



# **Notificações de webhook**

## **Data Infrastructure Insights**

NetApp

February 11, 2026

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



# Índice

Notificações de webhook .....	1
Notificações de segurança de carga de trabalho usando webhooks .....	1
Criando um webhook .....	1
Parâmetros: O que são e como usá-los? .....	3
Página da lista de webhooks de segurança de carga de trabalho .....	3
Configurar notificação de Webhook na política de alerta .....	4
Exemplo de webhook de segurança de carga de trabalho para Discord .....	6
Configuração do Discord: .....	6
Criar Webhook de Segurança de Carga de Trabalho: .....	6
Notificações via Webhook .....	8
Exemplo de webhook de segurança de carga de trabalho para PagerDuty .....	10
Configuração do PagerDuty: .....	10
Criar Webhook do PagerDuty de Segurança de Carga de Trabalho: .....	11
Notificações via Webhook .....	12
Exemplo de webhook de segurança de carga de trabalho para Slack .....	14
Exemplo de webhook de segurança de carga de trabalho para Microsoft Teams .....	18
Configuração das equipes: .....	18
Criar Webhook de Equipes de Segurança de Carga de Trabalho: .....	18
Notificações via Webhook .....	21



# Notificações de webhook

## Notificações de segurança de carga de trabalho usando webhooks

Os webhooks permitem que os usuários enviem notificações de alerta críticas ou de advertência para vários aplicativos usando um canal de webhook personalizado.

Muitos aplicativos comerciais oferecem suporte a webhooks como uma interface de entrada padrão, por exemplo: Slack, PagerDuty, Teams e Discord. Ao oferecer suporte a um canal webhook genérico e personalizável, o Workload Security pode oferecer suporte a muitos desses canais de entrega. Informações sobre como configurar os webhooks podem ser encontradas nos sites dos respectivos aplicativos. Por exemplo, o Slack fornece ["este guia útil"](#).

Você pode criar vários canais de webhook, cada canal direcionado a uma finalidade diferente, aplicativos separados, destinatários diferentes, etc.

A instância do canal webhook é composta pelos seguintes elementos

Nome	Descrição
URL	URL de destino do webhook, incluindo o prefixo http:// ou https:// junto com os parâmetros de URL
Método	GET/POST - O padrão é POST
Cabeçalho personalizado	Especifique quaisquer cabeçalhos personalizados aqui
Corpo da mensagem	Coloque o corpo da sua mensagem aqui
Parâmetros de alerta padrão	Lista os parâmetros padrão para o webhook
Parâmetros e segredos personalizados	Parâmetros e segredos personalizados permitem que você adicione parâmetros exclusivos e elementos seguros, como senhas

### Criando um webhook

Para criar um Webhook de segurança de carga de trabalho, vá para Admin > Notificações e selecione a aba "Webhooks de segurança de carga de trabalho". A imagem a seguir mostra uma tela de exemplo de criação de webhook do Slack.

Observação: o usuário deve ser um *Administrador* do Workload Security para criar e gerenciar Webhooks do Workload Security.



## 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

- Insira as informações apropriadas para cada um dos campos e clique em "Salvar".
- Você também pode clicar no botão "Testar Webhook" para testar a conexão. Observe que isso enviará o "Corpo da Mensagem" (sem substituições) para a URL definida de acordo com o Método selecionado.
- Os webhooks do SWS compreendem uma série de parâmetros padrão. Além disso, você pode criar seus próprios parâmetros ou segredos personalizados.



## Parâmetros: O que são e como usá-los?

Parâmetros de alerta são valores dinâmicos preenchidos por alerta. Por exemplo, o parâmetro `%%severity%%` será substituído pelo tipo de gravidade do alerta.

Observe que as substituições não são realizadas ao clicar no botão "Testar Webhook"; o teste envia uma carga útil que mostra os espaços reservados do parâmetro (`%%<param-name>%%`), mas não os substitui por dados.

