



Webhook 通知

Data Infrastructure Insights

NetApp
February 03, 2026

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

目錄

Webhook 通知	1
使用 webhook 的工作負載安全通知	1
創建 webhook	1
參數：它們是什麼以及如何使用它們？	3
工作負載安全 Webhook 清單頁面	3
在警報策略中設定 Webhook 通知	4
Discord 的工作負載安全性 Webhook 範例	6
Discord 設定：	6
建立工作負載安全性 Webhook：	6
透過 Webhook 發送通知	8
PagerDuty 的工作負載安全性 Webhook 範例	9
PagerDuty 設定：	10
建立工作負載安全性 PagerDuty Webhook：	11
透過 Webhook 發送通知	12
Slack 的工作負載安全性 Webhook 範例	13
Microsoft Teams 的工作負載安全性 Webhook 範例	18
團隊設定：	18
建立工作負載安全團隊 Webhook：	18
透過 Webhook 發送通知	19

Webhook 通知

使用 webhook 的工作負載安全通知

Webhook 允許使用者使用自訂的 webhook 通道向各種應用程式發送關鍵或警告警報通知。

許多商業應用程式支援 webhook 作為標準輸入接口，例如：Slack、PagerDuty、Teams 和 Discord。透過支援通用、可自訂的 webhook 通道，Workload Security 可以支援許多這樣的交付通道。有關配置 webhook 的資訊可以在相應應用程式的網站上找到。例如，Slack 提供["這個有用的指南"](#)。

您可以建立多個 webhook 通道，每個通道針對不同的目的、單獨的應用程式、不同的收件者等。

Webhook 通道實例由下列元素組成

Name	描述
網址	Webhook 目標 URL，包括 http:// 或 https:// 前綴以及 URL 參數
方法	GET/POST - 預設為 POST
自訂標題	在此處指定任何自訂標題
訊息正文	在此處填寫您的郵件正文
預設警報參數	列出 webhook 的預設參數
自訂參數和機密	自訂參數和秘密可讓您新增唯一參數和安全元素，例如密碼

創建 webhook

若要建立工作負載安全性 Webhook，請前往管理 > 通知並選擇「工作負載安全性 Webhook」標籤。下圖顯示了 Slack webhook 建立畫面的範例。

