



# **Notificaciones de webhook**

## **Data Infrastructure Insights**

NetApp

February 11, 2026

This PDF was generated from [https://docs.netapp.com/es-es/data-infrastructure-insights/ws\\_notifications\\_using\\_webhooks.html](https://docs.netapp.com/es-es/data-infrastructure-insights/ws_notifications_using_webhooks.html) on February 11, 2026. Always check docs.netapp.com for the latest.

# Tabla de contenidos

- Notificaciones de webhook. . . . . 1
  - Notificaciones de seguridad de la carga de trabajo mediante webhooks . . . . . 1
    - Creando un webhook . . . . . 1
    - Parámetros: ¿Qué son y cómo utilizarlos? . . . . . 3
    - Página de lista de webhooks de seguridad de carga de trabajo . . . . . 3
    - Configurar la notificación de webhook en la política de alertas . . . . . 4
  - Ejemplo de webhook de seguridad de carga de trabajo para Discord . . . . . 6
    - Configuración de Discord: . . . . . 6
    - Crear un webhook de seguridad de carga de trabajo: . . . . . 6
    - Notificaciones mediante webhook . . . . . 8
  - Ejemplo de webhook de seguridad de carga de trabajo para PagerDuty . . . . . 10
    - Configuración de PagerDuty: . . . . . 10
    - Crear un webhook de PagerDuty para la seguridad de la carga de trabajo: . . . . . 11
    - Notificaciones mediante webhook . . . . . 12
  - Ejemplo de webhook de seguridad de carga de trabajo para Slack . . . . . 14
  - Ejemplo de webhook de seguridad de carga de trabajo para Microsoft Teams . . . . . 18
    - Configuración de los equipos: . . . . . 18
    - Crear webhook de equipos de seguridad de carga de trabajo: . . . . . 18
    - Notificaciones mediante webhook . . . . . 21

# Notificaciones de webhook

## Notificaciones de seguridad de la carga de trabajo mediante webhooks

Los webhooks permiten a los usuarios enviar notificaciones de alerta críticas o de advertencia a varias aplicaciones utilizando un canal webhook personalizado.

Muchas aplicaciones comerciales admiten webhooks como interfaz de entrada estándar, por ejemplo: Slack, PagerDuty, Teams y Discord. Al admitir un canal webhook genérico y personalizable, Workload Security puede admitir muchos de estos canales de entrega. Puede encontrar información sobre la configuración de los webhooks en los sitios web de las respectivas aplicaciones. Por ejemplo, Slack ofrece ["Esta útil guía"](#).

Puede crear múltiples canales webhook, cada uno destinado a un propósito diferente, aplicaciones independientes, diferentes destinatarios, etc.

La instancia del canal webhook se compone de los siguientes elementos

Nombre	Descripción
URL	URL de destino del webhook, incluido el prefijo http:// o https:// junto con los parámetros de la URL
Método	GET/POST - El valor predeterminado es POST
Encabezado personalizado	Especifique aquí cualquier encabezado personalizado
Cuerpo del mensaje	Coloque el cuerpo de su mensaje aquí
Parámetros de alerta predeterminados	Enumera los parámetros predeterminados para el webhook
Parámetros y secretos personalizados	Los parámetros y secretos personalizados le permiten agregar parámetros únicos y elementos seguros como contraseñas.

### Creando un webhook

Para crear un webhook de seguridad de carga de trabajo, vaya a Admin > Notificaciones y seleccione la pestaña "Webhooks de seguridad de carga de trabajo". La siguiente imagen muestra un ejemplo de pantalla de creación de webhook de Slack.

Nota: El usuario debe ser un *Admin* de seguridad de carga de trabajo para poder crear y administrar webhooks de seguridad de carga de trabajo.

