Configurer les mises à jour automatiques de la base de données des failles sur FMC

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Configurations

Vérifier

- Affichage des tâches planifiées dans le calendrier
  - Procédure

Dépannage

Informations connexes

Introduction

Ce document décrit comment configurer les mises à jour automatiques pour la base de données des failles (VDB) sur FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Base de données des failles (VDB)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FMC 7.0
- DFT 7,0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

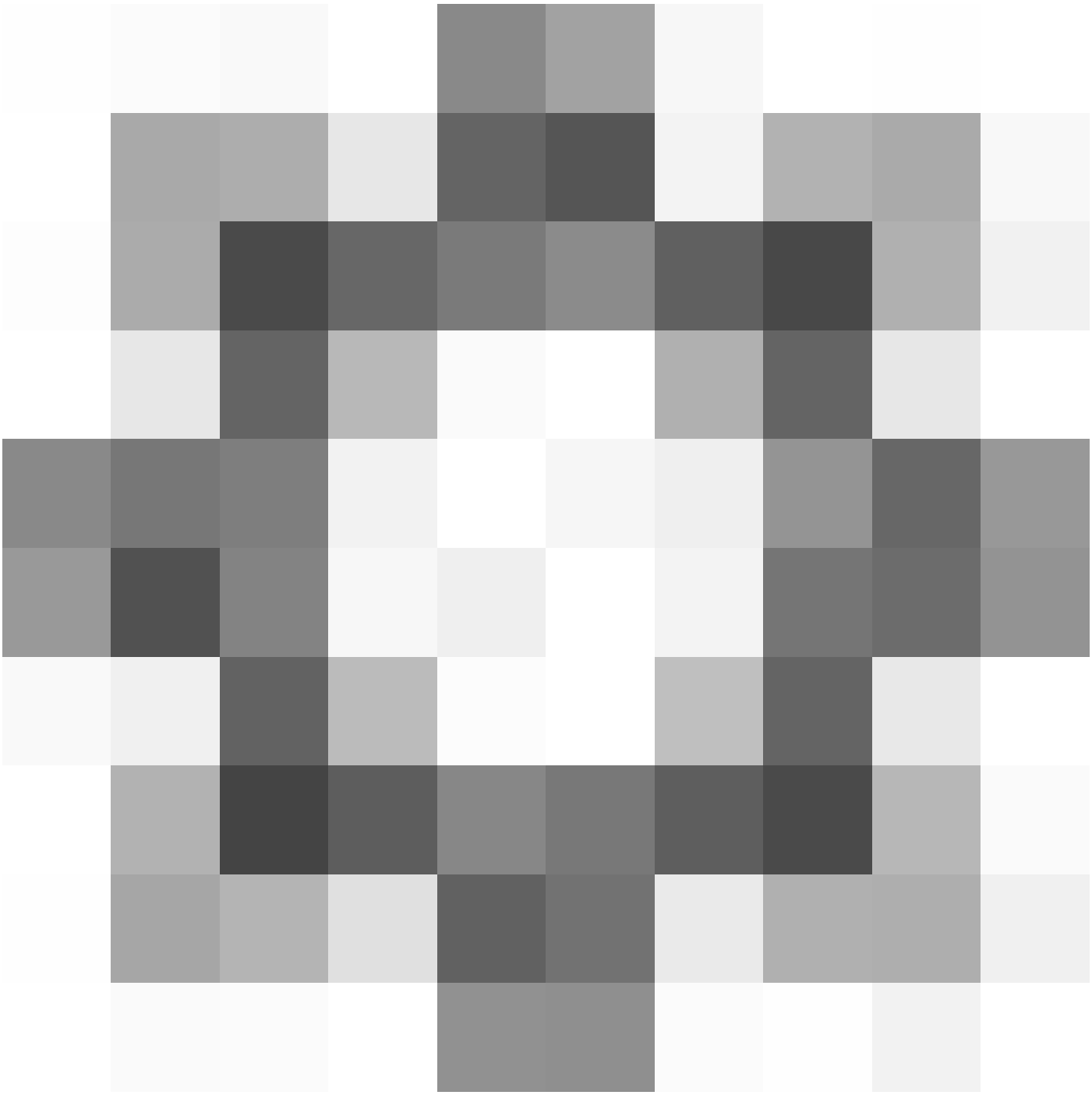
Configurer

Configurations

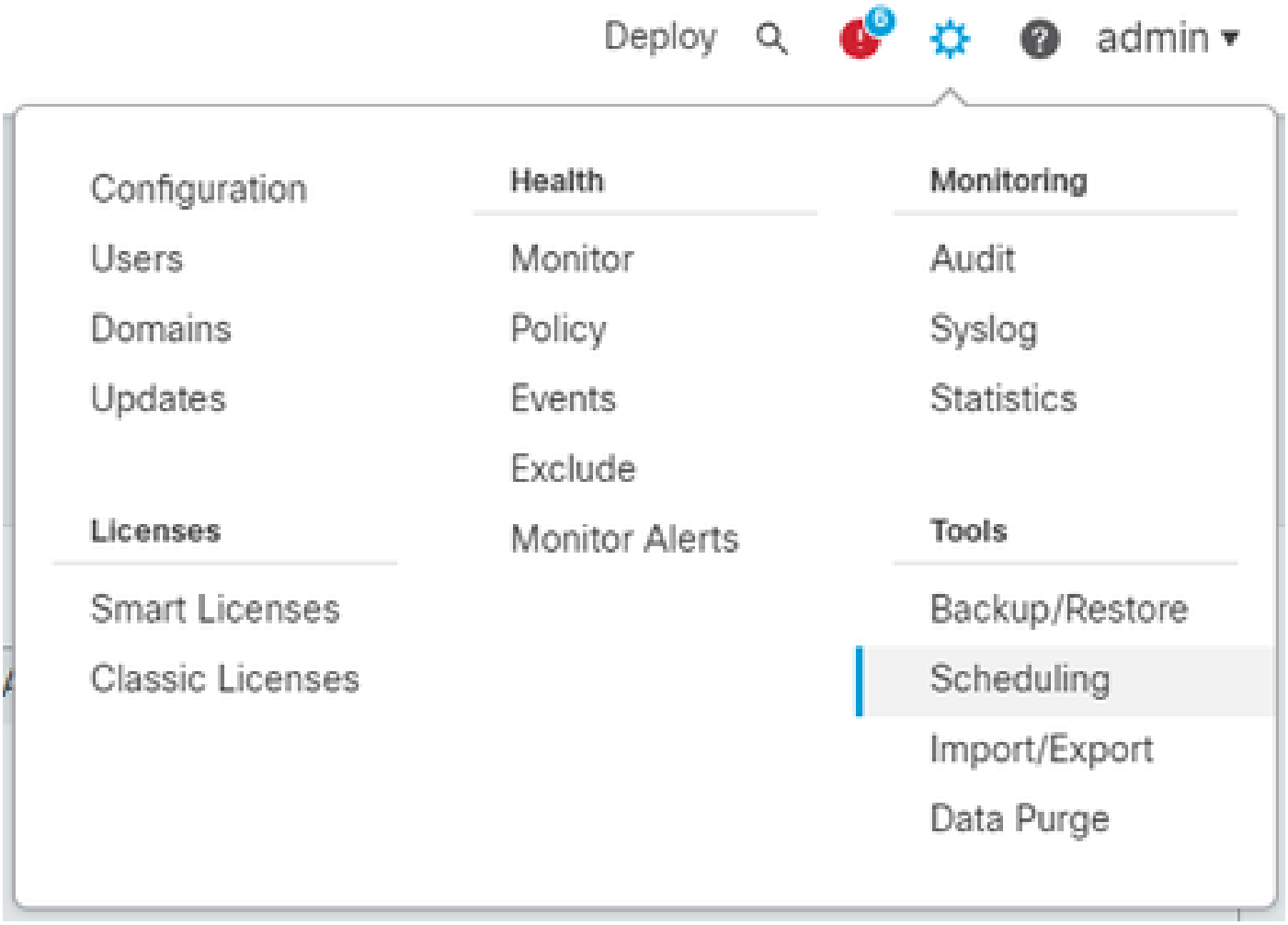
1. Connectez-vous à Firepower Management Center.



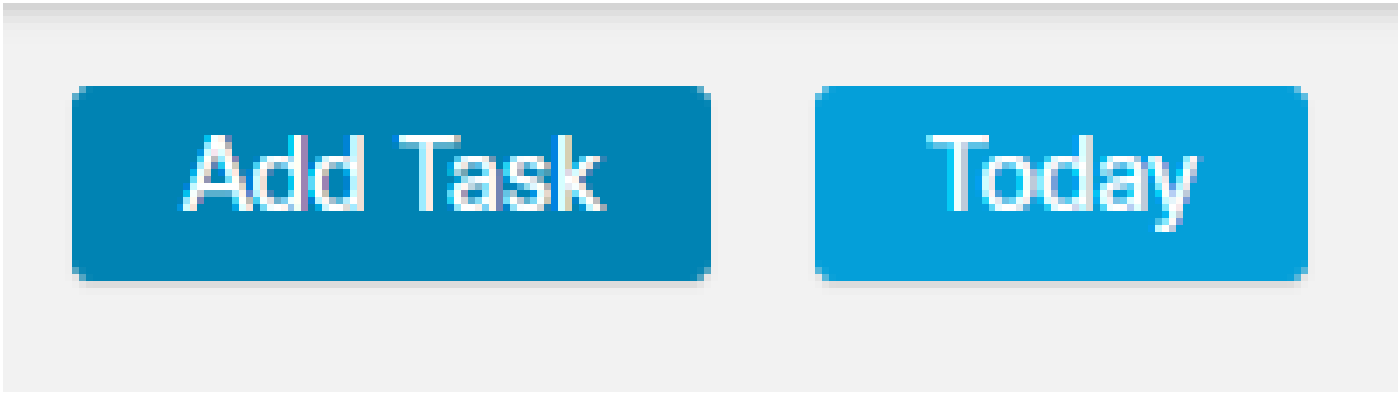
2. Accédez à System(



)> Scheduling.



