



Webhook 通知

Data Infrastructure Insights

NetApp
February 03, 2026

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

目录

Webhook 通知	1
使用 webhook 的工作负载安全通知	1
创建 webhook	1
参数：它们是什么以及如何使用它们？	3
工作负载安全 Webhook 列表页面	3
在警报策略中配置 Webhook 通知	4
Discord 的工作负载安全 Webhook 示例	6
Discord 设置：	6
创建工作负载安全 Webhook：	6
通过 Webhook 发送通知	8
PagerDuty 的工作负载安全 Webhook 示例	9
PagerDuty 设置：	10
创建工作负载安全 PagerDuty Webhook：	11
通过 Webhook 发送通知	12
Slack 的工作负载安全 Webhook 示例	13
Microsoft Teams 的工作负载安全 Webhook 示例	18
团队设置：	18
创建工作负载安全团队 Webhook：	18
通过 Webhook 发送通知	19

Webhook 通知

使用 webhook 的工作负载安全通知

Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送关键或警告警报通知。

许多商业应用程序支持 webhook 作为标准输入接口，例如：Slack、PagerDuty、Teams 和 Discord。通过支持通用、可定制的 webhook 通道，Workload Security 可以支持许多这样的交付通道。有关配置 webhook 的信息可以在相应应用程序的网站上找到。例如，Slack 提供[“这个有用的指南”](#)。

您可以创建多个 webhook 通道，每个通道针对不同的目的、单独的应用程序、不同的收件人等。

Webhook 通道实例由以下元素组成

名称	描述
URL	Webhook 目标 URL，包括 http:// 或 https:// 前缀以及 URL 参数
方法	GET/POST - 默认为 POST
自定义标题	在此处指定任何自定义标题
消息正文	在此处填写您的邮件正文
默认警报参数	列出 webhook 的默认参数
自定义参数和机密	自定义参数和秘密允许您添加唯一参数和安全元素，例如密码

