Comprendre les améliorations de la sécurité UCCE 12.5

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Vérification de l'ISO téléchargé

Utiliser des certificats avec SHA-256 et taille de clé 2048 bits

- Outil SSLUtil
- Commande DiagFwCertMgr

Outil de protection des données

Introduction

Ce document décrit les dernières améliorations de sécurité ajoutées avec Unified Contact Center Enterprise (UCCE) 12.5.

Conditions préalables

- UCCE
- Protocole SSL (Open Secure Sockets Layer)

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCCE 12,5
- Ouvrir SSL

Composants utilisés

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

- UCCE 12,5
- OpenSSL (64 bits) pour Windows

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.

Informations générales

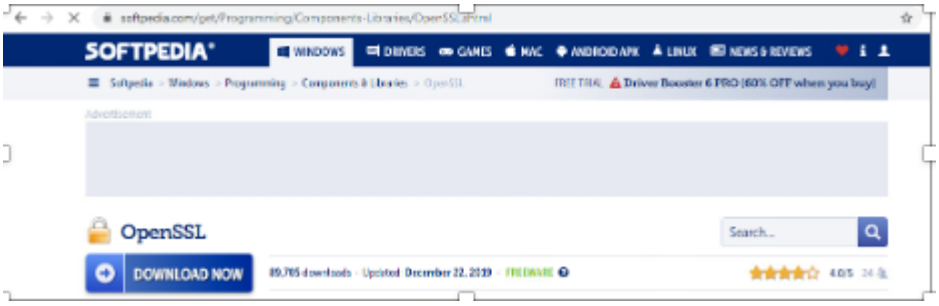
Cisco Security Control Framework (SCF) : Le cadre de contrôle de la sécurité de la collaboration fournit les directives de conception et de mise en oeuvre pour créer une infrastructure de collaboration sécurisée et fiable. Ces infrastructures résistent à la fois aux attaques connues et aux nouvelles formes d'attaques. Guide de référence sur la sécurité pour Cisco Unified ICM/Contact Center Enterprise, version 12.5 .

Dans le cadre de l'effort SCF de Cisco, des améliorations de sécurité supplémentaires sont ajoutées pour UCCE 12.5. Le présent document décrit ces améliorations.

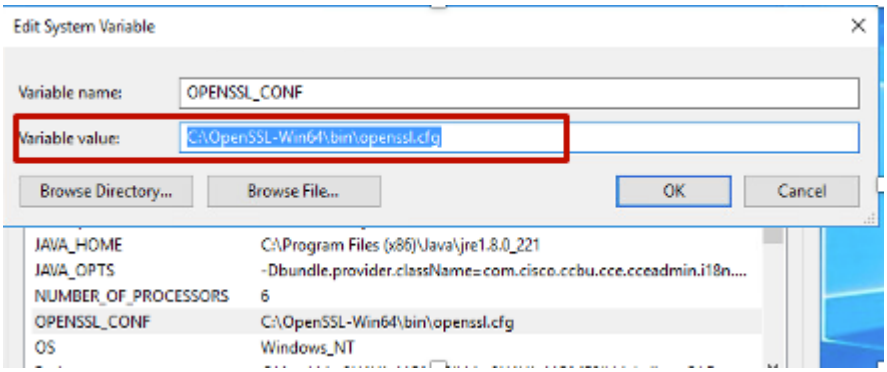
Vérification de l'ISO téléchargé

Afin de valider l'ISO téléchargé signé par Cisco et de s'assurer qu'il est autorisé, les étapes sont les suivantes :

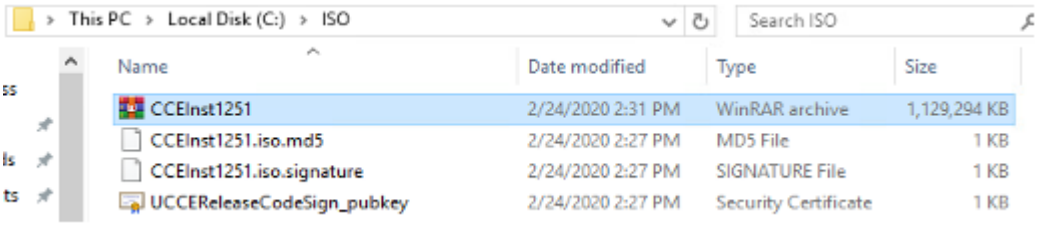
1. Téléchargez et installez OpenSSL. Recherchez le logiciel "openssl softpedia".