3. Dans la partie supérieure droite de l'écran Planification, cliquez sur le bouton Ajouter une tâche.

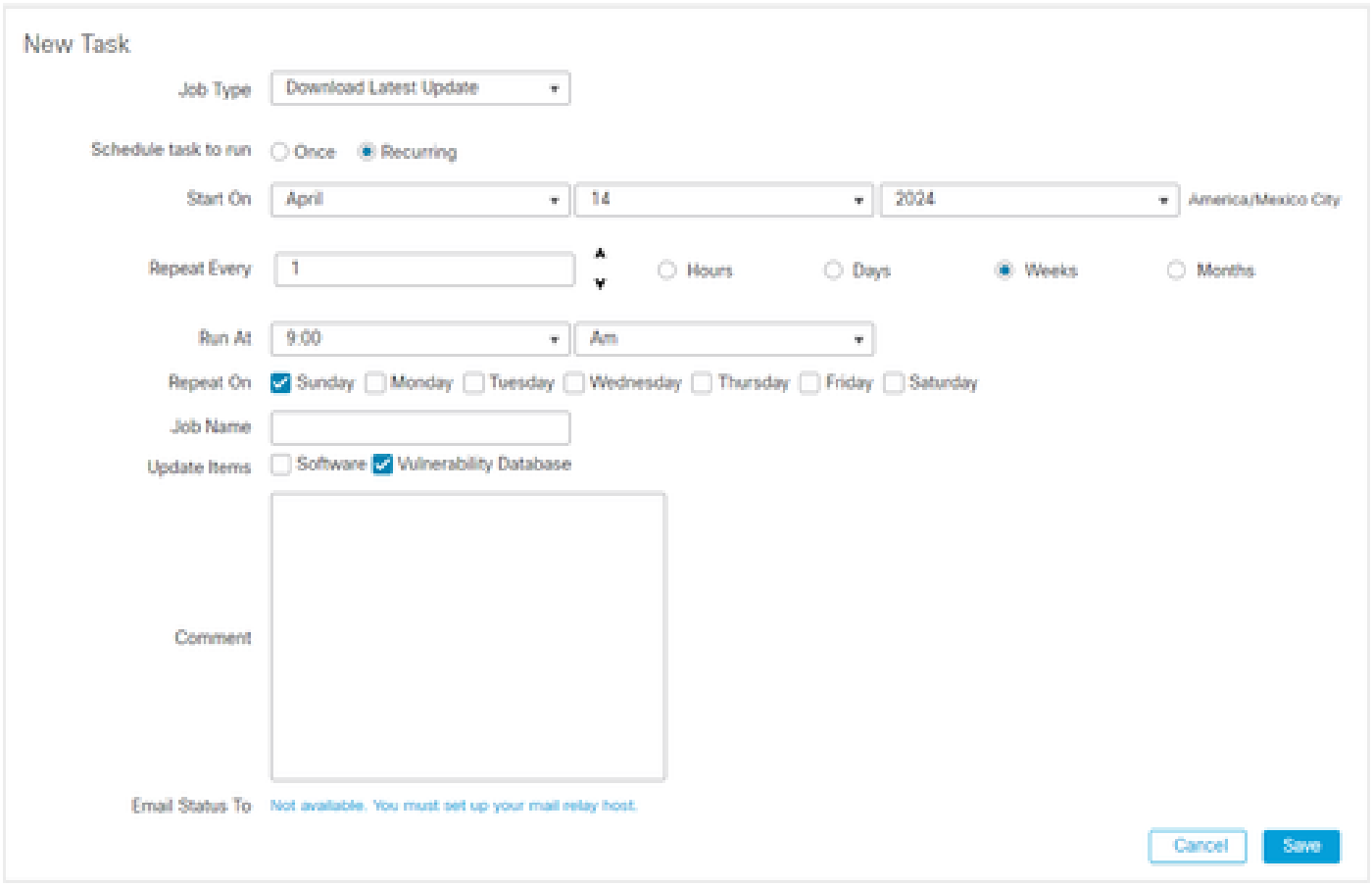


4. Sur l'écran Nouvelle tâche, sélectionnez Télécharger la dernière mise à jour dans le menu déroulant Type de travail et sélectionnez les paramètres correspondant à vos besoins.