创建 webhook

要创建工作负载安全 Webhook，请转到管理 > 通知并选择“工作负载安全 Webhook”选项卡。下图显示了 Slack webhook 创建屏幕的示例。

注意：用户必须是工作负载安全_管理员_才能创建和管理工作负载安全 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"
    }
  ]
}
```

- 在每个字段中输入适当的信息，然后单击“保存”。
- 您也可以点击“测试 Webhook”按钮来测试连接。请注意，这将根据所选方法将“消息正文”（不带替换）发送到定义的 URL。
- SWS webhook 包含许多默认参数。此外，您还可以创建自己的自定义参数或秘密。

参数：它们是什么以及如何使用它们？

警报参数是每个警报填充的动态值。例如，`%%severity%%` 参数将被替换为警报的严重性类型。

请注意，单击“测试 Webhook”按钮时不会执行替换；测试会发送一个有效负载，显示参数的占位符（`%%<param-name>%%`），但不会用数据替换它们。

自定义参数和机密

在本节中，您可以添加任何您想要的自定义参数和/或秘密。自定义参数或秘密可以位于 URL 或消息正文中。秘密允许用户配置安全的自定义参数，如密码、apiKey 等。

下面的示例图展示了如何在 webhook 创建中使用自定义参数。

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

工作负载安全 Webhook 列表页面

Webhooks 列表页面显示名称、创建者、创建日期、状态、安全和上次报告字段。注意：'status' 列的值将根据最后一个 webhook 触发结果不断变化。以下是状态结果的示例。

状态	描述
确定	通知已成功发送。
403	禁止。
404	未找到 URL。

400	错误的请求。如果消息正文中存在任何错误，您可能会看到此状态，例如： <ul style="list-style-type: none">• json 格式错误。• 为保留键提供无效值。例如，PagerDuty 仅接受“严重性”为严重/警告/错误/信息。任何其他结果都可能产生 400 状态。• 应用程序特定的验证错误。例如，Slack 允许一个部分内最多有 10 个字段。包含超过 10 个可能会导致 400 状态。
410	资源不再可用

“上次报告”列表示 webhook 上次触发的时间。

从 webhook 列表页面，用户还可以编辑/复制/删除 webhook。

在警报策略中配置 **Webhook** 通知

要将 webhook 通知添加到警报策略，请转到“工作负载安全”>“策略”，然后选择现有策略或添加新策略。在“操作”部分 > “Webhook 通知”下拉菜单中，选择所需的 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

Test-Webhook-1

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

Webhook 通知与策略相关。当攻击 (RW/DD/WARN) 发生时，将采取配置的操作 (拍摄快照/用户阻止)，然后触发相关的 webhook 通知。

注意：电子邮件通知与策略无关，它们将照常触发。

- 如果策略暂停，则不会触发 webhook 通知。
- 可以将多个 webhook 附加到单个策略，但建议将不超过 5 个 webhook 附加到策略。

工作负载安全 Webhook 示例

Webhook 适用于"松弛"

Webhook 适用于"PagerDuty" Webhook 适用于"团队" Webhook 适用于"不和谐"

Discord 的工作负载安全 Webhook 示例

Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。本页提供了为 Discord 设置 webhook 的示例。



本页引用第三方说明，这些说明可能会有所变更。请参阅["Discord 文档"](#)以获取最新信息。

Discord 设置：

- 在 Discord 中，选择服务器，在文本频道下，选择编辑频道（齿轮图标）
- 选择“集成”>“查看 Webhook”，然后单击“新建 Webhook”
- 复制 Webhook URL。您需要将其粘贴到 Workload Security webhook 配置中。

创建工作负载安全 Webhook：

- 导航到“管理”>“通知”，然后选择“Workload Security Webhooks”选项卡。单击“+ Webhook”创建一个新的 webhook。
- 为 webhook 赋予一个有意义的名称。
- 在“模板类型”下拉菜单中，选择“Discord”。
- 将上面的 Discord URL 粘贴到 URL 字段中。

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

为了测试 webhook，请暂时将消息正文中的 URL 值替换为任何有效的 URL（例如 <https://netapp.com>），然后单击 **测试 Webhook** 按钮。Discord 要求提供有效的 URL 才能使测试 Webhook 功能正常工作。

测试完成后，请务必重新设置消息正文。

通过 **Webhook** 发送通知

要通过 webhook 通知事件, 请导航至_工作负载安全 > 策略_。单击“+攻击策略”或“+警告策略”。

- 输入一个有意义的策略名称。
- 选择所需的攻击类型、应附加策略的设备以及所需的操作。
- 在“Webhooks Notifications”下拉菜单下, 选择所需的 Discord webhook 并保存。

注意: 还可以通过编辑将 Webhook 附加到现有策略。

Add Attack Policy

X

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

PagerDuty 的工作负载安全 Webhook 示例

Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。本页面提

供了为 PagerDuty 设置 webhook 的示例。



本页引用第三方说明，可能会有变更。请参阅["PagerDuty 文档"](#)以获取最新信息。

PagerDuty 设置：

1. 在 PagerDuty 中，导航到 服务 > 服务目录 并单击 **+新服务** 按钮。
2. 输入 名称 并选择 直接使用我们的 API。选择“添加服务”。

Add a Service

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

General Settings

Name:

Description:

Integration Settings

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

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

Integration Type Select a tool

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

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

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

Events API v2

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

3. 选择“Integrations”选项卡来查看“Integration Key”。当您创建下面的工作负载安全 webhook 时，您将需要此密钥。
4. 前往*事件*或*服务*查看警报。

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	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	1	Critical Alert: Data Destruction - File Deletion attack from user account #403996 + SHOW DETAILS (1 triggered alert)	Chandan SS	Today at 5:41 AM		

创建工作负载安全 PagerDuty Webhook:

- 导航到“管理”>“通知”，然后选择“Workload Security Webhooks”选项卡。选择“+ Webhook”来创建一个新的 webhook。
- 为 webhook 赋予一个有意义的名称。
- 在“模板类型”下拉菜单中，选择“PagerDuty 触发器”。
- 创建一个名为`_routingKey`的自定义参数密钥，并将其值设置为上面创建的`PagerDuty_Integration Key`。

Custom Parameters and Secrets

Name	Value ↑	Description
<code>%%routingKey%%</code>	*****	
+ Parameter		
Name	Value	
<code>routingKey</code>	*****	
Type	Description	
Secret		
Cancel	Save Parameter	

Add a Webhook

Name

Test PagerDuty

Template Type

PagerDuty Trigger

URL 

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

 Validate SSL Certificate for secure communication

Method

POST

Custom Header

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

Message Body