注意：使用者必須是工作負載安全性_管理員_才能建立和管理工作負載安全性 Webhook。

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"
    }
  ]
}
```

- 在每個欄位中輸入適當的信息，然後按一下「儲存」。
- 您也可以點擊「測試 Webhook」按鈕來測試連線。請注意，這將根據所選方法將「訊息正文」（不含替換）傳送到定義的 URL。
- SWS webhook 包含許多預設參數。此外，您還可以建立自己的自訂參數或秘密。

參數：它們是什麼以及如何使用它們？

警報參數是每個警報填充的動態值。例如，`%%severity%%` 參數將被替換為警報的嚴重性類型。

請注意，按一下「測試 Webhook」按鈕時不會執行替換；測試會傳送有效負載，顯示參數的佔位符（`%%<param-name>%%`），但不會用資料取代它們。

自訂參數和機密

在本節中，您可以新增任何您想要的自訂參數和/或秘密。自訂參數或秘密可以位於 URL 或訊息正文中。秘密允許使用者配置安全的自訂參數，如密碼、apiKey 等。

下面的範例圖展示如何在 webhook 建立中使用自訂參數。

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

工作負載安全 Webhook 清單頁面

Webhooks 清單頁面顯示名稱、建立者、建立日期、狀態、安全性和上次報告欄位。注意：'status' 欄位的值會根據最後一個 webhook 觸發結果不斷變化。以下是狀態結果的範例。

地位	描述
好的	通知已成功發送。
403	禁止。
404	未找到 URL。

400	<p>錯誤的請求。如果訊息正文中存在任何錯誤，您可能會看到此狀態，例如：</p> <ul style="list-style-type: none"> • json 格式錯誤。 • 為保留鍵提供無效值。例如，PagerDuty 僅接受“嚴重性”為嚴重/警告/錯誤/訊息。任何其他結果都可能產生 400 狀態。 • 應用程式特定的驗證錯誤。例如，Slack 允許一個部分內最多有 10 個欄位。包含超過 10 個可能會導致 400 狀態。
410	資源不再可用

「上次報告」欄位表示 webhook 上次觸發的時間。

從 webhook 清單頁面，使用者還可以編輯/複製/刪除 webhook。

在警報策略中設定 **Webhook** 通知

若要將 webhook 通知新增至警報策略，請前往“工作負載安全性”>“策略”，然後選擇現有策略或新增策略。在「動作」部分 > “Webhook 通知” 下拉式功能表中，選擇所需的 webhook。

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

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

Webhook 通知與策略相關。當攻擊 (RW/DD/WARN) 發生時，將採取配置的操作 (拍攝快照/使用者封鎖) ，然後觸發相關的 webhook 通知。

注意：電子郵件通知與策略無關，它們將照常觸發。

- 如果策略暫停，則不會觸發 webhook 通知。
- 可以將多個 webhook 附加到單一策略，但建議將不超過 5 個 webhook 附加到策略。

工作負載安全性 Webhook 範例

Webhook 適用於"鬆弛"

Webhook 適用於"PagerDuty" Webhook 適用於"團隊" Webhook 適用於"不和諧"

Discord 的工作負載安全性 Webhook 範例

Webhook 允許使用者使用自訂的 webhook 通道向各種應用程式發送警報通知。本頁提供了為 Discord 設定 webhook 的範例。



本頁引用第三方說明，這些說明可能會有所變更。請參閱 "[Discord 文件](#)" 以獲取最新資訊。

Discord 設定：

- 在 Discord 中，選擇伺服器，在文字頻道下，選擇編輯頻道（齒輪圖示）
- 選擇“整合”>“查看 Webhook”，然後按一下“新 Webhook”
- 複製 Webhook URL。您需要將其貼上到 Workload Security webhook 設定中。

建立工作負載安全性 Webhook：

1. 導覽至“管理”>“通知”，然後選擇“Workload Security Webhooks”標籤。點擊“+ Webhook”以建立一個新的 webhook。
2. 為 webhook 賦予一個有意義的名稱。
3. 在“模板類型”下拉式選單中，選擇“Discord”。