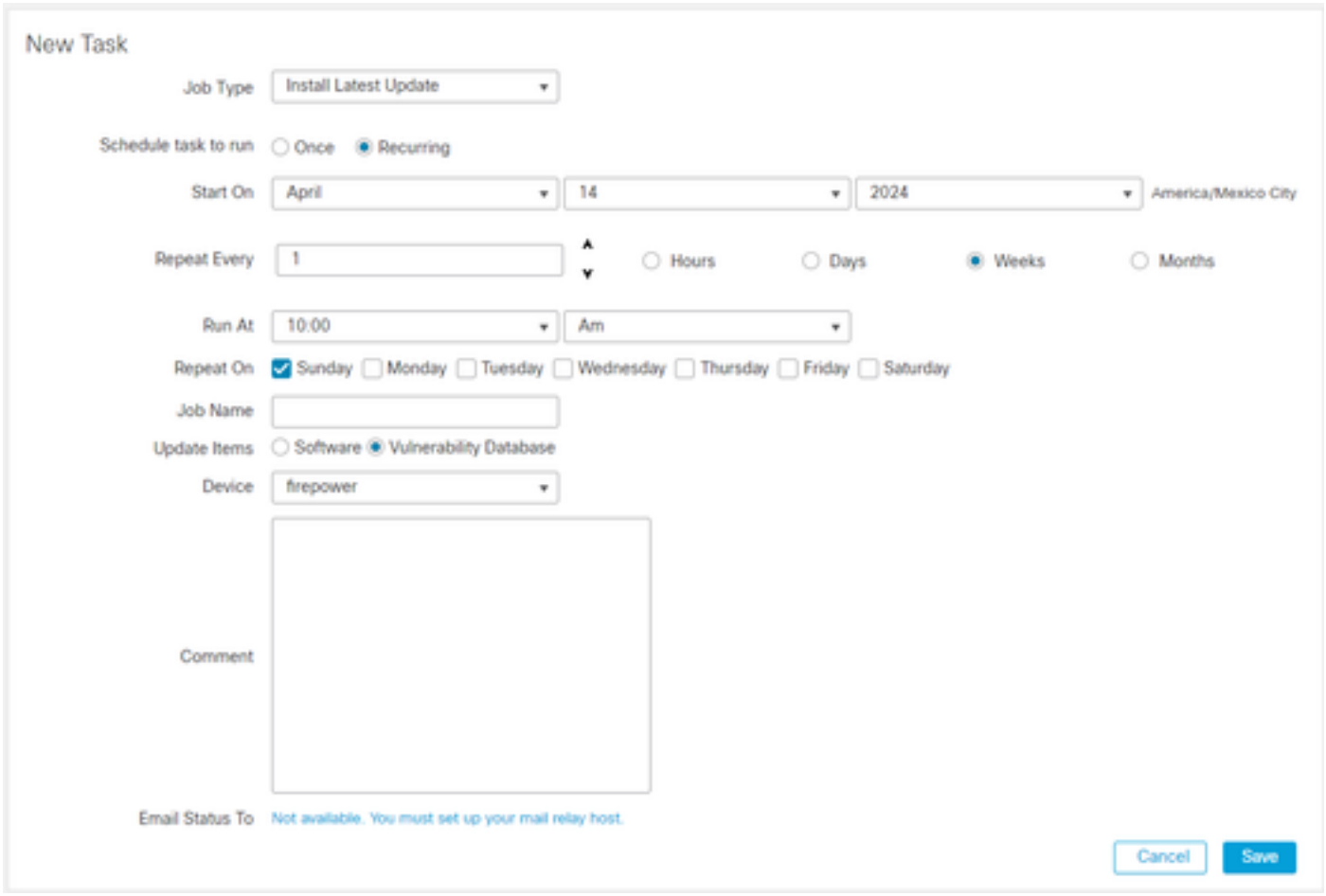
Dans la tâche Planifier à exécuter, sélectionnez Périodique.

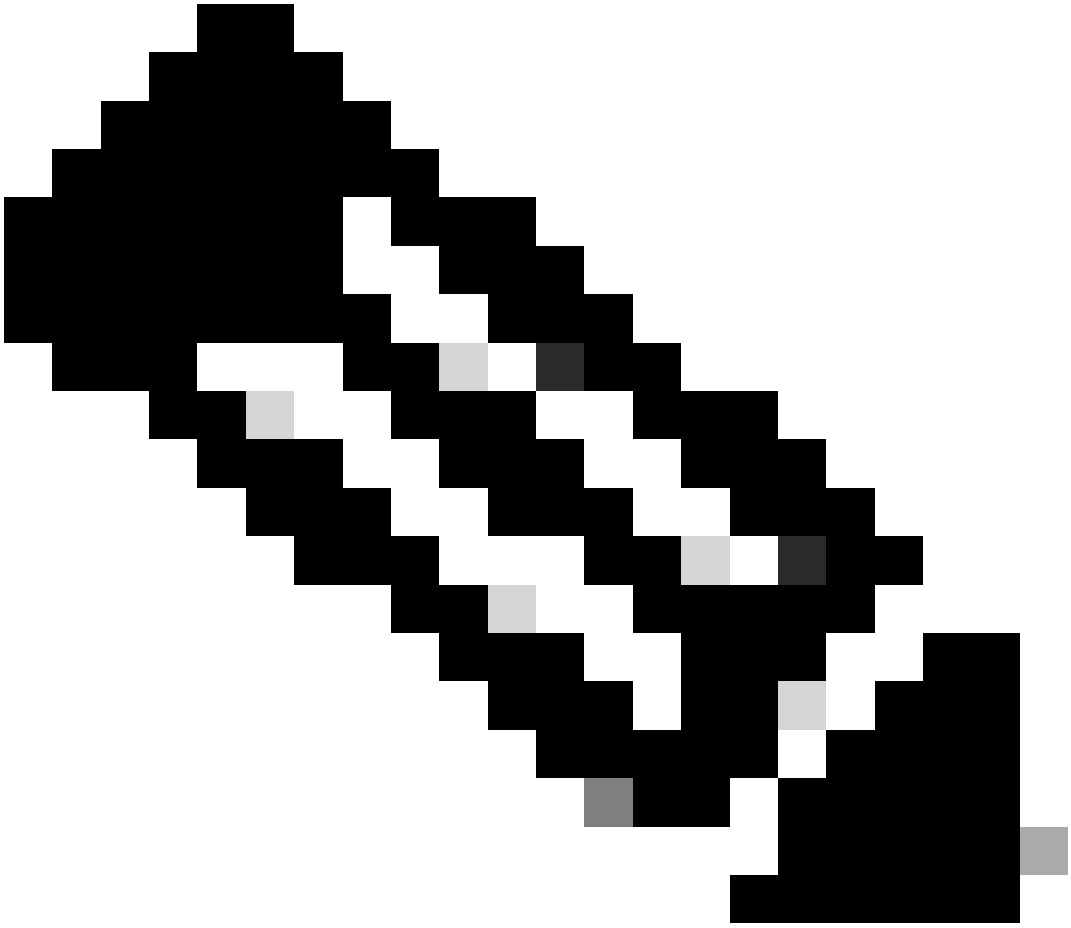
Dans la section Update Items, sélectionnez Vulnerability Database.

