



Notifications Webhook

Data Infrastructure Insights

NetApp
February 03, 2026

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

Sommaire

- Notifications Webhook 1
 - Notifications de sécurité de la charge de travail à l'aide de webhooks 1
 - Créer un webhook 1
 - Paramètres : que sont-ils et comment les utiliser ? 3
 - Page de liste des webhooks de sécurité de la charge de travail 3
 - Configurer la notification Webhook dans la politique d'alerte 4
 - Exemple de webhook de sécurité de charge de travail pour Discord 6
 - Configuration de Discord : 6
 - Créer un webhook de sécurité de charge de travail : 6
 - Notifications via Webhook 8
 - Exemple de webhook de sécurité de charge de travail pour PagerDuty 10
 - Configuration de PagerDuty : 10
 - Créer un Webhook PagerDuty de sécurité de charge de travail : 11
 - Notifications via Webhook 12
 - Exemple de webhook de sécurité de charge de travail pour Slack 14
 - Exemple de webhook de sécurité de charge de travail pour Microsoft Teams 18
 - Configuration des équipes : 18
 - Créer un webhook pour les équipes de sécurité de la charge de travail : 18
 - Notifications via Webhook 19

Notifications Webhook

Notifications de sécurité de la charge de travail à l'aide de webhooks

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte critiques ou d'avertissement à diverses applications à l'aide d'un canal webhook personnalisé.

De nombreuses applications commerciales prennent en charge les webhooks comme interface d'entrée standard, par exemple : Slack, PagerDuty, Teams et Discord. En prenant en charge un canal webhook générique et personnalisable, Workload Security peut prendre en charge bon nombre de ces canaux de diffusion. Des informations sur la configuration des webhooks peuvent être trouvées sur les sites Web des applications respectives. Par exemple, Slack fournit "[ce guide utile](#)".

Vous pouvez créer plusieurs canaux webhook, chaque canal ciblant un objectif différent, des applications distinctes, des destinataires différents, etc.

L'instance de canal webhook est composée des éléments suivants

Nom	Description
URL	URL cible du webhook, y compris le préfixe http:// ou https:// ainsi que les paramètres d'URL
Méthode	GET/POST - La valeur par défaut est POST
En-tête personnalisé	Spécifiez ici les en-têtes personnalisés
Corps du message	Mettez le corps de votre message ici
Paramètres d'alerte par défaut	Répertorie les paramètres par défaut du webhook
Paramètres et secrets personnalisés	Les paramètres et secrets personnalisés vous permettent d'ajouter des paramètres uniques et des éléments sécurisés tels que des mots de passe

Créer un webhook

Pour créer un Webhook de sécurité de charge de travail, accédez à Admin > Notifications et sélectionnez l'onglet « Webhooks de sécurité de charge de travail ». L'image suivante montre un exemple d'écran de création de webhook Slack.

Remarque : l'utilisateur doit être un administrateur de Workload Security pour créer et gérer les Webhooks de Workload Security.

Add a Webhook

Name

Template Type

URL 

Validate SSL Certificate for secure communication

Method

Custom Header

Message Body

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

- Saisissez les informations appropriées pour chacun des champs et cliquez sur « Enregistrer ».
- Vous pouvez également cliquer sur le bouton « Tester le Webhook » pour tester la connexion. Notez que cela enverra le « Corps du message » (sans substitutions) à l'URL définie selon la méthode sélectionnée.
- Les webhooks SWS comprennent un certain nombre de paramètres par défaut. De plus, vous pouvez créer vos propres paramètres ou secrets personnalisés.

Paramètres : que sont-ils et comment les utiliser ?

Les paramètres d'alerte sont des valeurs dynamiques renseignées par alerte. Par exemple, le paramètre `%%severity%%` sera remplacé par le type de gravité de l'alerte.

Notez que les substitutions ne sont pas effectuées lorsque vous cliquez sur le bouton « Tester le Webhook » ; le test envoie une charge utile qui affiche les espaces réservés du paramètre (`%%<param-name>%%`) mais ne les remplace pas par des données.