2. Confirmez le chemin (il est défini par défaut, mais toujours valide à vérifier). Sous Windows 10, accédez à Propriétés système, puis sélectionnez Variables d'environnement.



3. Fichiers nécessaires à la vérification ISO



4. Exécutez l'outil OpenSSL à partir de la ligne de commande.



5. Exécutez la commande

```
dgst -sha512 -keyform der -verify <public Key.der> -signature <ISO image.iso.signature> <ISO Image>
```

6. En cas d'échec, la ligne de commande affiche une erreur, comme illustré dans l'image



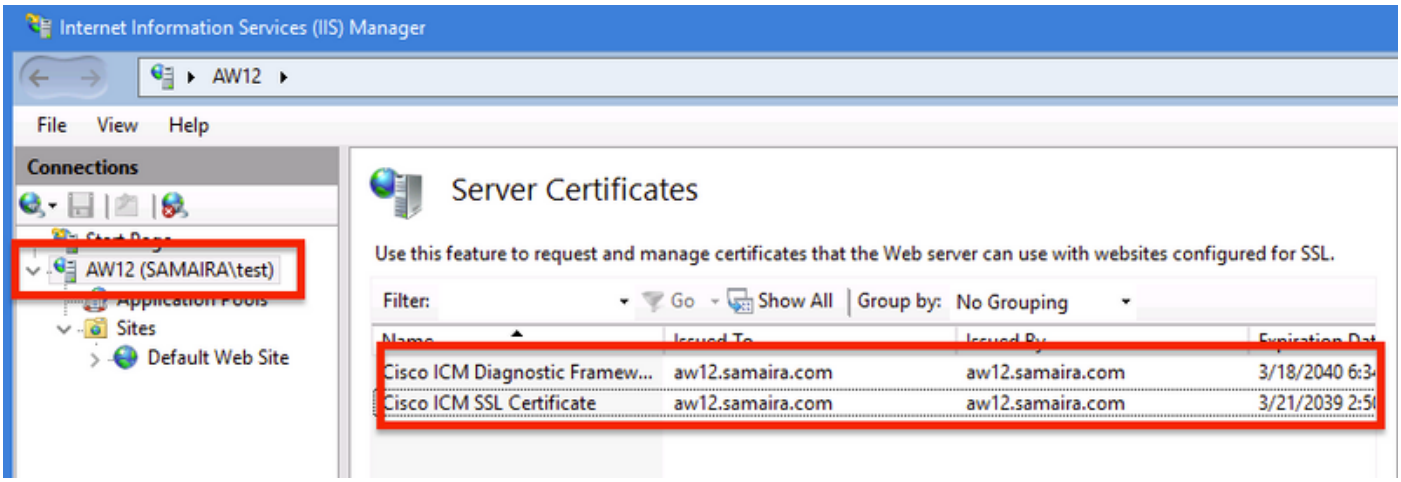
Utiliser des certificats avec SHA-256 et taille de clé 2048 bits

Les journaux signalent une erreur en cas d'identification de certificats non conformes (c'est-à-dire ne répondant pas à l'exigence de SHA-256 et/ou de taille de clé de 2048 bits).

Du point de vue d'UCCE, il existe deux certificats importants :

- Certificat de service Cisco ICM Diagnostic Framework
- Certificat SSL Cisco ICM

Les certificats peuvent être révisés dans l'option Gestionnaire des services Internet (IIS) du serveur Windows.