## 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"
    }
  ]
}
```

Cancel

Test Webhook

Create Webhook

- Ingrese la información adecuada para cada uno de los campos y haga clic en "Guardar".
- También puede hacer clic en el botón "Probar webhook" para probar la conexión. Tenga en cuenta que esto enviará el "Cuerpo del mensaje" (sin sustituciones) a la URL definida según el método seleccionado.
- Los webhooks de SWS comprenden una serie de parámetros predeterminados. Además, puedes crear tus propios parámetros o secretos personalizados.

## Parámetros: ¿Qué son y cómo utilizarlos?

Los parámetros de alerta son valores dinámicos que se completan por cada alerta. Por ejemplo, el parámetro `%%severity%%` se reemplazará con el tipo de gravedad de la alerta.

Tenga en cuenta que no se realizan sustituciones al hacer clic en el botón "Probar webhook"; la prueba envía una carga útil que muestra los marcadores de posición del parámetro (`%%<param-name>%%`) pero no los reemplaza con datos.

### Parámetros y secretos personalizados

En esta sección puedes agregar cualquier parámetro personalizado y/o secretos que desees. Un parámetro personalizado o secreto puede estar en la URL o en el cuerpo del mensaje. Los secretos permiten al usuario configurar un parámetro personalizado seguro como contraseña, apiKey, etc.

La siguiente imagen de muestra muestra cómo se utilizan los parámetros personalizados en la creación de webhooks.

/ Notifications / Add Webhook

Template Type  
Slack

URL  
`https://hooks.slack.com/services/%%slack-id%%`

☒ Validate SSL Certificate for secure communication

Method  
POST

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

Message Body  

```
{
  "text": "Status: %%status%%",
  "type": "mrkdwn",
  "text": "Configured by: %%webhookConfiguredBy%%"
}
```

Cancel Test Webhook Create Webhook

%%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

Custom Parameters and Secrets

Name	Value	Description
%%webhookConfiguredBy%%	system_admin_1	
%%slack-id%%	*****	

+ Parameter

## Página de lista de webhooks de seguridad de carga de trabajo

En la página de lista de Webhooks, se muestran los campos Nombre, Creado por, Creado el, Estado, Seguro y Último informe. Nota: El valor de la columna 'estado' seguirá cambiando según el resultado del último activador del webhook. Los siguientes son ejemplos de resultados de estado.

Estado	Descripción
DE ACUERDO	Notificación enviada exitosamente.
403	Prohibido.

404	URL no encontrada.
400	<p>Solicitud incorrecta. Es posible que vea este estado si hay algún error en el cuerpo del mensaje, por ejemplo:</p> <ul style="list-style-type: none"> <li>• Json mal formateado.</li> <li>• Proporcionar valor no válido para claves reservadas. Por ejemplo, PagerDuty solo acepta información/advertencia/error/crítico para “Gravedad”. Cualquier otro resultado puede producir un estado 400.</li> <li>• Errores de validación específicos de la aplicación. Por ejemplo, Slack permite un máximo de 10 campos dentro de una sección. Incluir más de 10 puede dar como resultado un estado 400.</li> </ul>
410	El recurso ya no está disponible

La columna “Último informe” indica el momento en que se activó el webhook por última vez.

Desde la página de listado de webhooks, los usuarios también pueden editar, duplicar y eliminar webhooks.

## Configurar la notificación de webhook en la política de alertas

Para agregar una notificación de webhook a una política de alerta, vaya a -Seguridad de carga de trabajo > Políticas- y seleccione una política existente o agregue una nueva. En la sección *Acciones* > menú desplegable *Notificaciones de webhook*, seleccione los webhooks necesarios.

## Edit Attack Policy

Policy Name\*

Test-attack-policy

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

Las notificaciones de webhook están vinculadas a las políticas. Cuando ocurre el ataque (RW/DD/WARN), se tomará la acción configurada (Tomar instantánea/bloqueo de usuario) y luego se activará la notificación de webhook asociada.

Nota: Las notificaciones por correo electrónico son independientes de las políticas y se activarán como de costumbre.

- Si se pausa una política, no se activarán las notificaciones de webhook.
- Se pueden adjuntar varios webhooks a una sola política, pero se recomienda no adjuntar más de 5 webhooks a una política.

## Ejemplos de webhooks de seguridad de carga de trabajo

Webhooks para ["Flojo"](#)

Webhooks para ["PagerDuty"](#) Webhooks para ["Equipos"](#) Webhooks para ["Discordia"](#)

## Ejemplo de webhook de seguridad de carga de trabajo para Discord

Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un ejemplo para configurar webhooks para Discord.



Esta página hace referencia a instrucciones de terceros, que están sujetas a cambios. Consulte la ["Documentación de Discord"](#) para obtener la información más actualizada.

### Configuración de Discord:

- En Discord, selecciona el Servidor, en Canales de texto, selecciona Editar canal (ícono de engranaje)
- Seleccione **Integraciones > Ver webhooks** y haga clic en **Nuevo webhook**
- Copiar la URL del webhook. Necesitará pegar esto en la configuración del webhook de seguridad de carga de trabajo.

### Crear un webhook de seguridad de carga de trabajo:

1. Vaya a Admin > Notificaciones y seleccione la pestaña *Webhooks de seguridad de carga de trabajo*. Haga clic en "+ Webhook" para crear un nuevo webhook.
2. Dale al webhook un nombre significativo.
3. En el menú desplegable *Tipo de plantilla*, seleccione **Discord**.
4. Pegue la URL de Discord de arriba en el campo *URL*.

## Add a Webhook

### Name

Discord webhook

### Template Type

Discord

### URL ?

https://discord.com/api/webhooks/%%discord-id%%

☒ Validate SSL Certificate for secure communication

### Method

POST

### 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": "User"
```