4. 將上面的 Discord URL 貼到 URL 欄位中。

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

為了測試 webhook，請暫時將訊息正文中的 URL 值替換為任何有效的 URL（例如 <https://netapp.com>），然後按一下測試 Webhook 按鈕。Discord 要求提供有效的 URL 才能讓測試 Webhook 功能正常運作。

測試完成後，請務必將訊息正文重新設定。

透過 Webhook 發送通知

若要透過 webhook 通知事件，請導覽至_工作負載安全性 > 策略_。按一下“+攻擊策略”或“+警告策略”。

- 輸入一個有意義的策略名稱。
- 選擇所需的攻擊類型、應附加策略的設備以及所需的操作。
- 在「Webhooks Notifications」下拉式功能表下，選擇所需的 Discord webhook 並儲存。

注意：也可以透過編輯將 Webhook 附加到現有策略。

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](#)

PagerDuty 的工作負載安全性 Webhook 範例

Webhook 允許使用者使用自訂的 webhook 通道向各種應用程式發送警報通知。本頁面提

供了為 PagerDuty 設定 webhook 的範例。



本頁引用第三方說明，可能會有變更。請參閱"PagerDuty 文檔"以獲取最新資訊。

PagerDuty 設定：

1. 在 PagerDuty 中，導覽至 服務 > 服務目錄 並點選 +新服務 按鈕。
2. 輸入_名稱_並選擇_直接使用我們的 API_。選擇“新增服務”。

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 Integrate via email Use our API directly Don't use an integration

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.

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

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

Events API v2

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

3. 選擇“Integrations”標籤來查看“Integration Key”。當您建立下面的工作負載安全 webhook 時，您將需要此金鑰。
4. 前往*事件*或*服務*查看警報。

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		

建立工作負載安全性 PagerDuty Webhook：

- 導覽至“管理”>“通知”，然後選擇“Workload Security Webhooks”標籤。選擇“+ Webhook”來建立一個新的 webhook。
- 為 webhook 賦予一個有意義的名稱。
- 在「範本類型」下拉式功能表中，選擇「PagerDuty 觸發器」。
- 建立一個名為_routingKey_的自訂參數金鑰，並將其值設為上面建立的PagerDuty_Integration Key_。

Custom Parameters and Secrets 

Name	Value ↑	Description
%%routingKey%%	*****	***
<a data-bbox="169 1148 349 1184" href="#">+ Parameter		
Name 	Value	
routingKey	*****	
Type	Description	
Secret		
<a data-bbox="169 1698 251 1727" href="#">Cancel	<a data-bbox="306 1698 512 1727" href="#">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](#)

透過 Webhook 發送通知

- 若要透過 webhook 通知事件，請導覽至_工作負載安全性 > 策略_。選擇“+攻擊策略”或“+警告策略”。
- 輸入一個有意義的策略名稱。
- 選擇所需的攻擊類型、應附加策略的設備以及所需的操作。
- 在「Webhooks Notifications」下拉式功能表下，選擇所需的 PagerDuty webhook。保存策略。