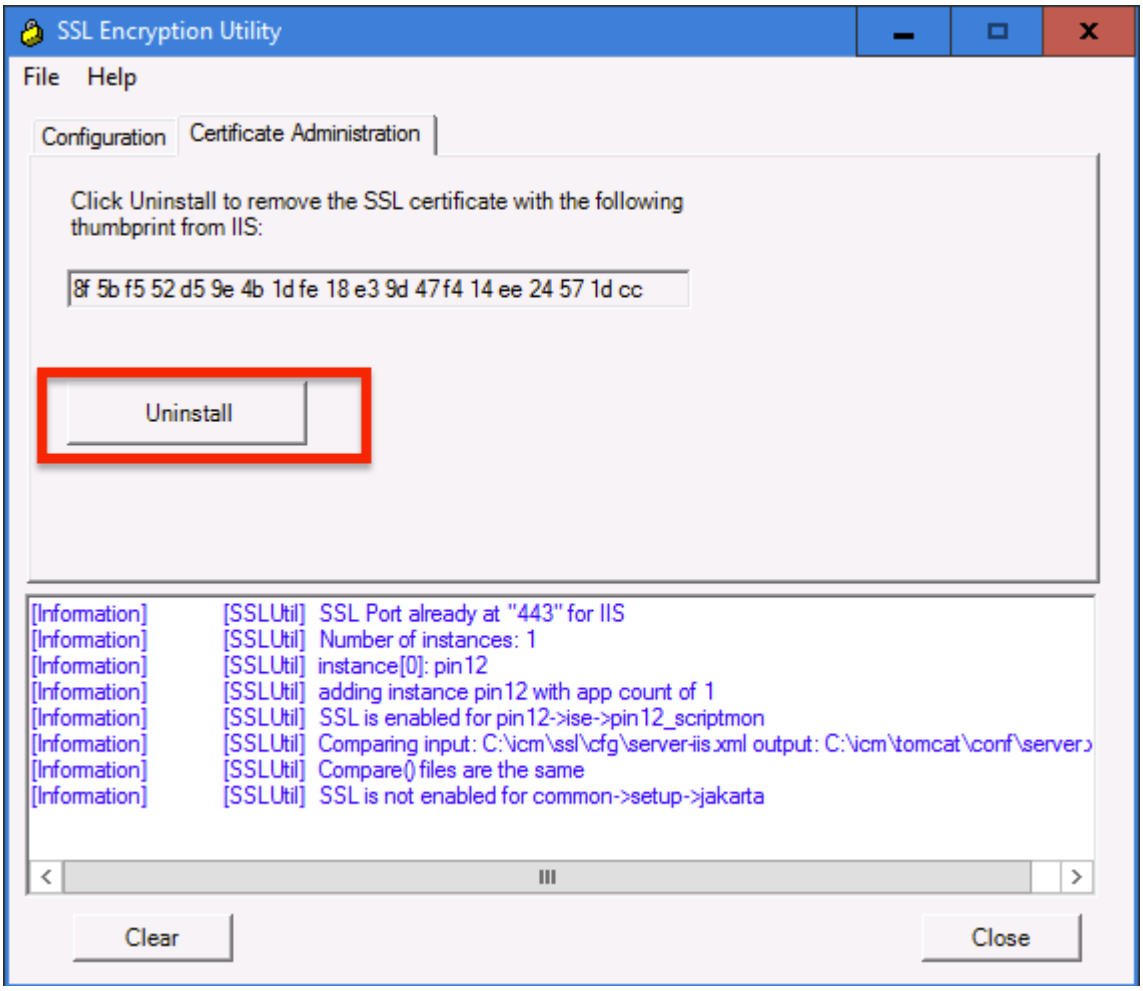
Pour les certificats auto-signés (pour Diagnose Portico ou Web Setup) , la ligne d'erreur signalée est la suivante :

```
Re-generating Cisco ICM SSL Certificate with SHA-256 and key size '2048' and will be binded with port 4
```