Cancel

Test Webhook

Create Webhook

Para probar el webhook, reemplace temporalmente el valor de la URL en el cuerpo del mensaje con cualquier URL válida (como <https://netapp.com>) y luego haga clic en el botón *Probar webhook*. Discord requiere que se proporcione una URL válida para que la funcionalidad de prueba webhook funcione.

Asegúrese de volver a configurar el cuerpo del mensaje una vez que se complete la prueba.

## Notificaciones mediante webhook

Para notificar eventos a través de webhook, navegue a *Seguridad de carga de trabajo > Políticas*. Haga clic en *+Política de ataque* o *+Política de advertencia*.

- Introduzca un nombre de política significativo.
- Seleccione los tipos de ataque requeridos, los dispositivos a los que se debe adjuntar la política y las acciones requeridas.
- En el menú desplegable *Notificaciones de webhooks*, seleccione los webhooks de Discord necesarios y guárdelos.

Nota: Los webhooks también se pueden adjuntar a políticas existentes editándolas.

## 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

# Ejemplo de webhook de seguridad de carga de trabajo para PagerDuty

Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un ejemplo para configurar webhooks para PagerDuty.



Esta página hace referencia a instrucciones de terceros, que están sujetas a cambios. Consulte la ["Documentación de PagerDuty"](#) para obtener la información más actualizada.

## Configuración de PagerDuty:

1. En PagerDuty, navegue a **Servicios > Directorio de servicios** y haga clic en el botón **+Nuevo servicio**.
2. Ingrese un *Nombre* y seleccione *Usar nuestra API directamente*. Seleccione *Agregar servicio*.

**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.

☐ Don't use an integration

If you only want incidents to be manually created. You can always add additional integrations later.

3. Seleccione la pestaña *Integraciones* para ver la **Clave de integración**. Necesitará esta clave cuando cree el webhook de seguridad de carga de trabajo a continuación.
4. Vaya a **Incidentes** o **Servicios** para ver las alertas.

Activity	Integrations	Workflows	Settings	Service Dependencies
----------	--------------	-----------	----------	----------------------

**Open Incidents (5)**

! Acknowledge ✓ Resolve Snooze Merge Incidents All statuses Go to incident # 25 per page 1 - 5 of 5

<input type="checkbox"/>	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

## Crear un webhook de PagerDuty para la seguridad de la carga de trabajo:

- Vaya a Admin > Notificaciones y seleccione la pestaña *Webhooks de seguridad de carga de trabajo*. Seleccione '+ Webhook' para crear un nuevo webhook.
- Dale al webhook un nombre significativo.
- En el menú desplegable *Tipo de plantilla*, seleccione *Activador PagerDuty*.
- Cree un parámetro secreto personalizado llamado *routingKey* y establezca el valor en la clave de integración de PagerDuty *Integration Key* creada anteriormente.