Cliquez ensuite sur Enregistrer.

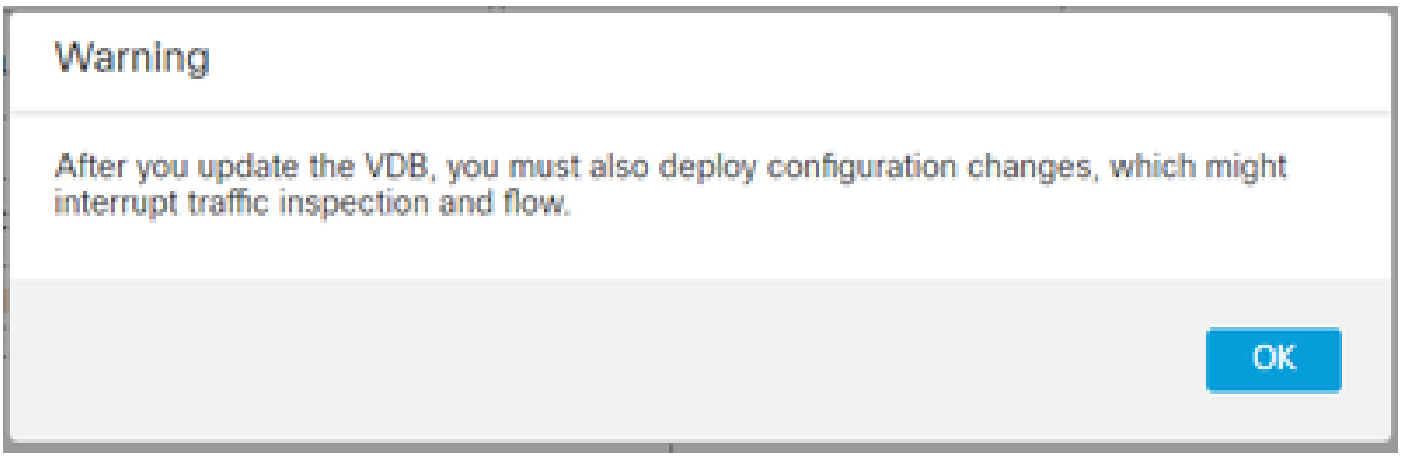


5. Répétez l'étape 3 pour revenir à l'écran Nouvelle tâche et sélectionnez Installer la dernière mise à jour dans le menu déroulant Type de travail et utilisez les paramètres pour répondre à vos besoins, puis cliquez sur Enregistrer.

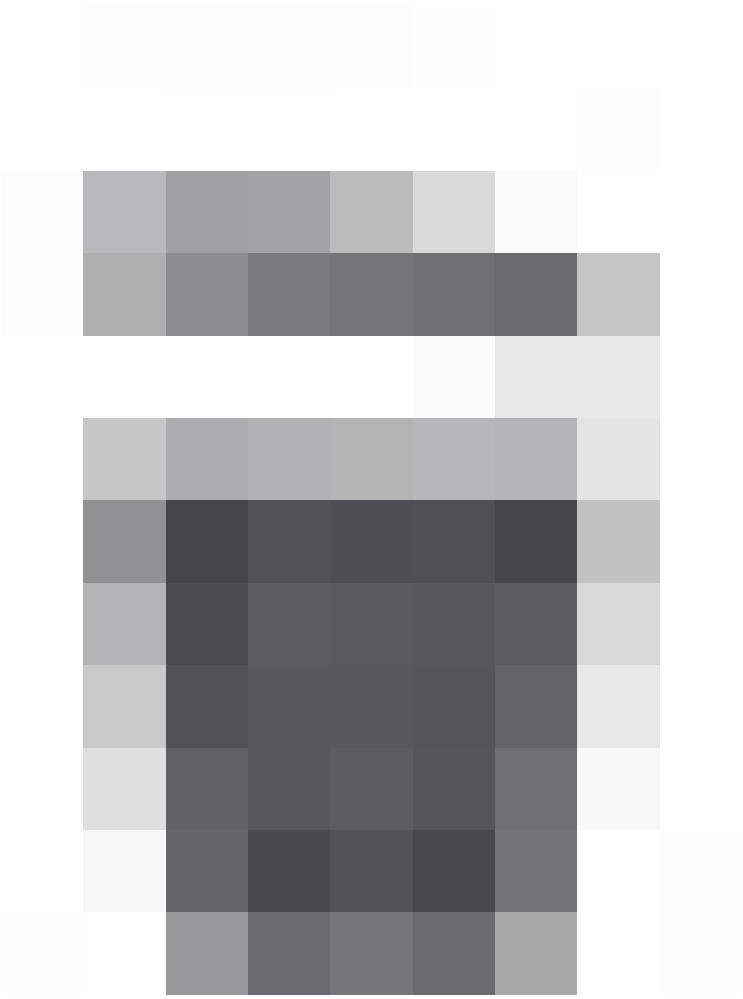

New Task
Job Type
Install Latest Update
Schedule task to run
Once
Recurring
Start On
April
14
2024
America/Mexico City
Repeat Every
1
Hours
Days
Weeks
Months
Run At
10:00
Am
Repeat On
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Job Name
Update Items
Software
Vulnerability Database
Device
firepower
Comment
Email Status To
Not available. You must set up your mail relay host.
Cancel
Save