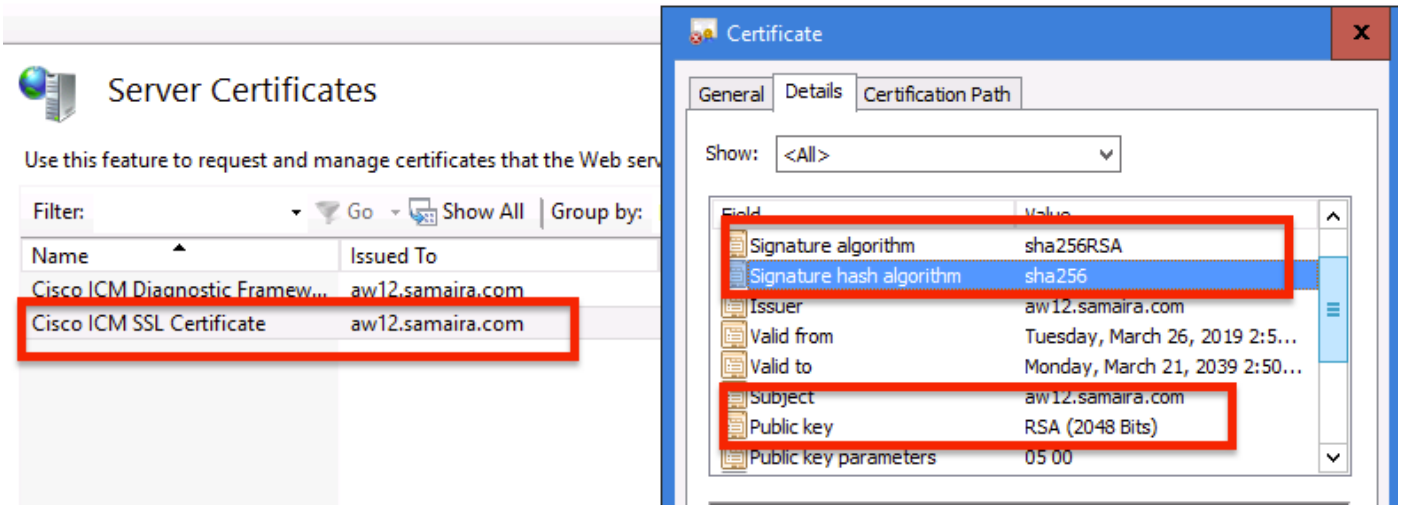
Outil SSLUtil

a. Pour régénérer des certificats auto-signés (pour la page WebSetup/CCEAdmin), utilisez l'outil SSLUtil (à partir de l'emplacement C:\icm\bin).

b. Sélectionnez Désinstaller pour supprimer le « Certificat SSL Cisco ICM » actuel.



c. Ensuite, sélectionnez Install in SSLUtil tool et une fois le processus terminé , notez que le certificat créé inclut désormais les bits SHA-256 et keysize '2048'.



Commande DiagFwCertMgr

Afin de régénérer un certificat auto-signé pour le certificat de service Cisco ICM Diagnostic Framework, utilisez la ligne de commande "DiagFwCertMgr", comme indiqué dans l'image :

```
C:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:CreateAndBindCert

********************************************************************
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
********************************************************************

Executing Task: 'CreateAndBindCert'
```

```
Deleted old binding successfully
Binding new certificate with HTTP service completed successfully
Found existing registry key for the service
Hash of certificate used saved in the service registry
ALL TASKS FOR BINDING THE CERTIFICATE WITH HTTP SERVICE COMPLETED SUCCESSFULLY


C:\icm\serviceability\diagnostics\bin>_
```

Outil de protection des données

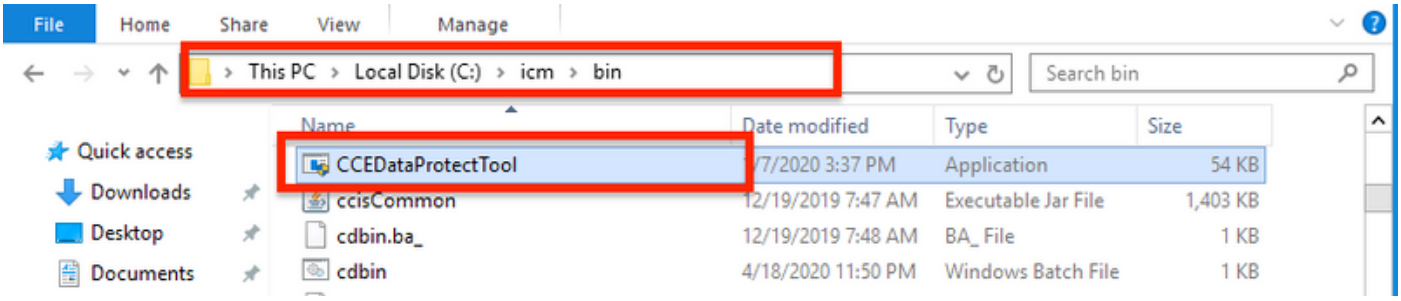
1. CCEDataProtectTool est utilisé pour chiffrer et déchiffrer les informations sensibles stockées dans le registre Windows. Après la mise à niveau vers SQL 12.5, le magasin de valeurs dans le registre SQLogin doit être reconfiguré avec CCEDataProtectTool. Seul un administrateur, un utilisateur de domaine disposant de droits d'administration ou un administrateur local peut exécuter cet outil.

