Générer un kit de diagnostics pour les appliances Secure Network Analytics

Contenu

Introduction

Ce document décrit les différentes procédures disponibles pour collecter un pack de diagnostics pour les appliances SNA (Secure Network Analytics).

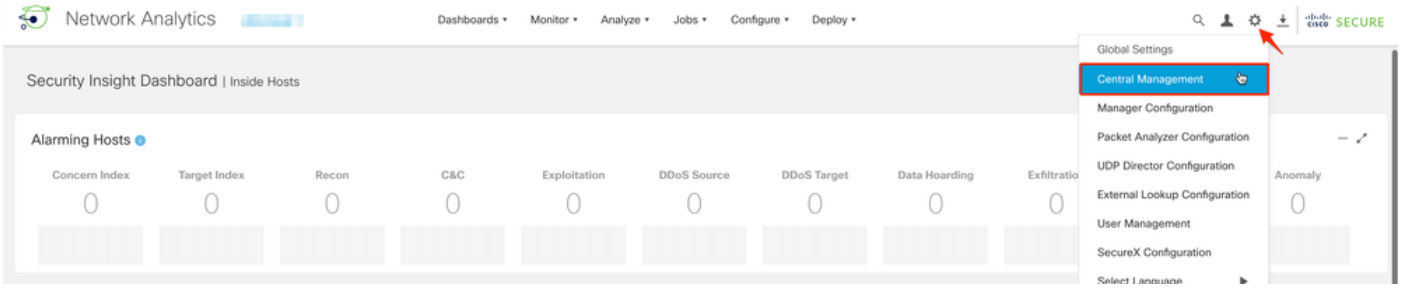
Procédure

Il existe trois méthodes principales pour générer le pack de diagnostics pour les appliances SNA. La méthode suggérée est **la méthode 1. À partir de l'interface utilisateur Web du gestionnaire**, les deux autres méthodes sont toutefois une option au cas où l'interface utilisateur Web du gestionnaire n'est pas disponible.

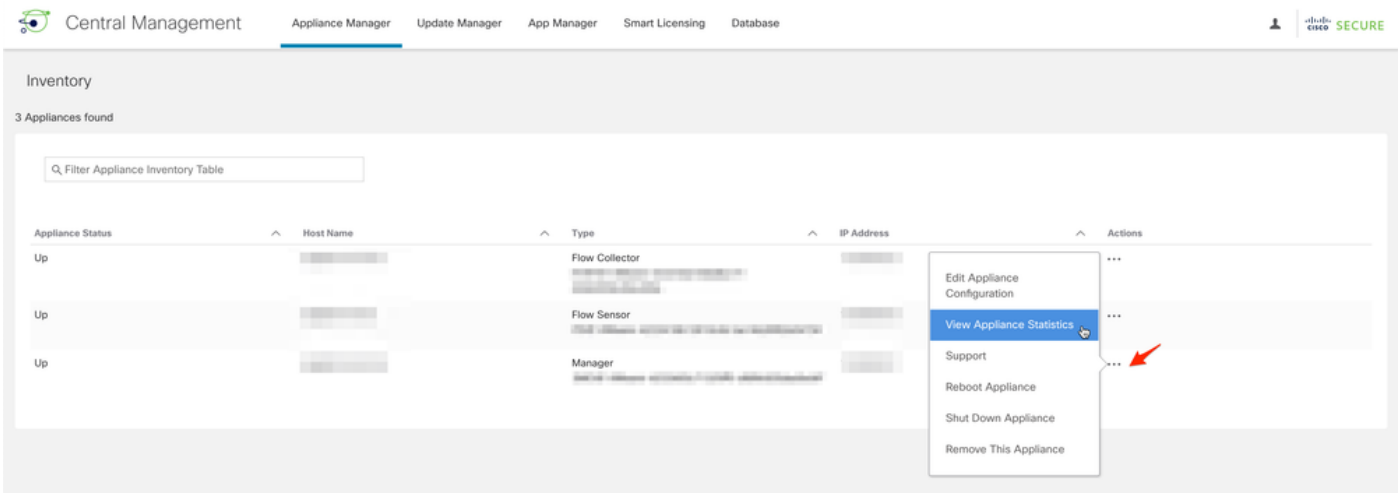
> **Note**: Si l'interface utilisateur Web du gestionnaire n'est pas disponible et que vous devez générer un pack de diagnostics à partir du gestionnaire, reportez-vous à la **méthode 3. À partir de l'interface de ligne de commande de chaque appareil**.