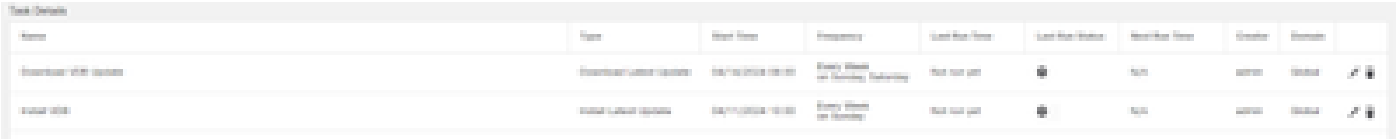
Remarque : sachez qu'après la mise à jour de la VDB, vous devez également déployer des modifications de configuration qui peuvent interrompre l'inspection et le flux du trafic.



Vous pouvez affiner le réglage des tâches planifiées en cliquant sur le stylet de modification (

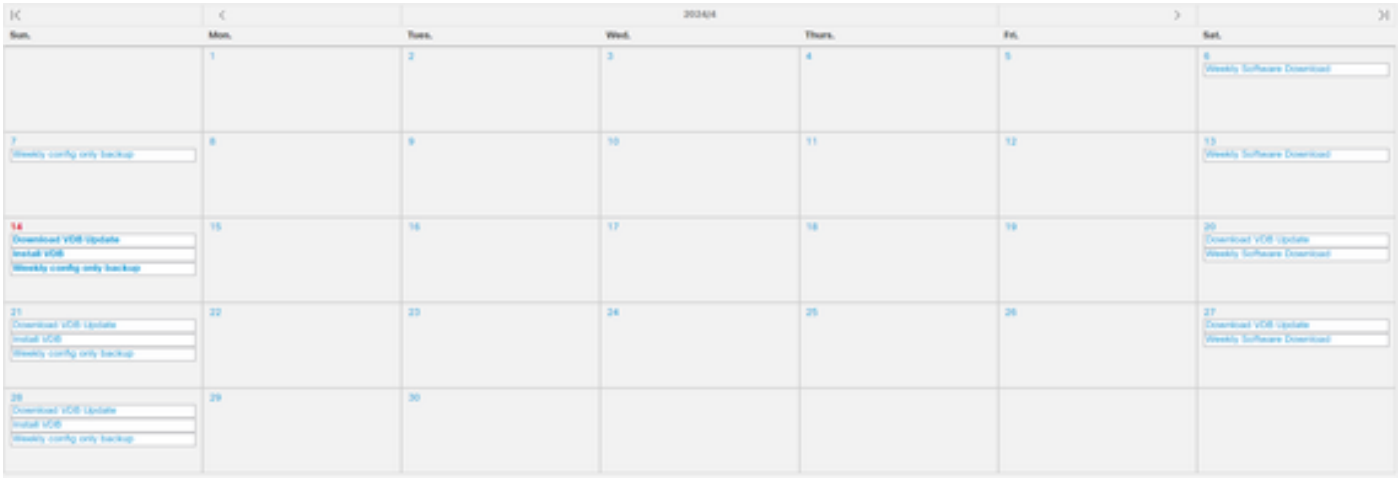


) ou les supprimer en cliquant sur la corbeille (
) dans la section Détails de la tâche de l'écran Planification.