2. Cet outil peut être utilisé pour afficher, configurer, modifier, supprimer la banque de valeurs chiffrées dans le registre SQLogin.

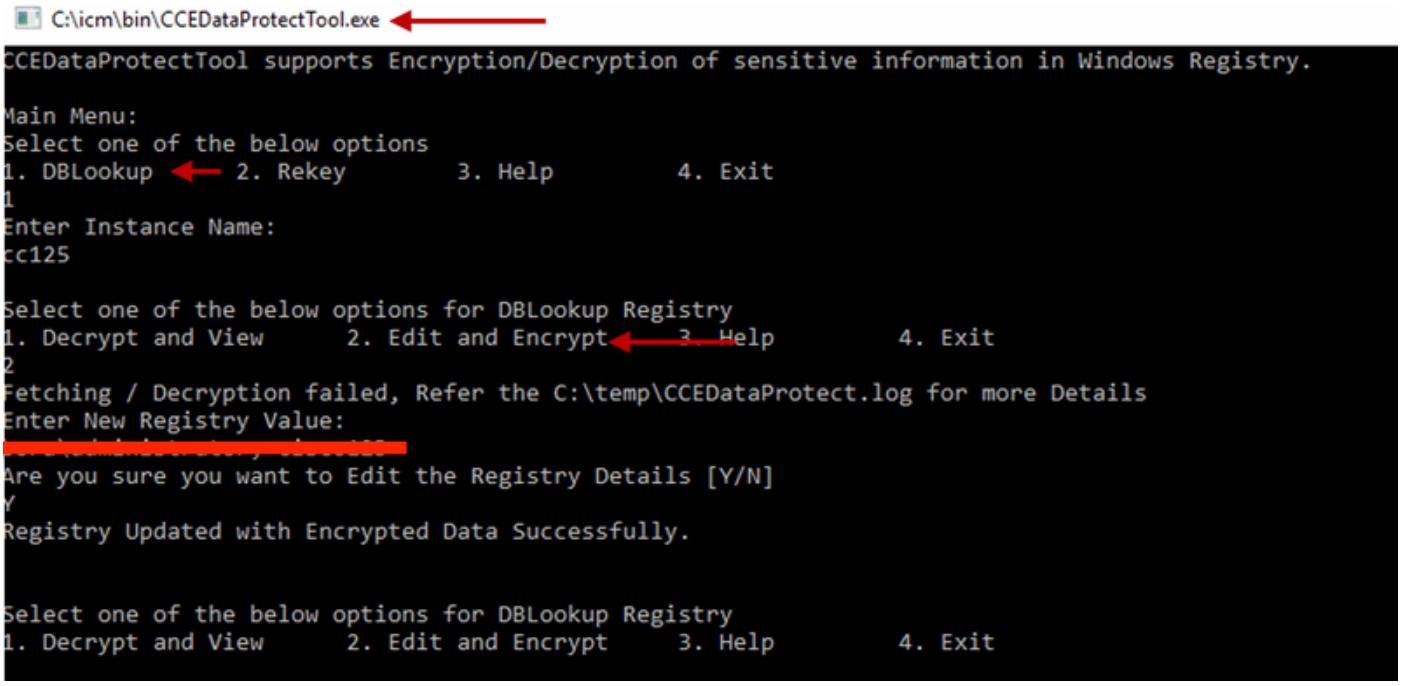
3. L'outil se trouve à l'emplacement ;

```
<Install Directory>:\icm\bin\CCEDataProtectTool.exe
```