Méthode 1. À partir de l'interface utilisateur Web du gestionnaire

1. Connectez-vous à l'interface utilisateur Web du manager.
2. Accédez à **Paramètres globaux > Gestion centrale**.



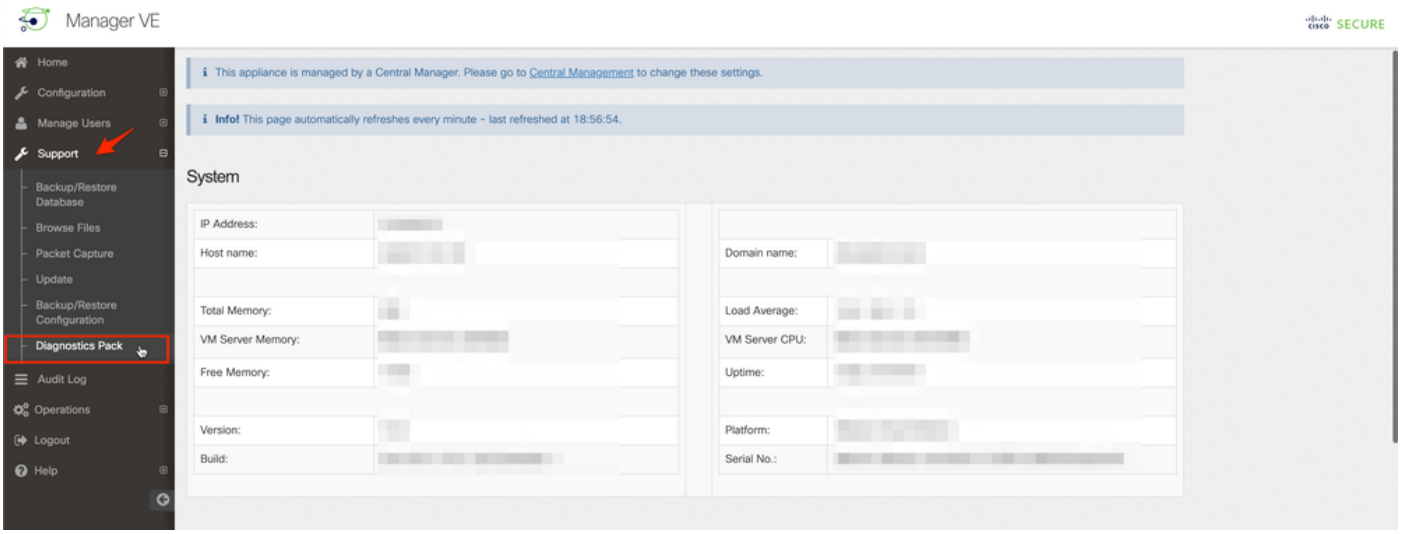
3. Dans les appliances répertoriées, localisez l'appliance à partir de laquelle vous devez créer le pack de diagnostics et sélectionnez **Actions (icône Ellipse) > Afficher les statistiques de l'appliance**.



