



Notifiche webhook

Data Infrastructure Insights

NetApp
February 03, 2026

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

Sommario

Notifiche webhook	1
Notifiche di sicurezza del carico di lavoro tramite webhook	1
Creazione di un webhook	1
Parametri: cosa sono e come utilizzarli?	3
Pagina elenco webhook sicurezza carico di lavoro	3
Configurare la notifica Webhook nel criterio di avviso	4
Esempio di webhook di sicurezza del carico di lavoro per Discord	6
Configurazione Discord:	6
Crea webhook sulla sicurezza del carico di lavoro:	6
Notifiche tramite Webhook	8
Esempio di webhook di sicurezza del carico di lavoro per PagerDuty	10
Configurazione PagerDuty:	10
Crea webhook Workload Security PagerDuty:	11
Notifiche tramite Webhook	12
Esempio di webhook di sicurezza del carico di lavoro per Slack	14
Esempio di webhook di sicurezza del carico di lavoro per Microsoft Teams	18
Configurazione delle squadre:	18
Crea webhook per i team di sicurezza del carico di lavoro:	18
Notifiche tramite Webhook	19

Notifiche webhook

Notifiche di sicurezza del carico di lavoro tramite webhook

I webhook consentono agli utenti di inviare notifiche di avviso critiche o di avvertimento a varie applicazioni utilizzando un canale webhook personalizzato.

Molte applicazioni commerciali supportano i webhook come interfaccia di input standard, ad esempio: Slack, PagerDuty, Teams e Discord. Supportando un canale webhook generico e personalizzabile, Workload Security può supportare molti di questi canali di distribuzione. Le informazioni sulla configurazione dei webhook sono disponibili sui siti web delle rispettive applicazioni. Ad esempio, Slack fornisce "[questa guida utile](#)".

È possibile creare più canali webhook, ognuno dei quali è destinato a uno scopo diverso, ad applicazioni separate, a destinatari diversi, ecc.

L'istanza del canale webhook è composta dai seguenti elementi

Nome	Descrizione
URL	URL di destinazione del webhook, incluso il prefisso http:// o https:// insieme ai parametri URL
Metodo	GET/POST - Il valore predefinito è POST
Intestazione personalizzata	Specifica qui eventuali intestazioni personalizzate
Corpo del messaggio	Inserisci qui il corpo del tuo messaggio
Parametri di avviso predefiniti	Elenca i parametri predefiniti per il webhook
Parametri e segreti personalizzati	I parametri e i segreti personalizzati consentono di aggiungere parametri univoci ed elementi sicuri come le password

Creazione di un webhook

Per creare un webhook di sicurezza del carico di lavoro, vai su Amministrazione > Notifiche e seleziona la scheda "Webhook di sicurezza del carico di lavoro". L'immagine seguente mostra un esempio di schermata di creazione di un webhook Slack.

Nota: per creare e gestire i webhook di Workload Security, l'utente deve essere un amministratore di Workload Security.

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

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

CancelTest WebhookCreate Webhook

- Inserisci le informazioni appropriate per ciascun campo e fai clic su "Salva".
- Puoi anche cliccare sul pulsante "Test Webhook" per testare la connessione. Si noti che in questo modo verrà inviato il "Corpo del messaggio" (senza sostituzioni) all'URL definito in base al metodo selezionato.
- I webhook SWS comprendono una serie di parametri predefiniti. Inoltre, puoi creare parametri o segreti personalizzati.

Parametri: cosa sono e come utilizzarli?

I parametri di avviso sono valori dinamici popolati per avviso. Ad esempio, il parametro `%%severity%%` verrà sostituito con il tipo di gravità dell'avviso.

Si noti che le sostituzioni non vengono eseguite quando si fa clic sul pulsante "Test Webhook"; il test invia un payload che mostra i segnaposto del parametro (`%%<param-name>%%`) ma non li sostituisce con i dati.

Parametri e segreti personalizzati

In questa sezione puoi aggiungere tutti i parametri personalizzati e/o segreti che desideri. Un parametro personalizzato o un segreto può essere presente nell'URL o nel corpo del messaggio. I segreti consentono all'utente di configurare un parametro personalizzato sicuro come password, apiKey ecc.

L'immagine di esempio seguente mostra come vengono utilizzati i parametri personalizzati nella creazione di webhook.