```
{
  "dedup_key": "%%id%%",
  "event_action": "trigger",
  "links": [
    {
      "href": "https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%",
      "text": "%%severity%% | %%id%% | %%detected%%"
    }
  ],
  "payload": {
    "user": "00000000000000000000"
  }
}
```

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

通过 Webhook 发送通知

- 要通过 webhook 通知事件，请导航至 工作负载安全 > 策略。选择“+攻击策略”或“+警告策略”。
- 输入一个有意义的策略名称。
- 选择所需的攻击类型、应附加策略的设备以及所需的操作。
- 在“Webhooks Notifications”下拉菜单下，选择所需的 PagerDuty webhook。保存策略。

注意：还可以通过编辑将 Webhook 附加到现有策略。

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 的工作负载安全 Webhook 示例

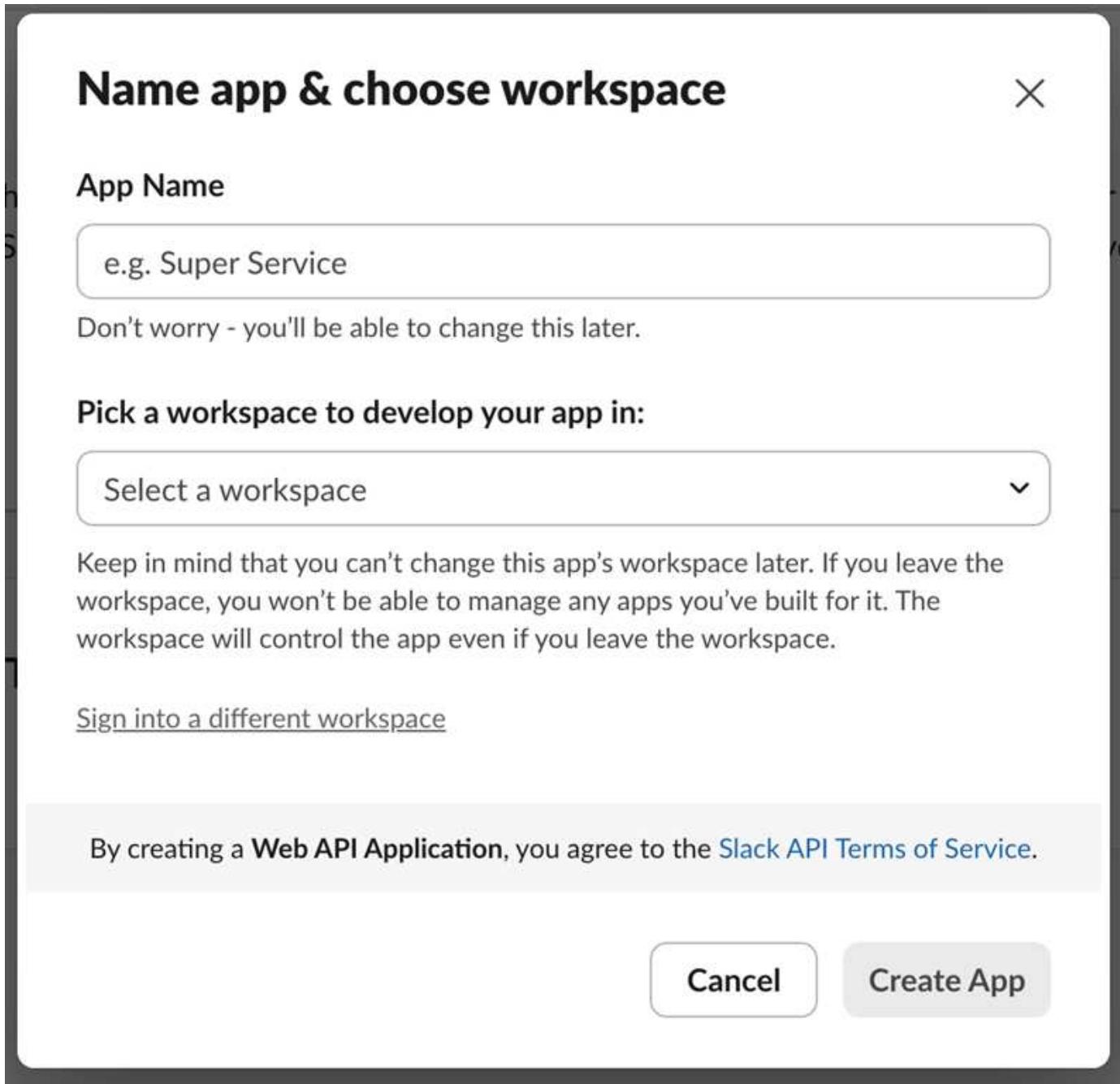
Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。本页提供

了为 Slack 设置 webhook 的示例。

本页引用第三方说明，可能会有变更。请参阅 Slack 文档以获取最新信息。

Slack 示例

- 前往 <https://api.slack.com/apps> 并创建一个新的应用程序。给它一个有意义的名字并选择一个工作区。



- 转到传入 Webhook，单击_激活传入 Webhook_，选择_添加新 Webhook_，然后选择要发布的频道。
- 复制 Webhook URL。创建工作负载安全 webhook 时将提供此 URL。

创建工作负载安全 Slack Webhook

1. 导航到“管理”>“通知”，然后选择“*Workload Security Webhooks*”选项卡。选择 + *Webhook* 来创建一个新的 webhook。
2. 为 webhook 赋予一个有意义的名称。
3. 在“模板类型”下拉菜单中，选择“Slack”。
4. 粘贴从上面复制的 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"
    }
  ]
}
```