## Custom Parameters and Secrets ⓘ

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

+ Parameter

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

Cancel

Save Parameter

## Add a Webhook

**Name****Template Type****URL** ☒ Validate SSL Certificate for secure communication**Method****Custom Header**  
**Message Body**

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

## Notificaciones mediante webhook

- Para notificar eventos a través de webhook, navegue a *Seguridad de carga de trabajo > Políticas*. Seleccione *+Política de ataque* o *+Política de advertencia*.
- Introduzca un nombre de política significativo.
- Seleccione los tipos de ataque requeridos, los dispositivos a los que se debe adjuntar la política y las acciones requeridas.
- En el menú desplegable *Notificaciones de webhooks*, seleccione los webhooks de PagerDuty necesarios. Guardar la política.

Nota: Los webhooks también se pueden adjuntar a políticas existentes editándolas.

## 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

# Ejemplo de webhook de seguridad de carga de trabajo para Slack

Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un ejemplo para configurar webhooks para Slack.

Esta página hace referencia a instrucciones de terceros, que están sujetas a cambios. Consulte la documentación de Slack para obtener la información más actualizada.

## Ejemplo de holgura

- Ir a <https://api.slack.com/apps> y crea una nueva aplicación. Asígnele un nombre significativo y seleccione un espacio de trabajo.

## Name app & choose workspace



### 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

- Vaya a Webhooks entrantes, haga clic en *Activar webhooks entrantes*, seleccione *Agregar nuevo webhook* y seleccione el canal en el que desea publicar.
- Copiar la URL del webhook. Esta URL se proporcionará al crear un webhook de seguridad de carga de trabajo.

#### Crear un webhook de Slack para la seguridad de la carga de trabajo

1. Vaya a Admin > Notificaciones y seleccione la pestaña *Webhooks de seguridad de carga de trabajo*. Seleccione + *Webhook* para crear un nuevo webhook.
2. Dale al webhook un nombre significativo.
3. En el menú desplegable *Tipo de plantilla*, seleccione *Slack*.
4. Pegue la URL copiada arriba.

## 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"
    }
  ]
}
```

Cancel

Test Webhook

Create Webhook

### Notificaciones mediante webhook

- Para notificar eventos a través de webhook, navegue a *Seguridad de carga de trabajo > Políticas*. Haga clic en *+Política de ataque* o *+Política de advertencia*.
- Introduzca un nombre de política significativo.
- Seleccione los tipos de ataque requeridos, los dispositivos a los que se debe adjuntar la política y las acciones requeridas.

- En el menú desplegable *Notificaciones de webhooks*, seleccione los webhooks necesarios. Guardar la política.

Nota: Los webhooks también se pueden adjuntar a políticas existentes editándolas.

## 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

# Ejemplo de webhook de seguridad de carga de trabajo para Microsoft Teams

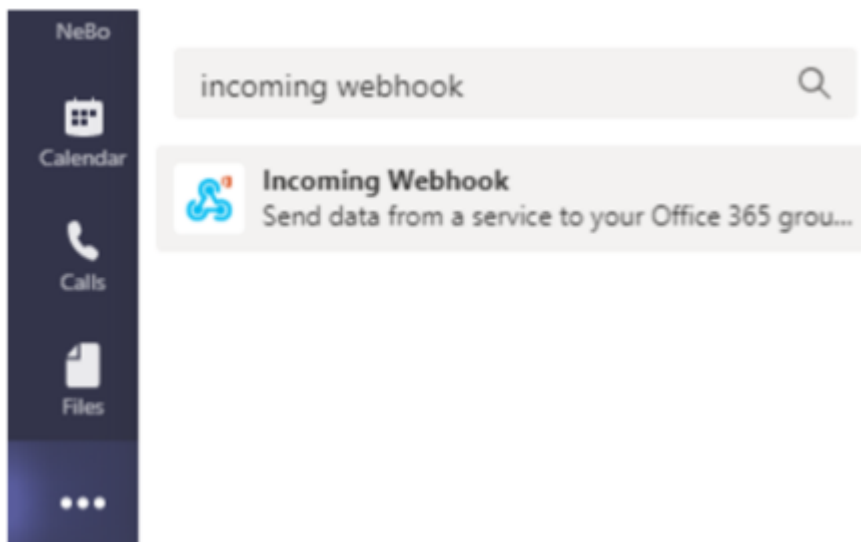
Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un ejemplo para configurar webhooks para Teams.



Esta página hace referencia a instrucciones de terceros, que están sujetas a cambios. Consulte la ["Documentación de Teams"](#) para obtener la información más actualizada.

## Configuración de los equipos:

1. En Teams, seleccione el kebab y busque Webhook entrante.



2. Seleccione **Agregar a un equipo > Seleccionar un equipo > Configurar un conector**.
3. Copiar la URL del webhook. Necesitará pegar esto en la configuración del webhook de seguridad de carga de trabajo.

## Crear webhook de equipos de seguridad de carga de trabajo:

1. Vaya a Admin > Notificaciones y seleccione la pestaña *"Webhooks de seguridad de carga de trabajo"*. Seleccione **+ Webhook** para crear un nuevo webhook.
2. Dale al webhook un nombre significativo.
3. En el menú desplegable *Tipo de plantilla*, seleccione **Equipos**.

## Add a Webhook

### Name

Teams Webhook

### Template Type

Teams

### URL

https://netapp.webhook.office.com/webhook/<id>

☒ Validate SSL Certificate for secure communication

### Method

POST

### 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": [
```