## Parâmetros e segredos personalizados

Nesta seção, você pode adicionar quaisquer parâmetros personalizados e/ou segredos que desejar. Um parâmetro personalizado ou segredo pode estar no URL ou no corpo da mensagem. Os segredos permitem que o usuário configure um parâmetro personalizado seguro, como senha, apiKey etc.

A imagem de exemplo a seguir mostra como parâmetros personalizados são usados na criação de webhook.

/ 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 da lista de webhooks de segurança de carga de trabalho

Na página da lista Webhooks, são exibidos os campos Nome, Criado por, Criado em, Status, Seguro e Último relatório. Observação: o valor da coluna 'status' continuará mudando com base no resultado do último gatilho do webhook. A seguir estão alguns exemplos de resultados de status.

Status	Descrição
OK	Notificação enviada com sucesso.
403	Proibido.



404	URL não encontrada.
400	<p>Pedido ruim. Você poderá ver esse status se houver algum erro no corpo da mensagem, por exemplo:</p> <ul style="list-style-type: none"> <li>• JSON mal formatado.</li> <li>• Fornecendo valor inválido para chaves reservadas. Por exemplo, o PagerDuty aceita apenas crítico/aviso/erro/informação para “Gravidade”. Qualquer outro resultado pode render um status 400.</li> <li>• Erros de validação específicos do aplicativo. Por exemplo, o Slack permite no máximo 10 campos dentro de uma seção. Incluir mais de 10 pode resultar em um status 400.</li> </ul>
410	O recurso não está mais disponível

A coluna “Último relatório” indica o horário em que o webhook foi acionado pela última vez.

Na página de listagem de webhooks, os usuários também podem editar/duplicar/excluir webhooks.

## Configurar notificação de Webhook na política de alerta

Para adicionar uma notificação de webhook a uma política de alerta, acesse -Segurança de carga de trabalho > Políticas- e selecione uma política existente ou adicione uma nova política. Na seção *Ações* > menu suspenso *Notificações de webhook*, selecione os webhooks necessários.



## 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

As notificações do webhook estão vinculadas às políticas. Quando o ataque (RW/DD/WARN) acontecer, a ação configurada (Tirar snapshot/bloqueio de usuário) será tomada e então a notificação de webhook associada será acionada.



Observação: as notificações por e-mail são independentes de políticas e serão acionadas normalmente.

- Se uma política for pausada, as notificações do webhook não serão acionadas.
- Vários webhooks podem ser anexados a uma única política, mas é recomendável anexar no máximo 5 webhooks a uma política.

### Exemplos de webhook de segurança de carga de trabalho

Webhooks para ["Folga"](#)

Webhooks para ["PagerDuty"](#) Webhooks para ["Equipes"](#) Webhooks para ["Discórdia"](#)

## Exemplo de webhook de segurança de carga de trabalho para Discord

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o Discord.



Esta página se refere a instruções de terceiros, que estão sujeitas a alterações. Consulte o ["Documentação do Discord"](#) para obter as informações mais atualizadas.

### Configuração do Discord:

- No Discord, selecione o Servidor, em Canais de Texto, selecione Editar Canal (ícone de engrenagem)
- Selecione **Integrações > Exibir Webhooks** e clique em **Novo Webhook**
- Copie o URL do Webhook. Você precisará colar isso na configuração do webhook do Workload Security.

### Criar Webhook de Segurança de Carga de Trabalho:

1. Navegue até Admin > Notificações e selecione a aba *Workload Security Webhooks*. Clique em "+ Webhook" para criar um novo webhook.
2. Dê ao webhook um nome significativo.
3. No menu suspenso *Tipo de modelo*, selecione **Discord**.
4. Cole a URL do Discord acima no 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 testar o webhook, substitua temporariamente o valor da URL no corpo da mensagem por qualquer URL válida (como <https://netapp.com>) e clique no botão *Testar Webhook*. O Discord exige que uma URL válida seja fornecida para que a funcionalidade Test Webhook funcione.