Paramètres et secrets personnalisés

Dans cette section, vous pouvez ajouter tous les paramètres personnalisés et/ou secrets que vous souhaitez. Un paramètre personnalisé ou un secret peut figurer dans l'URL ou le corps du message. Les secrets permettent à l'utilisateur de configurer un paramètre personnalisé sécurisé comme un mot de passe, une clé API, etc.

L'exemple d'image suivant montre comment les paramètres personnalisés sont utilisés dans la création 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

<code>%%alertDetailsPageUrl%%</code>	<code>https://%%cloudinsightsHostname%%/%%alertDetailsPageUrl%%</code>
<code>%%alertTimestamp%%</code>	Alert timestamp in Epoch format (milliseconds)
<code>%%changePercentage%%</code>	Change Percentage
<code>%%detected%%</code>	Alert timestamp in GMT (Tue, 27 Oct 2020 01:20:30 GMT)
<code>%%id%%</code>	Alert ID
<code>%%note%%</code>	Note
<code>%%severity%%</code>	Alert severity
<code>%%status%%</code>	Alert status
<code>%%synopsis%%</code>	Alert Synopsis
<code>%%type%%</code>	Alert type
<code>%%userId%%</code>	User id
<code>%%userName%%</code>	User name
<code>%%filesDeleted%%</code>	Files deleted
<code>%%encryptedFilesSuffix%%</code>	Encrypted files suffix
<code>%%filesEncrypted%%</code>	Files encrypted

Custom Parameters and Secrets

Name	Value	Description
<code>%%webhookConfiguredBy%%</code>	system_admin_1	
<code>%%slack-id%%</code>	

+ Parameter

Page de liste des webhooks de sécurité de la charge de travail

Sur la page de liste des Webhooks, les champs Nom, Créé par, Créé le, Statut, Sécurisé et Dernier signalement sont affichés. Remarque : la valeur de la colonne « statut » continuera de changer en fonction du résultat du dernier déclencheur de webhook. Voici quelques exemples de résultats d'état.

Statut	Description
OK	Notification envoyée avec succès.

403	Interdit.
404	URL non trouvée.
400	<p>Mauvaise demande. Vous pouvez voir ce statut s'il y a une erreur dans le corps du message, par exemple :</p> <ul style="list-style-type: none"> • Json mal formaté. • Fourniture d'une valeur non valide pour les clés réservées. Par exemple, PagerDuty accepte uniquement les valeurs critiques/avertissements/erreurs/informations pour « Gravité ». Tout autre résultat peut donner un statut 400. • Erreurs de validation spécifiques à l'application. Par exemple, Slack autorise un maximum de 10 champs dans une section. L'inclusion de plus de 10 peut entraîner un statut 400.
410	La ressource n'est plus disponible

La colonne « Dernier signalement » indique l'heure à laquelle le webhook a été déclenché pour la dernière fois.

À partir de la page de liste des webhooks, les utilisateurs peuvent également modifier/dupliquer/supprimer les webhooks.

Configurer la notification Webhook dans la politique d'alerte

Pour ajouter une notification webhook à une politique d'alerte, accédez à - Sécurité de la charge de travail > Politiques - et sélectionnez une politique existante ou ajoutez une nouvelle politique. Dans la section *Actions* > liste déroulante *Notifications Webhook*, sélectionnez les webhooks requis.

Edit Attack Policy ✕

Policy Name*

For Attack Type(s) *

- Ransomware Attack
- Data Destruction - File Deletion

On Device

Actions

- Take Snapshot ?
- Block User File Access ?

Time Period

Webhooks Notifications

Les notifications Webhook sont liées aux politiques. Lorsque l'attaque (RW/DD/WARN) se produit, l'action configurée (Prendre un instantané / blocage de l'utilisateur) sera effectuée, puis la notification webhook associée sera déclenchée.

Remarque : les notifications par e-mail sont indépendantes des politiques, elles seront déclenchées comme d'habitude.