4. Vous devez être redirigé vers l'interface utilisateur Admin de l'appareil sélectionné.

5. Connectez-vous à l'interface utilisateur Admin de l'appliance avec les informations d'identification **admin**.

6. Dans le menu de gauche, accédez à **Support > Diagnostics Pack**.

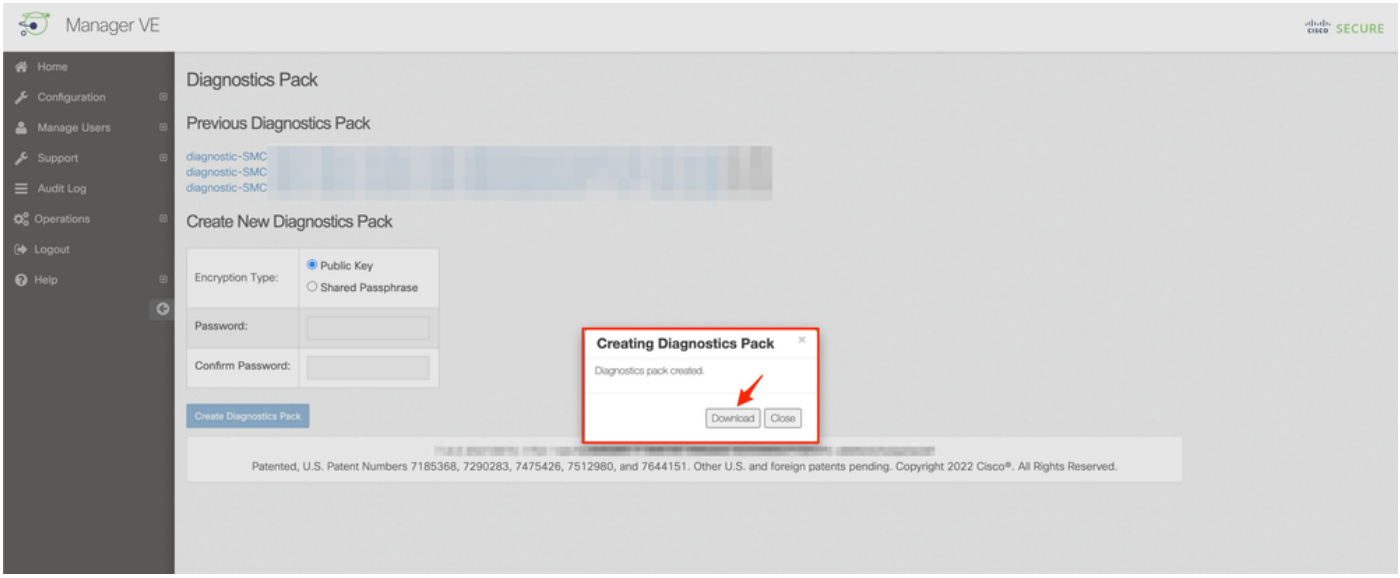


7. Une fois dans la page Pack de diagnostics, vous devez sélectionner le chiffrement de **clé publique** par défaut ou fournir une clé/phrase de passe partagée à utiliser pour le chiffrement.

> **Note**: Si vous choisissez d'utiliser une clé/un mot de passe personnalisé, vous devez fournir cette phrase de passe dans la description du fichier lorsque vous téléchargez le pack Diagnostics dans le Gestionnaire de dossiers d'assistance.

8. Sélectionnez **Create Diagnostics Pack** pour générer le pack de diagnostics de l'appliance.

9. Une fois terminé, vous devez disposer d'une fenêtre contextuelle comprenant le bouton **Télécharger** pour télécharger le Pack de diagnostics.



Méthode 2. À partir de l'interface utilisateur Admin de chaque appareil

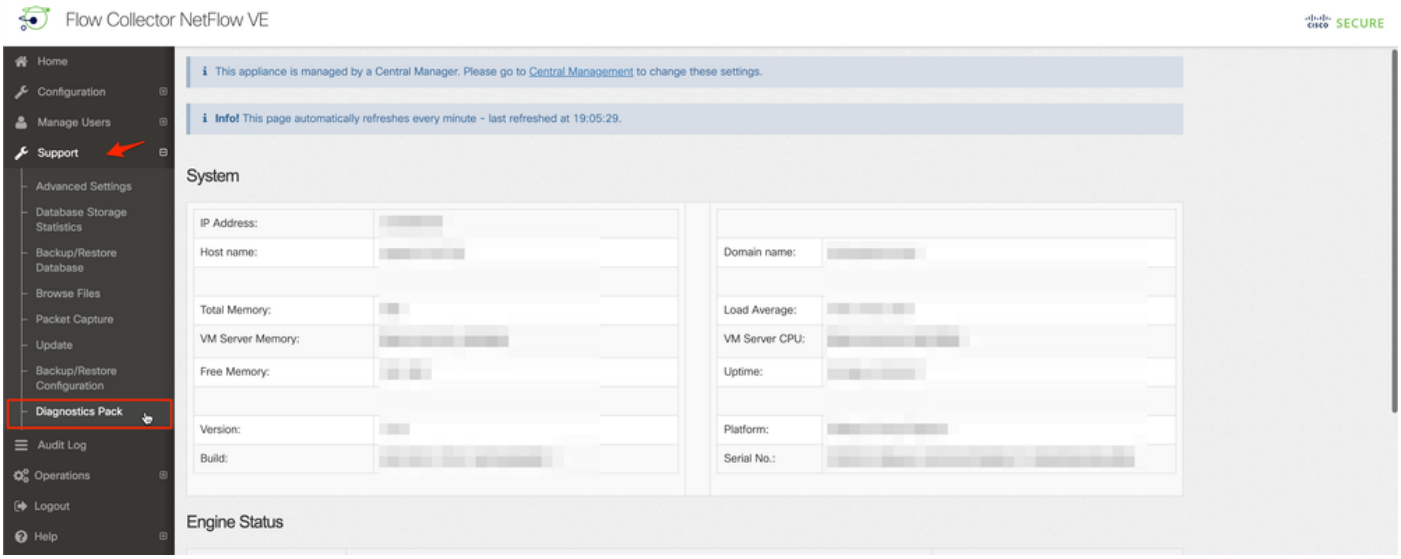
Pour cette méthode, vous devez accéder à la solution matérielle-logicielle à partir de laquelle vous souhaitez générer le pack de diagnostics, via HTTPS (Hypertext Transfer Protocol Secure).