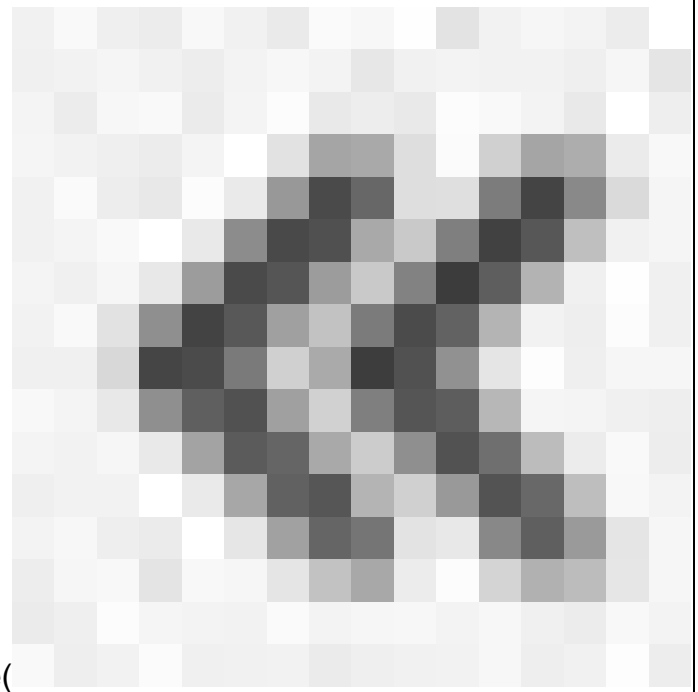
Vérifier

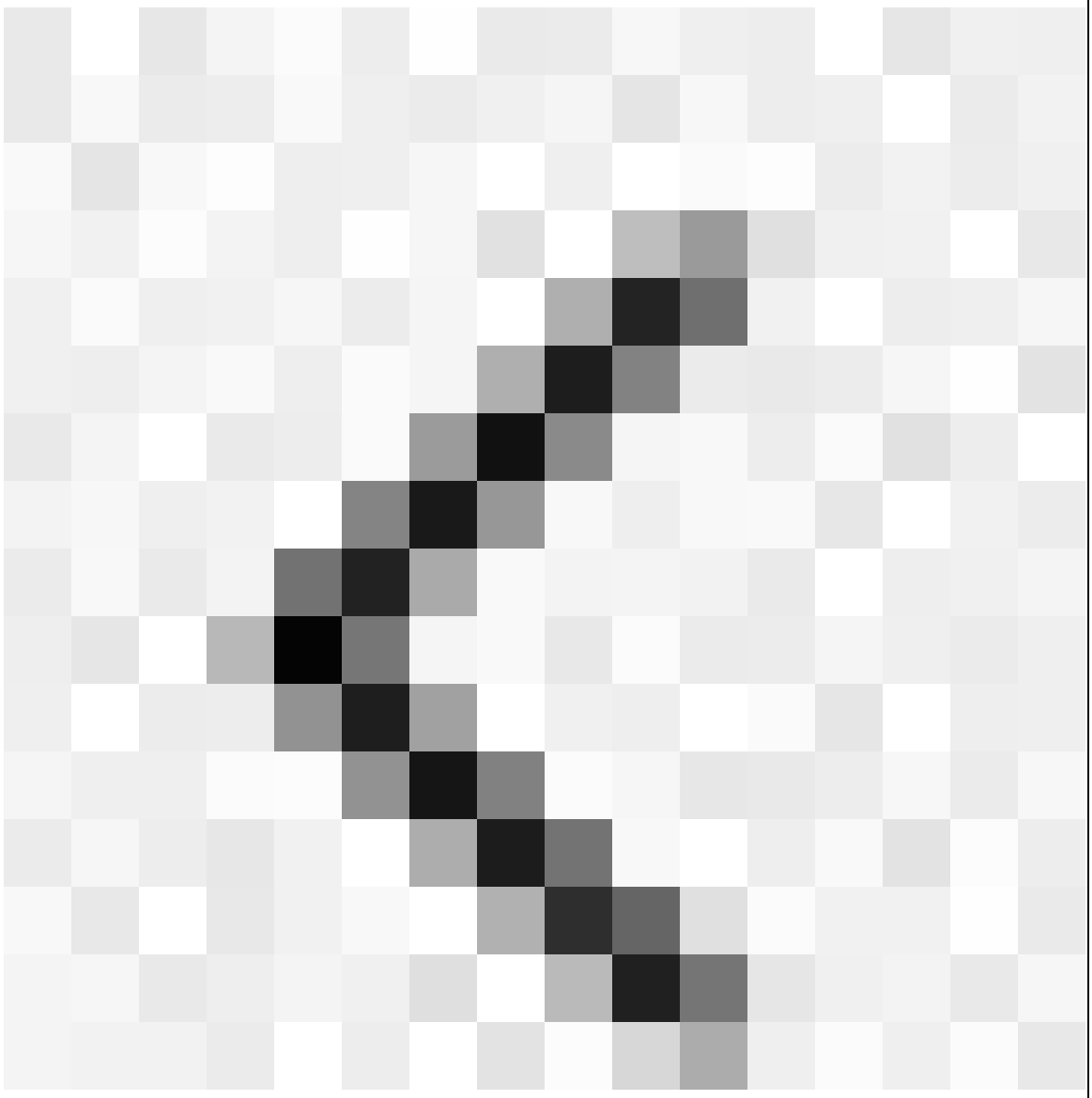
La tâche planifiée est visible dans le calendrier de l'écran Planification.



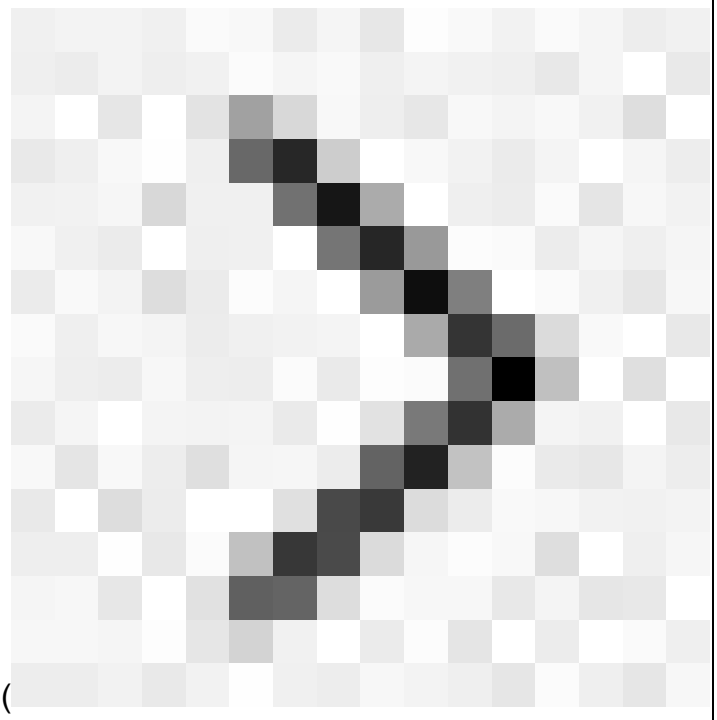
Affichage des tâches planifiées dans le calendrier

