
Content-Type: application/json
Accept: application/json
```

Message Body

```
{
  "@type": "MessageCard",
  "@context": "http://schema.org/extensions",
  "themeColor": "0076D7",
  "summary": "%%severity%% Alert: %%synopsis%%",
  "sections": [
    {
      "activityTitle": "%%severity%% Alert: %%synopsis%%",
      "activitySubtitle": "%%detected%%",
      "markdown": false,
      "facts": [
        {
          "name": "Severity",
          "value": "%%severity%%"
        },
        {
          "name": "Detected At",
          "value": "%%detected%%"
        }
      ]
    }
  ]
}
```

4. Paste the URL from above into the *URL* field.

Notifications via Webhook

To notify on events via webhook, navigate to *Workload Security > Policies*. Select *+Attack Policy* or *+Warning Policy*.

- Enter a meaningful policy name.
- Select required Attack Type(s), Devices to which policy should be attached, and required Actions.

- Under the *Webhooks Notifications* dropdown, select the required Teams webhooks. Save the policy.

Note: Webhooks can also be attached to existing policies by editing them.

Add Attack Policy

Policy Name*
Test policy 1

For Attack Type(s) *
 Ransomware Attack
 Data Destruction - File Deletion

On Device
All Devices

Actions
 Take Snapshot ?
 Block User File Access ?

Time Period
12 hours

Webhooks Notifications
Please Select
Test-Webhook-1

Cancel **Save**

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.