> **Note**: Pour accéder directement à l'**interface utilisateur Admin** du manager, vous devez utiliser l'URL suivante : https://<Manager_IP_address>/smc/index.html, sinon vous êtes redirigé vers l'interface utilisateur Web du manager.

Par exemple, afin de générer le pack de diagnostics d'un collecteur de flux avec cette méthode, vous devez suivre les étapes suivantes :

1. Àpartir d'un navigateur Web, accédez à **https://<adresse_IP_FC>**
2. Connectez-vous à l'interface utilisateur Admin de l'appliance avec les informations d'identification admin.

3. Dans le menu de gauche, accédez à **Support > Diagnostics Pack**.

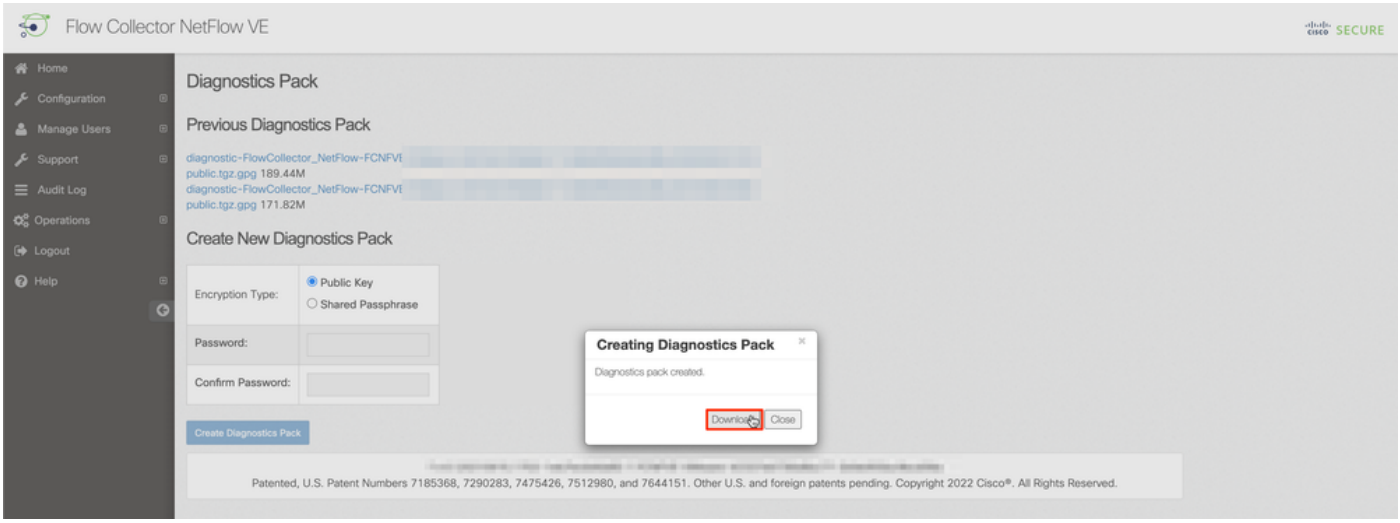


4. Une fois dans la page Pack de diagnostics, vous devez sélectionner le chiffrement de **clé publique** par défaut ou fournir une clé/phrase de passe partagée à utiliser pour le chiffrement.