Procédure

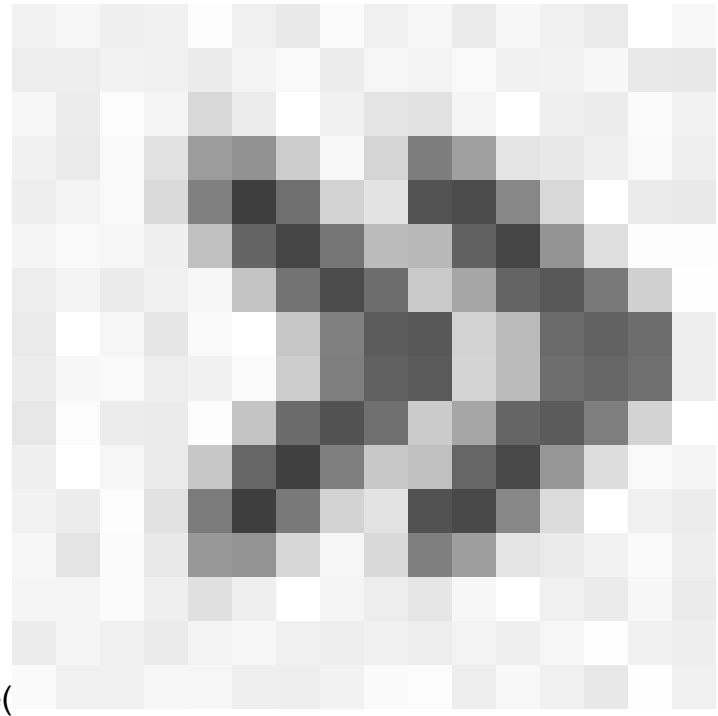
Étape 1	Sélectionnez Système > Outils > Planification.
Étape 2	Vous pouvez effectuer les tâches suivantes à l'aide de l'affichage calendrier :  • Cliquez sur Double flèche gauche( ) pour revenir en arrière d'une année. • Cliquez surFlèche gauche unique(



) pour reculer d'un mois.



- Cliquez sur Flèche droite unique(

	) pour avancer d'un mois.  • Cliquez sur Double flèche droite( ) pour avancer d'une année. • Cliquez sur Aujourd'hui pour revenir au mois et à l'année en cours. • Cliquez sur Ajouter une tâche pour planifier une nouvelle tâche. • Cliquez sur une date pour afficher toutes les tâches planifiées pour la date spécifique dans une table de liste des tâches. • Cliquez sur une tâche spécifique à une date pour l'afficher dans une table de liste des tâches.

Dépannage

Si la mise à niveau automatique de la VDB ne fonctionne pas comme prévu, vous pouvez restaurer la VDB.

Étapes :

Établissez une connexion SSH avec l'interface de ligne de commande du périphérique de gestion (FMC, FDM ou SFR onbox).

Passez en mode expert et en mode racine, puis définissez la variable d'annulation :

```
<#root>
expert
```

```
sudo su
export ROLLBACK_VDB=1
```

Vérifiez que le package VDB vers lequel vous souhaitez effectuer la rétrogradation se trouve sur le périphérique dans /var/sf/updates et installez-le :

<#root>

```
install_update.pl --detach /var/sf/updates/<name of desired VDB Package file>
```

Les journaux d'installation de vdb normaux se trouvent à l'emplacement approprié, à l'adresse /var/log/sf/vdb-*

Une fois l'installation de VDB terminée, déployez la stratégie sur les périphériques.

Sur FMC, pour vérifier l'état d'installation de VDB, vous pouvez consulter le contenu du répertoire suivant :

root@firepower:/var/log/sf/vdb-4.5.0-338# ls -la
total 40
drwxr-xr-x 5 root root 4096 15 mai 2023 .
drwxr-xr-x 11 root root 4096 Apr 23 06:00 ..
-rw-r—r— 1 racine 3308 15 mai 2023 flags.conf.complete
drwxr-xr-x 2 root 4096 May 15 2023 installer
drwxr-xr-x 2 root 4096 15 mai 2023 post
drwxr-xr-x 2 root root 4096 15 mai 2023 pre
-rw-r—r— 1 racine 1603 15 mai 2023 status.log
-rw-r—r— 1 racine 5703 15 mai 2023 vdb.log
-rw-r—r— 1 racine 5 mai 15 2023 vdb.pid

Sur FTD, pour vérifier l'historique des installations de VDB, vérifiez le contenu du répertoire suivant :

root@firepower:/ngfw/var/cisco/deploy/pkg/var/cisco/packages# ls -al
total 72912
drwxr-xr-x 5 root 130 sep 1 08:49 .
drwxr-xr-x 4 root root 34 Aug 16 14:40 ..
drwxr-xr-x 3 root 18 août 16 14:40 exporter-7.2.4-169
-rw-r—r— 1 racine 2371661 juil 27 15:34 exporter-7.2.4-169.tgz
drwxr-xr-x 3 root 21 août 16 14:40 vdb-368
-rw-r—r— 1 racine 36374219 juil 27 15:34 vdb-368.tgz
drwxr-xr-x 3 root 21 sep 1 08:49 vdb-369
-rw-r—r— 1 racine 35908455 sept. 1 08:48 vdb-369.tgz

Informations connexes

Mettre à jour la base de données des failles (VDB)

Planification des tâches

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.