- Si une politique est suspendue, les notifications webhook ne seront pas déclenchées.
- Plusieurs webhooks peuvent être attachés à une seule politique, mais il est recommandé de ne pas attacher plus de 5 webhooks à une politique.

Exemples de webhooks de sécurité de charge de travail

Webhooks pour "[Mou](#)"

Webhooks pour "[PagerDuty](#)" Webhooks pour "[Équipes](#)" Webhooks pour "[Discorde](#)"

Exemple de webhook de sécurité de charge de travail pour Discord

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Discord.



Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Reportez-vous à la "[Documentation Discord](#)" pour les informations les plus récentes.

Configuration de Discord :

- Dans Discord, sélectionnez le serveur, sous Canaux texte, sélectionnez Modifier le canal (icône en forme d'engrenage)
- Sélectionnez **Intégrations > Afficher les webhooks** et cliquez sur **Nouveau webhook**
- Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Workload Security.

Créer un webhook de sécurité de charge de travail :

1. Accédez à Admin > Notifications et sélectionnez l'onglet *Webhooks de sécurité de la charge de travail*. Cliquez sur « + Webhook » pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Discord**.
4. Collez l'URL Discord ci-dessus dans le champ *URL*.

Add a Webhook

Name

Template Type

URL

 Validate SSL Certificate for secure communication

Method

Custom Header

Message Body

```
{
  "content": null,
  "embeds": [
    {
      "title": "%%severity%% | %%id%%",
      "description": "%%synopsis%%",
      "url": "https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%% ",
      "color": 3244733,
      "fields": [
        {
          "name": "User"
```

Afin de tester le webhook, remplacez temporairement la valeur de l'URL dans le corps du message par n'importe quelle URL valide (telle que <https://netapp.com>), puis cliquez sur le bouton *Tester le Webhook*. Discord exige qu'une URL valide soit fournie pour que la fonctionnalité Test Webhook fonctionne.

Assurez-vous de réinitialiser le corps du message une fois le test terminé.

Notifications via Webhook

Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail* > *Politiques*. Cliquez sur *+Politique d'attaque* ou *+Politique d'avertissement*.

- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les périphériques auxquels la stratégie doit être associée et les actions requises.
- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks Discord requis et enregistrez.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.

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

Exemple de webhook de sécurité de charge de travail pour PagerDuty

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour PagerDuty.



Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Reportez-vous à la ["Documentation de PagerDuty"](#) pour les informations les plus récentes.

Configuration de PagerDuty :

1. Dans PagerDuty, accédez à **Services > Répertoire des services** et cliquez sur le bouton **+Nouveau service**.
2. Saisissez un *Nom* et sélectionnez *Utiliser directement notre API*. Sélectionnez *Ajouter un service*.

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. Sélectionnez l'onglet *Intégrations* pour voir la **Clé d'intégration**. Vous aurez besoin de cette clé lorsque vous créez le webhook Workload Security ci-dessous.
4. Accédez à **Incidents** ou **Services** pour afficher les alertes.

Activity Integrations Workflows Settings Service Dependencies

Open Incidents (5)

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

Créer un Webhook PagerDuty de sécurité de charge de travail :

- Accédez à Admin > Notifications et sélectionnez l'onglet *Webhooks de sécurité de la charge de travail*. Sélectionnez « + Webhook » pour créer un nouveau webhook.
- Donnez au webhook un nom significatif.
- Dans la liste déroulante *Type de modèle*, sélectionnez *Déclencheur PagerDuty*.
- Créez un secret de paramètre personnalisé nommé *routingKey* et définissez la valeur sur la clé d'intégration PagerDuty *Integration Key* créée ci-dessus.