Cancel

Test Webhook

Create Webhook

4. Pegue la URL de arriba en el campo *URL*.

### Pasos para crear una notificación de Teams con la plantilla de tarjeta adaptable

1. Reemplaza el cuerpo del mensaje con la siguiente plantilla:

```
{
  "type": "message",
```

```

"attachments": [
  {
    "contentType": "application/vnd.microsoft.card.adaptive",
    "content": {
      "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
      "type": "AdaptiveCard",
      "version": "1.2",
      "body": [
        {
          "type": "TextBlock",
          "text": "%%severity%% Alert: %%synopsis%%",
          "wrap": true,
          "weight": "Bolder",
          "size": "Large"
        },
        {
          "type": "TextBlock",
          "text": "%%detected%%",
          "wrap": true,
          "isSubtle": true,
          "spacing": "Small"
        },
        {
          "type": "FactSet",
          "facts": [
            {
              "title": "User",
              "value": "%%userName%%"
            },
            {
              "title": "Attack/Abnormal Behavior",
              "value": "%%type%%"
            },
            {
              "title": "Action taken",
              "value": "%%actionTaken%%"
            },
            {
              "title": "Files encrypted",
              "value": "%%filesEncrypted%%"
            },
            {
              "title": "Encrypted files suffix",
              "value": "%%encryptedFilesSuffix%%"
            },
            {

```

```

        "title": "Files deleted",
        "value": "%%filesDeleted%%"
    },
    {
        "title": "Activity Change Rate",
        "value": "%%changePercentage%%"
    },
    {
        "title": "Severity",
        "value": "%%severity%%"
    },
    {
        "title": "Status",
        "value": "%%status%%"
    },
    {
        "title": "Notes",
        "value": "%%note%%"
    }
]
}
],
"actions": [
    {
        "type": "Action.OpenUrl",
        "title": "View Details",
        "url":
"https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%"
    }
]
}
]
}

```

2. Si usas Power Automate Flows, los parámetros de consulta en la URL están en formato codificado. Debes decodificar la URL antes de ingresarla.
3. Haz clic en "Probar Webhook" para asegurarte de que no hay errores.
4. Guarda el webhook.

## Notificaciones mediante webhook

Para notificar eventos a través de webhook, navegue a *Seguridad de carga de trabajo > Políticas*. Seleccione *+Política de ataque* o *+Política de advertencia*.

- Introduzca un nombre de política significativo.

- Seleccione los tipos de ataque requeridos, los dispositivos a los que se debe adjuntar la política y las acciones requeridas.
- En el menú desplegable *Notificaciones de webhooks*, seleccione los webhooks de Teams necesarios. Guardar la política.

Nota: Los webhooks también se pueden adjuntar a políticas existentes editándolas.

## 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

## Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.