通过 webhook 发送通知

- 要通过 webhook 通知事件，请导航至_工作负载安全 > 策略_。单击“+攻击策略”或“+警告策略”。
- 输入一个有意义的策略名称。
- 选择所需的攻击类型、应附加策略的设备以及所需的操作。
- 在“Webhooks Notifications”下拉菜单下，选择所需的 webhook。保存策略。

注意：还可以通过编辑将 Webhook 附加到现有策略。

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 的工作负载安全 Webhook 示例

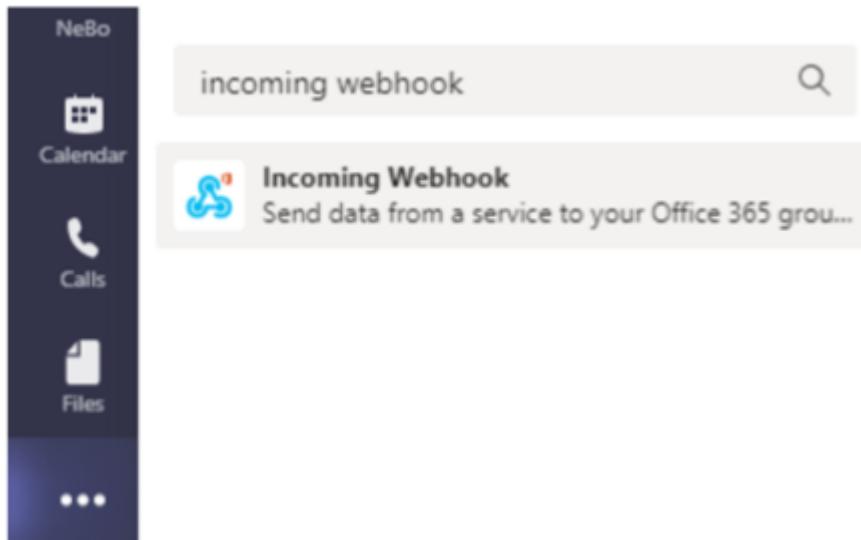
Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。本页提供了为 Teams 设置 webhook 的示例。



本页引用第三方说明，可能会有变更。请参阅["团队文档"](#)以获取最新信息。

团队设置：

1. 在 Teams 中，选择 kebab，然后搜索 Incoming Webhook。



2. 选择*添加到团队>选择团队>设置连接器*。
3. 复制 Webhook URL。您需要将其粘贴到 Workload Security webhook 配置中。

创建工作负载安全团队 Webhook：

1. 导航到“管理”>“通知”，然后选择“工作负载安全 Webhooks”选项卡。选择 + *Webhook* 来创建一个新的 webhook。
2. 为 webhook 赋予一个有意义的名称。
3. 在“模板类型”下拉菜单中，选择“团队”。

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. 将上面的 URL 粘贴到 URL 字段中。

通过 Webhook 发送通知

要通过 webhook 通知事件，请导航至_工作负载安全 > 策略_。选择“+攻击策略”或“+警告策略”。

- 输入一个有意义的策略名称。
- 选择所需的攻击类型、应附加策略的设备以及所需的操作。

- 在“Webhooks Notifications”下拉菜单下，选择所需的 Teams webhook。保存策略。

注意：还可以通过编辑将 Webhook 附加到现有策略。

Add Attack Policy

Policy Name*
Test policy 1

For Attack Type(s) *

Ransomware Attack
 Data Destruction - File Deletion

On Device

All Devices

Actions

Take Snapshot ?
 Block User File Access ?

Time Period

12 hours

Webhooks Notifications

Please Select

Test-Webhook-1

Cancel **Save**

版权信息

版权所有 © 2026 NetApp, Inc. 保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。