Custom Parameters and Secrets i

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

Name i

Value

Type

Description

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%%"
  }
}
```

Notifications via Webhook

- Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Sélectionnez *+Politique d'attaque* ou *+Politique d'avertissement*.
- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les périphériques auxquels la politique doit être attachée et les actions requises.
- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks PagerDuty requis. Sauvegarder la politique.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.

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

Exemple de webhook de sécurité de charge de travail pour Slack

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Slack.

Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Consultez la documentation Slack pour obtenir les informations les plus récentes.

Exemple de Slack

- Aller à <https://api.slack.com/apps> et créez une nouvelle application. Donnez-lui un nom significatif et sélectionnez un espace de travail.

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

- Accédez à Webhooks entrants, cliquez sur *Activer les Webhooks entrants*, sélectionnez *Ajouter un nouveau Webhook* et sélectionnez le canal sur lequel publier.
- Copiez l'URL du Webhook. Cette URL sera fournie lors de la création d'un webhook Workload Security.

Créer un webhook Slack pour la sécurité de la charge de travail

1. Accédez à Admin > Notifications et sélectionnez l'onglet *Webhooks de sécurité de la charge de travail*. Sélectionnez *_+ Webhook* pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Type de modèle*, sélectionnez *Slack*.
4. Collez l'URL copiée ci-dessus.

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"
```

Notifications via webhook

- Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Cliquez sur *+Politique d'attaque* ou *+Politique d'avertissement*.
- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les appareils auxquels la politique doit être attachée et les actions requises.

- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks requis. Sauvegarder la politique.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.

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](#)

Exemple de webhook de sécurité de charge de travail pour Microsoft Teams

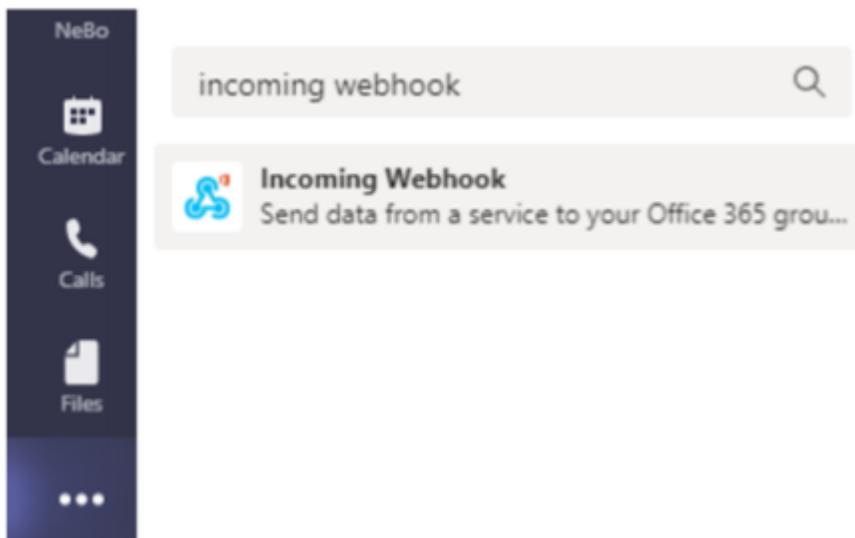
Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Teams.



Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Reportez-vous à la "[Documentation des équipes](#)" pour les informations les plus récentes.

Configuration des équipes :

1. Dans Teams, sélectionnez le kebab et recherchez Webhook entrant.



2. Sélectionnez **Ajouter à une équipe > Sélectionner une équipe > Configurer un connecteur**.
3. Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Workload Security.

Créer un webhook pour les équipes de sécurité de la charge de travail :

1. Accédez à Admin > Notifications et sélectionnez l'onglet « *Webhooks de sécurité de la charge de travail* ». Sélectionnez **_+ Webhook** pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Équipes**.

Add a Webhook

Name

Template Type

URL

 Validate SSL Certificate for secure communication

Method

Custom Header

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. Collez l'URL ci-dessus dans le champ *URL*.

Notifications via Webhook

Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Sélectionnez *+Politique d'attaque* ou *+Politique d'avertissement*.

- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les périphériques auxquels la stratégie doit être associée et les

actions requises.

- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks Teams requis. Sauvegarder la politique.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.

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

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.