> **Note**: Si vous choisissez d'utiliser une clé/phrase de passe personnalisée, vous devez fournir cette phrase de passe dans la description du fichier lorsque vous téléchargez le pack de diagnostics dans le Gestionnaire de dossiers d'assistance.

5. Sélectionnez **Create Diagnostics Pack** pour générer le pack de diagnostics de l'appliance.

6. Une fois terminé, vous devez disposer d'une fenêtre contextuelle comprenant le bouton **Télécharger** pour télécharger le Pack de diagnostics.



Méthode 3. À partir de l'interface de ligne de commande (CLI) de chaque appareil

Il arrive parfois qu'il soit impossible de générer le pack de diagnostics d'un appareil à l'aide des méthodes décrites précédemment, mais il peut être généré directement à partir de l'interface de ligne de commande de l'appareil. Pour effectuer cette tâche, procédez comme suit :

1. Connectez-vous à l'appliance SNA souhaitée via le protocole SSH (Secure Shell Protocol) ou directement via l'accès à la console.

   Note: Si vous avez besoin de collecter le pack de diagnostics à partir d'un matériel sans accès SSH, la console de machine virtuelle basée sur le noyau (KVM) de l'interface CIMC (Integrated Management Controller) de Cisco peut également être utilisée.

2. Connectez-vous avec les informations d'identification **racine**.
3. Entrez l'une des commandes suivantes (cela dépend de la version de SNA utilisée) :

   SNA version 7.1.x à 7.3.x

   Entrez la commande **doDiagPack**

   SNA version 7.4.x

Entrez la commande **diagnostics start**

4. Attendez que la tâche soit terminée.
5. Une fois la tâche terminée, le fichier du pack de diagnostics est stocké dans le **répertoire /lancope/var/admin/diagnostics/** avec un modèle de nom "**diagnostic-<type_périphérique>-<ID_périphérique>.<YYYYMMDD>.<HHMM>-*.tgz.gpg**"

```
smc:/# doDiagPack
smc:/# ls -l /lancope/var/admin/diagnostics/
total 32740
-rw-r--r-- 1 root root 33522766 Feb 24 02:29 diagnostic-SMC-SMCVE-VMware-4
        -6                .20220224.0227-public.tgz.gpg
smc:/#
```

6. Copiez le fichier généré depuis l'appliance vers votre ordinateur local ou vers un serveur de fichiers avec le protocole SCP (Secure Copy Protocol) ou avec un client SFTP (SSH File Transfer Protocol) tel que WinSCP. Le pack de diagnostics se trouve dans le répertoire **/lancope/var/admin/diagnostics/**.

   Note : Il est utile de mentionner que SNA version 7.4.0 a introduit une nouvelle fonctionnalité qui permet de générer le pack de diagnostics à partir du menu SystemConfig (CLI se connecte avec les informations d'identification **racine** > Enter **SystemConfig** > Navigate to **Recovery** > **Diagnostics Pack**).

   Pour plus d'informations sur cette méthode, consultez le Guide de configuration de Secure Network Analytics System 7.4.x.

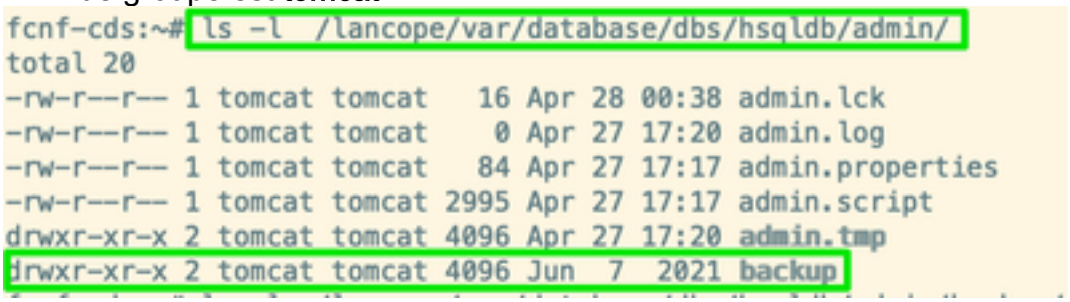
Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Il arrive que la création du pack de diagnostics échoue. Le symptôme le plus courant est lorsque vous recevez une erreur qui dit : « Une erreur s'est produite lors de la création du pack de diagnostics. Aucun fichier n'est disponible » après avoir cliqué sur le bouton **Créer un pack de diagnostics**.