注意：也可以透過編輯將 Webhook 附加到現有策略。

Add Attack Policy

Policy Name*

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

Slack 的工作負載安全性 Webhook 範例

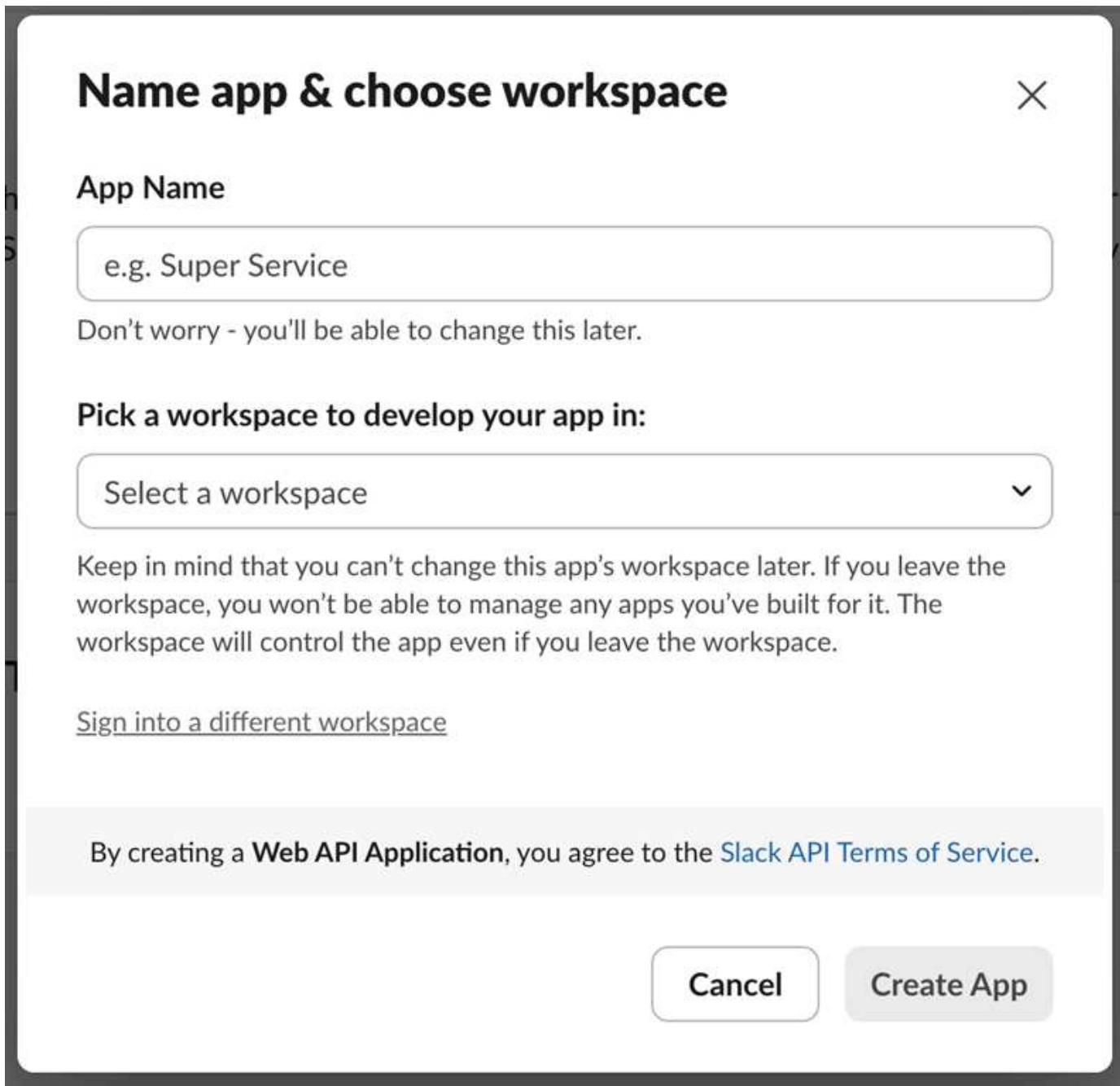
Webhook 允許使用者使用自訂的 webhook 通道向各種應用程式發送警報通知。本頁提供

了為 Slack 設定 webhook 的範例。

本頁引用第三方說明，可能會有變更。請參閱 Slack 文件以獲取最新資訊。

Slack 範例

- 前往 <https://api.slack.com/apps>並創建一個新的應用程式。給它一個有意義的名字並選擇一個工作區。



- 前往傳入 Webhook，按一下_啟動傳入 Webhook_，選擇_新增 Webhook_，然後選擇要發佈的頻道。
- 複製 Webhook URL。建立工作負載安全性 webhook 時將提供此 URL。

建立工作負載安全性 Slack Webhook

1. 導覽至“管理”>“通知”，然後選擇“*Workload Security Webhooks*”標籤。選擇 + *Webhook* 來建立一個新的 webhook。
2. 為 webhook 賦予一個有意義的名稱。
3. 在“模板類型”下拉式選單中，選擇“*Slack*”。
4. 貼上從上面複製的 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

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

透過 webhook 發送通知

- 若要透過 webhook 通知事件，請導覽至_工作負載安全性 > 策略_。按一下“+攻擊策略”或“+警告策略”。
- 輸入一個有意義的策略名稱。
- 選擇所需的攻擊類型、應附加策略的設備以及所需的操作。
- 在「Webhooks Notifications」下拉式功能表下，選擇所需的 webhook。保存策略。

注意：也可以透過編輯將 Webhook 附加到現有策略。

Add Attack Policy

Policy Name*

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**

Microsoft Teams 的工作負載安全性 Webhook 範例

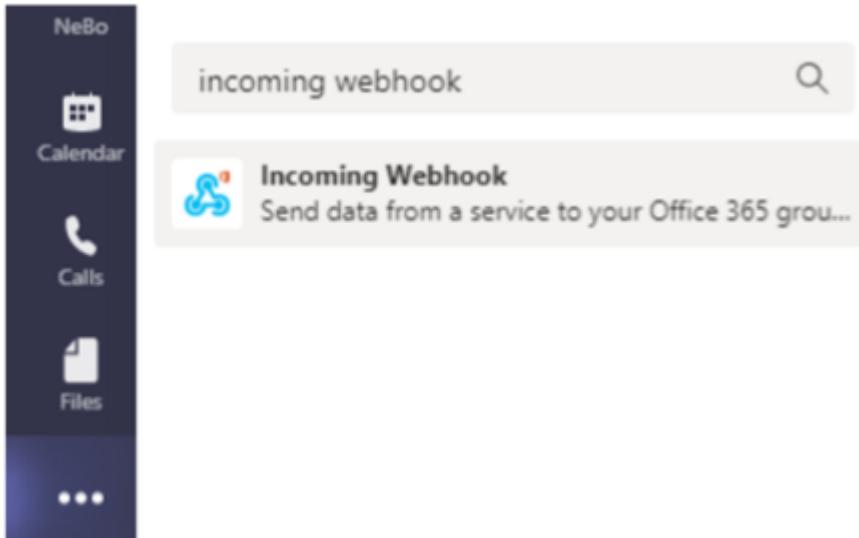
Webhook 允許使用者使用自訂的 webhook 通道向各種應用程式發送警報通知。本頁提供了為 Teams 設定 webhook 的範例。



本頁引用第三方說明，可能會有變更。請參閱["團隊文件"](#)以獲取最新資訊。

團隊設定：

1. 在 Teams 中，選擇 kebab，然後搜尋 Incoming Webhook。



2. 選擇*新增至團隊>選擇團隊>設定連接器*。
3. 複製 Webhook URL。您需要將其貼上到 Workload Security webhook 設定中。

建立工作負載安全團隊 Webhook：

1. 導覽至“管理”>“通知”，然後選擇“工作負載安全性 Webhooks”標籤。選擇 + *Webhook* 來建立一個新的 webhook。
2. 為 webhook 賦予一個有意義的名稱。
3. 在“模板類型”下拉式選單中，選擇“團隊”。

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. 將上面的 URL 貼到 URL 欄位中。

透過 Webhook 發送通知

若要透過 webhook 通知事件，請導覽至_工作負載安全性 > 策略_。選擇“+攻擊策略”或“+警告策略”。

- 輸入一個有意義的策略名稱。
- 選擇所需的攻擊類型、應附加策略的設備以及所需的操作。

- 在「Webhooks Notifications」下拉式功能表下，選擇所需的 Teams webhook。保存策略。

注意：也可以透過編輯將 Webhook 附加到現有策略。

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

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP 「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。