Não se esqueça de redefinir o corpo da mensagem quando o teste for concluído.



## Notificações via Webhook

Para notificar eventos via webhook, navegue até *Segurança de carga de trabalho > Políticas*. Clique em *+Política de Ataque* ou *+Política de Aviso*.

- Insira um nome de política significativo.
- Selecione o(s) Tipo(s) de Ataque necessário(s), os Dispositivos aos quais a política deve ser anexada e as Ações necessárias.
- No menu suspenso *Notificações de Webhooks*, selecione os webhooks do Discord necessários e salve.

Observação: os webhooks também podem ser anexados às políticas existentes editando-as.



## 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



# Exemplo de webhook de segurança de carga de trabalho para PagerDuty

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o PagerDuty.



Esta página se refere a instruções de terceiros, que estão sujeitas a alterações. Consulte o ["Documentação do PagerDuty"](#) para obter as informações mais atualizadas.

## Configuração do PagerDuty:

1. No PagerDuty, navegue até **Serviços > Diretório de serviços** e clique no botão **+Novo serviço**.
2. Digite um *Nome* e selecione *Usar nossa API diretamente*. Selecione *Adicionar serviço*.

**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. Selecione a aba *Integrações* para ver a **Chave de Integração**. Você precisará dessa chave ao criar o webhook do Workload Security abaixo.
4. Acesse **Incidentes** ou **Serviços** para visualizar 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

## Criar Webhook do PagerDuty de Segurança de Carga de Trabalho:

- Navegue até Admin > Notificações e selecione a aba *Workload Security Webhooks*. Selecione '+ Webhook' para criar um novo webhook.
- Dê ao webhook um nome significativo.
- No menu suspenso *Tipo de modelo*, selecione *Gatilho do PagerDuty*.
- Crie um segredo de parâmetro personalizado chamado *routingKey* e defina o valor como a *Chave de Integração* do PagerDuty criada acima.