The screenshot shows the 'Add Webhook' configuration interface. On the left, there are fields for 'Template Type' (Slack), 'URL' (https://hooks.slack.com/services/%%slack-id%%), 'Method' (POST), and 'Custom Header' (Content-type: application/json, Accept: application/json). On the right, a table lists various alert parameters and their descriptions. Below the table, a 'Message Body' field contains JSON code with placeholder values like '%%status%%' and '%%slack-id%%'. A red box highlights the '%%slack-id%%' placeholder in the URL and its definition in the table. A red box also highlights the '%%slack-id%%' placeholder in the message body and its definition in the table. At the bottom, there are 'Cancel', 'Test Webhook', and 'Create Webhook' buttons, and a 'Custom Parameters and Secrets' section containing two entries: '%%webhookConfiguredBy%' with value 'system_admin_1' and '%%slack-id%%' with value '*****'. A red box highlights this entire section.

%%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

Pagina elenco webhook sicurezza carico di lavoro

Nella pagina dell'elenco dei webhook vengono visualizzati i campi Nome, Creato da, Creato il, Stato, Sicuro e Ultimo segnalato. Nota: il valore della colonna "stato" continuerà a cambiare in base al risultato dell'ultimo trigger del webhook. Di seguito sono riportati alcuni esempi di risultati di stato.

Stato	Descrizione
OK	Notifica inviata correttamente.
403	Vietato.

404	URL non trovato.
400	<p>Brutta richiesta. Potresti visualizzare questo stato se c'è un errore nel corpo del messaggio, ad esempio:</p> <ul style="list-style-type: none"> • JSON formattato male. • Fornito valore non valido per le chiavi riservate. Ad esempio, PagerDuty accetta solo informazioni critiche/avviso/errore/informazioni per "Gravità". Qualsiasi altro risultato potrebbe comportare lo stato 400. • Errori di convalida specifici dell'applicazione. Ad esempio, Slack consente un massimo di 10 campi all'interno di una sezione. Includerne più di 10 può comportare lo stato 400.
410	La risorsa non è più disponibile

La colonna "Ultimo segnalato" indica l'ora in cui il webhook è stato attivato l'ultima volta.

Dalla pagina dell'elenco dei webhook gli utenti possono anche modificare/duplicare/eliminare i webhook.

Configurare la notifica Webhook nel criterio di avviso

Per aggiungere una notifica webhook a un criterio di avviso, vai su -Sicurezza del carico di lavoro > Criteri- e seleziona un criterio esistente o aggiungine uno nuovo. Nella sezione *Azioni* > menu a discesa *Notifiche webhook*, seleziona i webhook richiesti.

Edit 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](#)

Le notifiche webhook sono collegate alle policy. Quando si verifica l'attacco (RW/DD/WARN), verrà eseguita l'azione configurata (Scatta snapshot/blocco utente) e verrà quindi attivata la notifica webhook associata.

Nota: le notifiche e-mail sono indipendenti dalle policy e verranno attivate come di consueto.

- Se una policy viene sospesa, le notifiche webhook non verranno attivate.
- È possibile associare più webhook a una singola policy, ma si consiglia di non associarne più di 5.

Esempi di webhook sulla sicurezza del carico di lavoro

Webhook per "[Slack](#)"

Webhook per "[PagerDuty](#)" Webhook per "[Squadre](#)" Webhook per "[Discordia](#)"

Esempio di webhook di sicurezza del carico di lavoro per Discord

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per Discord.



Questa pagina fa riferimento a istruzioni di terze parti, che sono soggette a modifiche. Fare riferimento al "[Documentazione Discord](#)" per le informazioni più aggiornate.

Configurazione Discord:

- In Discord, seleziona il server, in Canali di testo, seleziona Modifica canale (icona a forma di ingranaggio)
- Seleziona **Integrazioni > Visualizza webhook** e fai clic su **Nuovo webhook**
- Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Workload Security.

Crea webhook sulla sicurezza del carico di lavoro:

1. Vai su Amministrazione > Notifiche e seleziona la scheda *Webhook di sicurezza del carico di lavoro*. Fare clic su '+ Webhook' per creare un nuovo webhook.
2. Assegnare al webhook un nome significativo.
3. Nel menu a discesa *Tipo di modello*, seleziona **Discord**.
4. Incolla l'URL di Discord riportato sopra nel campo *URL*.