Pour corriger ce comportement, procédez comme suit :

1. Connectez-vous à l'appliance qui a ce comportement avec les informations d'identification **racine** via SSH.
2. Exécutez la commande **ls -l /lancope/var/database/dbs/hsqldb/admin/** pour vérifier le contenu du répertoire.
3. Assurez-vous que le sous-répertoire **de sauvegarde** existe et que son utilisateur/propriétaire de groupe est **tomcat**.

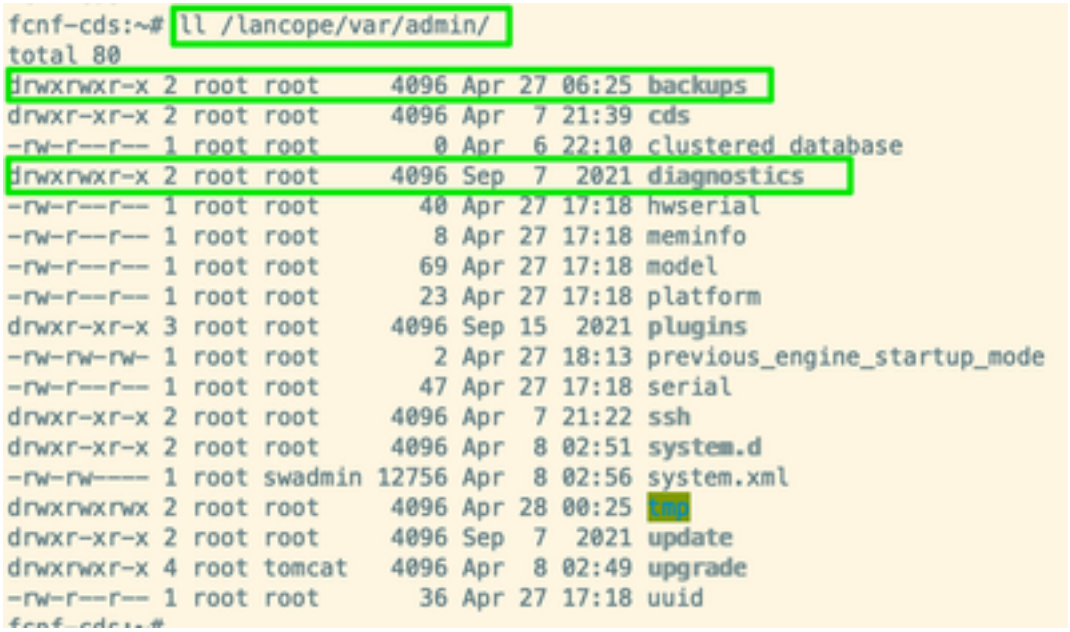


Si le sous-répertoire **de sauvegarde** n'existe pas dans le **/lancope/var/database/dbs/hsqldb/admin/**path, il doit être créé et la propriété correcte doit être attribuée. Pour cela, exécutez les commandes suivantes :

1. mkdir /lancope/var/database/dbs/hsqldb/admin/backup
2. chown tomcat : tomcat /lancope/var/database/dbs/hsqldb/admin/backup

4. Exécutez la commande **ls -l /lancope/var/admin/** pour vérifier le contenu du répertoire.

5. Assurez-vous que les sous-répertoires **des sauvegardes** et **diagnostics** existent et que leur propriétaire utilisateur/groupe est **racine**.



Si l'un ou l'autre des sous-répertoires mentionnés n'existe pas dans le chemin **/lancope/var/admin/**chemin, ils doivent être créés et la propriété correcte doit être attribuée. Pour cela, exécutez les commandes suivantes :

1. mkdir /lancope/var/admin/backup
2. mkdir /lancope/var/admin/diagnostics

Une fois cette vérification effectuée, essayez de générer à nouveau le pack de diagnostics de

l'appliance SNA.

Informations connexes

- Pour obtenir de l'aide supplémentaire, contactez le centre d'assistance technique Cisco (TAC). Un contrat d'assistance valide est requis : Coordonnées du service d’assistance Cisco à l’échelle mondiale.
- Support et documentation techniques - Cisco Systems