## Custom Parameters and Secrets ⓘ

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

+ Parameter

Name ⓘ

routingKey

Value

\*\*\*\*\*

Type

Secret ▼

Description

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": "%%user%%"
  }
}
```

Cancel

Test Webhook

Create Webhook

## Notificações via Webhook

- Para notificar eventos via webhook, navegue até *Segurança de carga de trabalho > Políticas*. Selecione *+Política de Ataque* ou *+Política de Aviso*.
- Insira um nome de política significativo.
- Selecione os tipos de ataque necessários, os dispositivos aos quais a política deve ser anexada e as ações necessárias.
- No menu suspenso *Notificações de Webhooks*, selecione os webhooks do PagerDuty necessários. Salve a política.



Observação: os webhooks também podem ser anexados às políticas existentes editando-as.

## 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



# Exemplo de webhook de segurança de carga de trabalho para Slack

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o Slack.

Esta página se refere a instruções de terceiros, que estão sujeitas a alterações. Consulte a documentação do Slack para obter as informações mais atualizadas.

## Exemplo de folga

- Vá para <https://api.slack.com/apps> e crie um novo aplicativo. Dê um nome significativo e selecione um espaço de trabalho.



## 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

- Vá para Webhooks de entrada, clique em *Ativar Webhooks de entrada*, selecione *Adicionar novo Webhook* e selecione o canal no qual deseja postar.
- Copie o URL do Webhook. Esta URL será fornecida ao criar um webhook de segurança de carga de trabalho.

#### Criar Webhook do Slack para Segurança de Carga de Trabalho

1. Navegue até Admin > Notificações e selecione a aba *Workload Security Webhooks*. Selecione *+ Webhook* para criar um novo webhook.
2. Dê ao webhook um nome significativo.
3. No menu suspenso *Tipo de modelo*, selecione *Slack*.
4. Cole a URL copiada acima.



## 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

### Notificações via webhook

- Para notificar eventos via webhook, navegue até *Segurança de carga de trabalho > Políticas*. Clique em *+Política de Ataque* ou *+Política de Aviso*.
- Insira um nome de política significativo.
- Selecione os tipos de ataque necessários, os dispositivos aos quais a política deve ser anexada e as ações necessárias.



- No menu suspenso *Notificações de webhooks*, selecione os webhooks necessários. Salve a política.

Observação: os webhooks também podem ser anexados às políticas existentes editando-as.

## 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



# Exemplo de webhook de segurança de carga de trabalho para Microsoft Teams

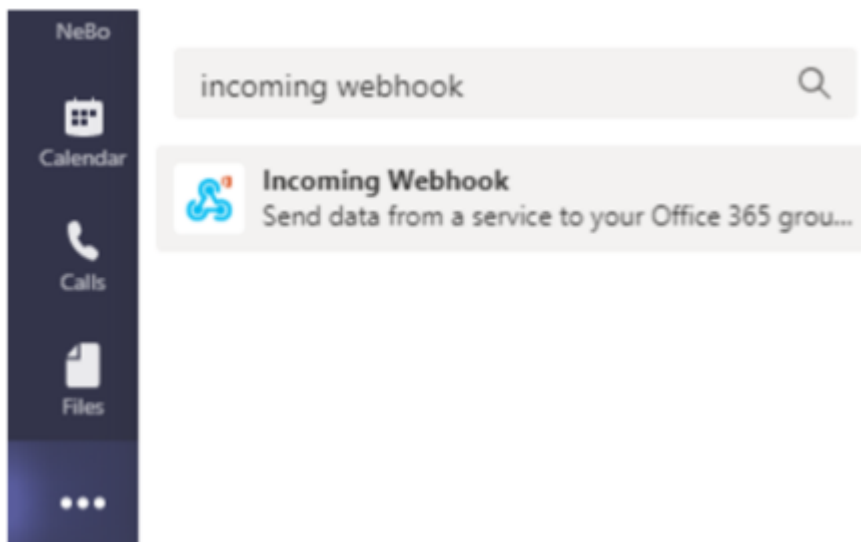
Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o Teams.



Esta página se refere a instruções de terceiros, que estão sujeitas a alterações. Consulte o "[Documentação das equipes](#)" para obter as informações mais atualizadas.

## Configuração das equipes:

1. No Teams, selecione o kebab e pesquise por Webhook de entrada.



2. Selecione **Adicionar a uma equipe** > **Selecionar uma equipe** > **Configurar um conector**.
3. Copie o URL do Webhook. Você precisará colar isso na configuração do webhook do Workload Security.

## Criar Webhook de Equipes de Segurança de Carga de Trabalho:

1. Navegue até Admin > Notificações e selecione a aba "*Workload Security Webhooks*". Selecione + *Webhook* para criar um novo webhook.
2. Dê ao webhook um nome significativo.
3. No menu suspenso *Tipo de modelo*, selecione **Equipes**.



## 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. Cole a URL acima no campo *URL*.

## Passos para criar uma notificação do Teams com o modelo de Adaptive Card

1. Substitua o corpo da mensagem pelo seguinte modelo:

```
{
  "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. Se você estiver usando Power Automate Flows, os parâmetros de consulta na URL estarão em formato codificado. Você deve decodificar a URL antes de inserir.
3. Clique em "Test Webhook" para garantir que não haja erros.
4. Salve o webhook.

## Notificações via Webhook

Para notificar eventos via webhook, navegue até *Segurança de carga de trabalho > Políticas*. Selecione *+Política de Ataque* ou *+Política de Aviso*.

- Insira um nome de política significativo.



- Selecione os tipos de ataque necessários, os dispositivos aos quais a política deve ser anexada e as ações necessárias.
- No menu suspenso *Notificações de Webhooks*, selecione os webhooks do Teams necessários. Salve a política.

Observação: os webhooks também podem ser anexados às políticas existentes editando-as.



## 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



## **Informações sobre direitos autorais**

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.