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": "%%"  
        }  
      ]  
    }  
  ]  
}
```

Per testare il webhook, sostituisci temporaneamente il valore URL nel corpo del messaggio con un URL valido (ad esempio <https://netapp.com>), quindi fai clic sul pulsante *Test Webhook*. Per far funzionare la funzionalità Test Webhook, Discord richiede che venga fornito un URL valido.

Una volta completato il test, assicurati di reimpostare il corpo del messaggio.

Notifiche tramite Webhook

Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro > Criteri*. Fare clic su *+Criterio di attacco* o *+Criterio di avviso*.

- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui associare la policy e le azioni richieste.
- Nel menu a discesa *Notifiche webhook*, seleziona i webhook Discord desiderati e salva.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.

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

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

Esempio di webhook di sicurezza del carico di lavoro per PagerDuty

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per PagerDuty.



Questa pagina fa riferimento a istruzioni di terze parti, soggette a modifiche. Fare riferimento all'["Documentazione PagerDuty"](#) per le informazioni più aggiornate.

Configurazione PagerDuty:

1. In PagerDuty, vai su **Servizi > Directory dei servizi** e clicca sul pulsante **+Nuovo servizio**.
2. Inserisci un *Nome* e seleziona *Usa direttamente la nostra API*. Selezionare *Aggiungi servizio*.

The screenshot shows the 'Add a Service' form. At the top, there's a note: 'A service may represent an application, component or team you wish to open incidents against.' Below it, the 'General Settings' section has fields for 'Name' and 'Description'. The 'Integration Settings' section is expanded, showing options for 'Integration Type':

- Select a tool: A tooltip explains that PagerDuty integrates with many tools like monitoring, ticketing, and deployment systems.
- Integrate via email: A tooltip says it's for tools that send email.
- Use our API directly: A tooltip says it's for custom integrations using the Events API.
- Don't use an integration: A tooltip says incidents will be manually created.

A dropdown menu below the integration type shows 'Events API v2'.

3. Selezionare la scheda *Integrazioni* per visualizzare la **Chiave di integrazione**. Questa chiave ti servirà quando creerai il webhook Workload Security qui sotto.
4. Vai a **Incidenti** o **Servizi** per visualizzare gli avvisi.

Open Incidents (5)

<input type="checkbox"/> Status	Priority	Urgency	Alerts	Title	Assigned To	Created
<input type="checkbox"/> Acknowledged	High	1		Critical Alert: Ransomware attack from user [REDACTED] 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 [REDACTED] account #403996 + SHOW DETAILS (1 triggered alert)	Chandan SS	Today at 5:41 AM

Crea webhook Workload Security PagerDuty:

- Vai su Amministrazione > Notifiche e seleziona la scheda *Webhook di sicurezza del carico di lavoro*. Selezionare '+ Webhook' per creare un nuovo webhook.
- Assegnare al webhook un nome significativo.
- Nel menu a discesa *Tipo di modello*, seleziona *Trigger PagerDuty*.
- Crea un parametro segreto personalizzato denominato *routingKey* e imposta il valore sulla *Chiave di integrazione* PagerDuty creata in precedenza.

Custom Parameters and Secrets 

Name	Value ↑	Description
%&%routingKey%&%	*****	

 Parameter

Name 	Value
<input type="text" value="routingKey"/>	<input type="text" value="*****"/>
Type	Description
<input type="text" value="Secret"/>	<input type="text"/>

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": {
    "user": "00000000000000000000"
  }
}
```

Cancel**Test Webhook****Create Webhook****Notifiche tramite Webhook**

- Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro > Criteri*. Selezionare *+Criterio di attacco* o *+Criterio di avviso*.
- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui deve essere associata la policy e le azioni richieste.
- Nel menu a discesa *Notifiche webhook*, seleziona i webhook PagerDuty desiderati. Salva la polizza.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.

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

Esempio di webhook di sicurezza del carico di lavoro per Slack

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per Slack.

Questa pagina fa riferimento a istruzioni di terze parti, soggette a modifiche. Per informazioni più aggiornate, consultare la documentazione di Slack.

Esempio di Slack

- Vai a <https://api.slack.com/apps> e crea una nuova app. Assegnagli un nome significativo e seleziona un'area di lavoro.

Name app & choose workspace

X

App Name

e.g. Super Service

Don't worry - you'll be able to change this later.