4. Accédez à l'emplacement et double-cliquez sur CCEDataProtectTool.exe.

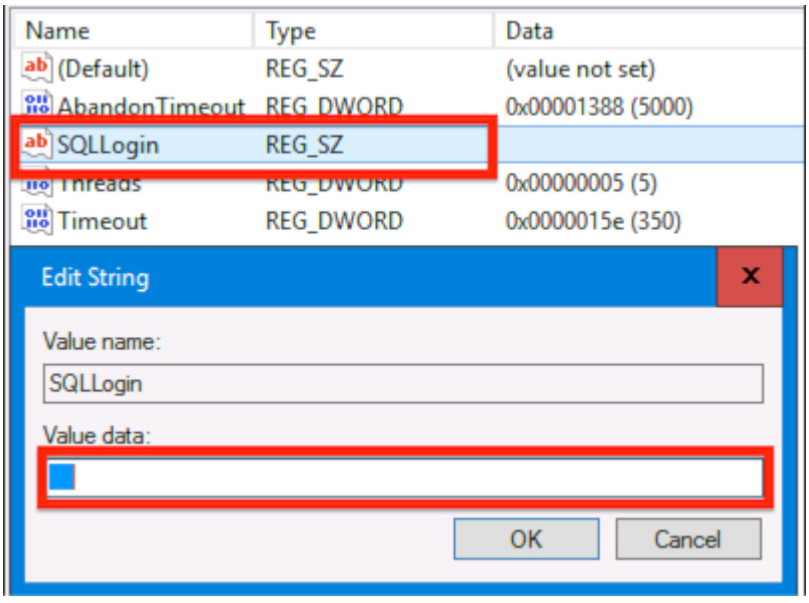


5. Pour chiffrer , appuyez sur 1 pour DBLookup, entrez Instance Name. Ensuite, appuyez sur 2 pour sélectionner « Edit and Encrypt » (Modifier et chiffrer)

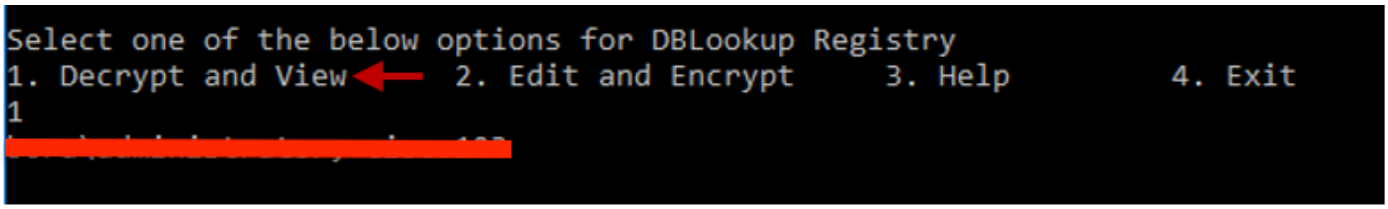


6. Naviguez jusqu'à l'emplacement du Registre et vérifiez que la valeur de chaîne SQLLogin semble vide , comme illustré dans l'image :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\pin12\RouterA\Router\CurrentVersion\Configuration\D
```



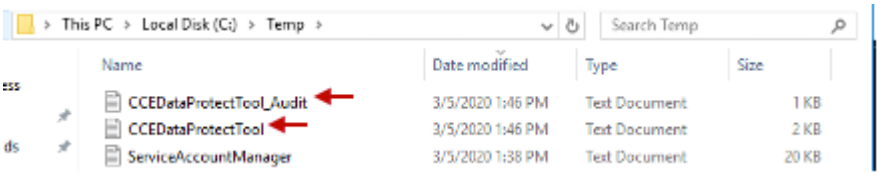
7. En cas de besoin de revoir la valeur chiffrée ; tandis que la ligne de commande de CCEDataProtectTool , sélectionnez appuyez sur 1 pour "Décrypter et afficher", comme illustré dans l'image ;



8. Tous les journaux de cet outil peuvent être trouvés dans l'emplacement ;

```
<Install Directory>:\temp

Audit logs filename : CCEDataProtectTool_Audit
CCEDataProtectTool logs : CCEDataProtectTool
```



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.