Pick a workspace to develop your app in:

Select a workspace



Keep in mind that you can't change this app's workspace later. If you leave the workspace, you won't be able to manage any apps you've built for it. The workspace will control the app even if you leave the workspace.

[Sign into a different workspace](#)

By creating a **Web API Application**, you agree to the [Slack API Terms of Service](#).

Cancel

Create App

- Vai a Webhook in arrivo, clicca su *Attiva webhook in arrivo*, seleziona *Aggiungi nuovo webhook* e seleziona il canale su cui pubblicare.
- Copia l'URL del webhook. Questo URL verrà fornito durante la creazione di un webhook di Workload Security.

Crea un webhook Slack per la sicurezza del carico di lavoro

1. Vai su Amministrazione > Notifiche e seleziona la scheda *Webhook di sicurezza del carico di lavoro*. Selezionare + *Webhook* per creare un nuovo webhook.
2. Assegnare al webhook un nome significativo.
3. Nel menu a discesa *Tipo di modello*, seleziona *Slack*.
4. Incolla l'URL copiato sopra.

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

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

CancelTest WebhookCreate Webhook

Notifiche tramite webhook

- Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro > Criteri*. Fare clic su *+Criterio di attacco* o *+Criterio di avviso*.
- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui deve essere associata la policy e le azioni richieste.
- Nel menu a discesa *Notifiche webhook*, seleziona i webhook desiderati. Salva la polizza.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.

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

Esempio di webhook di sicurezza del carico di lavoro per Microsoft Teams

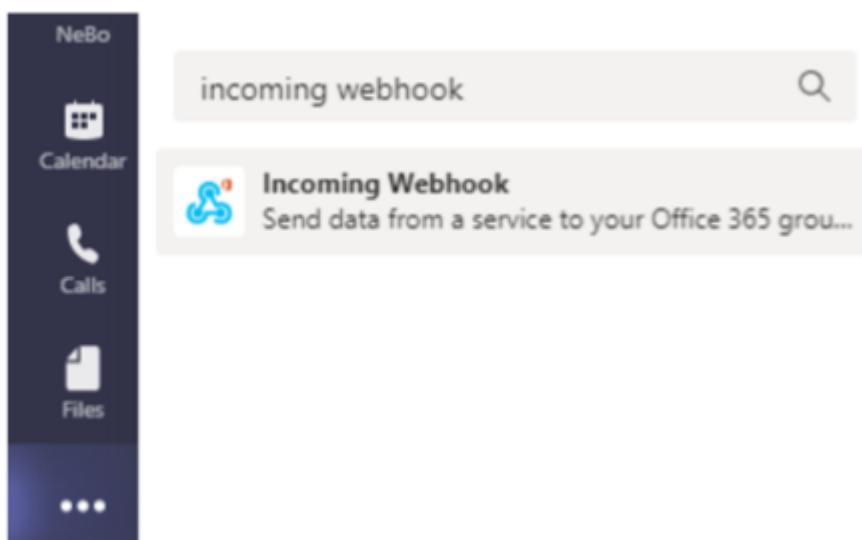
I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per la configurazione di webhook per Teams.



Questa pagina fa riferimento a istruzioni di terze parti, soggette a modifiche. Fare riferimento all'["Documentazione dei team"](#) per le informazioni più aggiornate.

Configurazione delle squadre:

1. In Teams, seleziona il kebab e cerca Webhook in arrivo.



2. Seleziona **Aggiungi a un team > Seleziona un team > Imposta un connettore**.
3. Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Workload Security.

Crea webhook per i team di sicurezza del carico di lavoro:

1. Vai su Amministrazione > Notifiche e seleziona la scheda "Webhook di sicurezza del carico di lavoro". Selezionare + *Webhook* per creare un nuovo webhook.
2. Assegnare al webhook un nome significativo.
3. Nel menu a discesa *Tipo di modello*, seleziona **Team**.

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": [
```

4. Incolla l'URL sopra nel campo *URL*.

Notifiche tramite Webhook

Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro > Criteri*. Selezionare *+Criterio di attacco* o *+Criterio di avviso*.

- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui deve essere associata la policy e le azioni richieste.

- Nel menu a discesa *Notifiche webhook*, seleziona i webhook di Teams desiderati. Salva la polizza.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.

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**

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.