Dépannage de l'intégration d'Umbrella ISR4k

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Aperçu

Enregistrement et importation de certificats

Vérification de l'importation du certificat et de l'enregistrement du périphérique

Débogage et consignation

Introduction

Ce document décrit comment dépanner l'intégration d'Umbrella ISR4k

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

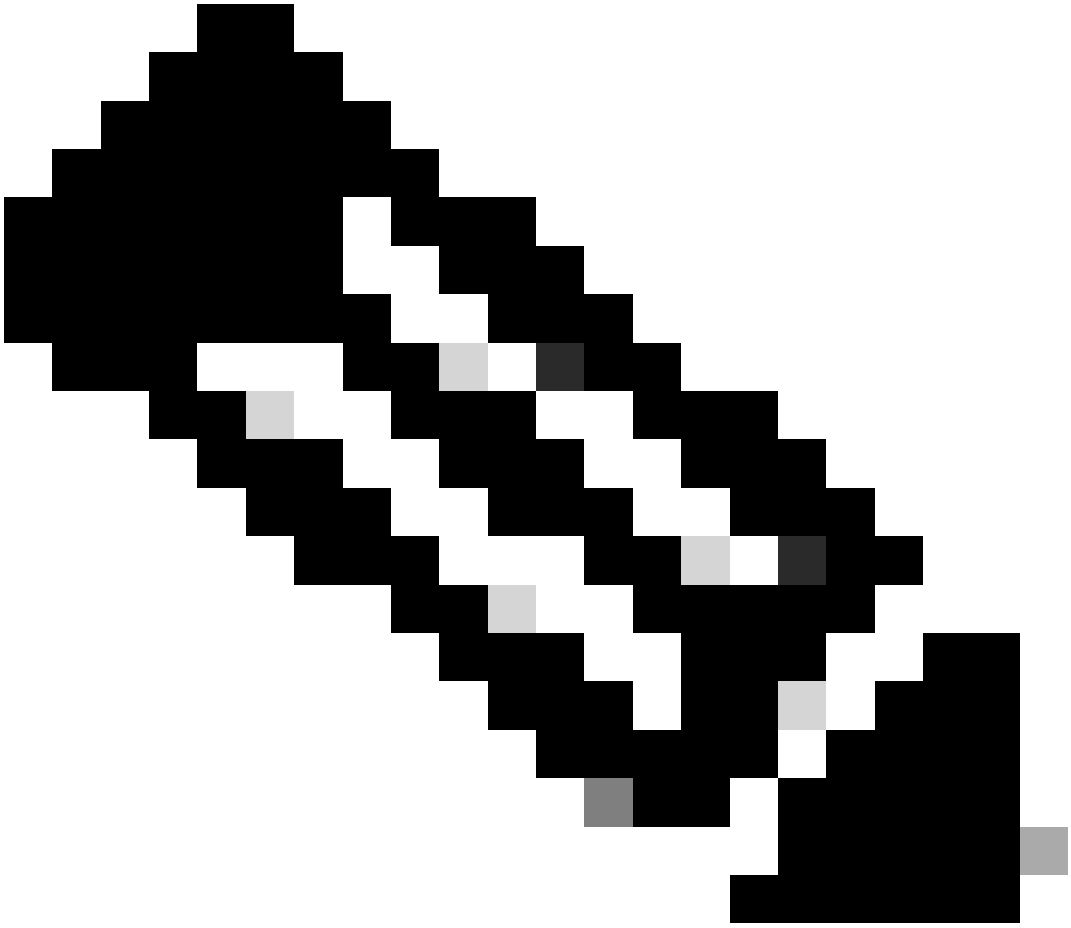
Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

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.

Aperçu

Cet article est une suite du guide de déploiement de Cisco Umbrella Integration pour ISR4k et est fourni comme un guide pour aider à résoudre les problèmes d'enregistrement, ainsi que les problèmes de résolution DNS interne et externe.



Remarque : Le certificat renouvelé pour api.opendns.com du 29 mai 2024 est maintenant signé par une nouvelle chaîne/intermédiaire/racine. La nouvelle racine est DigiCert Global Root G2 (série : 033af1e6a711a9a0bb2864b11d09fae5).

Enregistrement et importation de certificats

1. Obtenez votre jeton API à partir du tableau de bord Umbrella : Admin > Clés API > (créer) Périphériques réseau hérités.

2. Importez le certificat CA dans l'ISR4k via l'interface de ligne de commande en utilisant l'une des méthodes suivantes :

Importer depuis l'URL :
Exécutez la commande et autorisez ISR4k à récupérer le certificat :

```
crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

Importer directement dans le terminal :
Copiez et collez le certificat CA (voir pièce jointe) à l'aide de la commande suivante :

(Ce certificat est pour DigiCert Global Root G2.)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDExMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IEcyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuzfNNNx7a8myaJCtSnX/RrohCgiN9RlUyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHxmx
1x7e/dfgy5SDN67sH0NO3Xss0r0upS/kqbitOtSZpLYl6ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuumO6ZIya7XzV+hdG82MHauVBJVJ8zUtluNJbd134/tJS7SsVQepj5Wz
tCO7TG1F8PapspUwtP1MVYwnSlcUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vIOlCsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJobq7nMWxM4MphQIDAQABo0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rkS7QYXjzkwDQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Yl9PMWLSn/pvtsrF9+wX3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabAOUWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNU+MeKNhJ7jitralj41E6Vf8PlwUHBHQRFXGU7Aj64GxJUTFy8bJZ91
8rGOmaFvE7FBcf6IKshPECBV1/MUReXgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfjllDiIGknibVb63dDcY3fe0Dkhvld1927jyNxF1WW6LZZm6zNTfl
MrY=
-----END CERTIFICATE-----
```

Copiez et collez le certificat intermédiaire à l'aide de la commande suivante :

(Ce certificat est pour DigiCert Global G2 TLS RSA SHA256 2020 CA1.)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIEyDCCA7CgAwIBAgIQDPW9BitWAvR6uFAsI8zwZjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0yMTAzMzAwMDAwMDBaFw0zMTAzMjkyMzU5NTlaMFkxCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxMzAxBgNVBAMTKkRpZ2lDZXJ0IEdsb2Jh
bCBHMiBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMz3EGJPprtjb+2QUlbFbSd7ehJWivH0+dbn4Y+9lavyYEEV
cNsSAPonCrVXOFt9slGTcZUOakGUWzUb+nv6u8W+JDD+Vu/E832X4xT1FE3LpxDy
FuqrIvAxIhFhaZAmunjZlx/jfWardUSVc8is/+9dCopZQ+GssjoP8Oj812s3wWPc
3kbW2OX+fSP9kOhRBx5Ro1/tSUZUfyyIxfQTnJcVPAPooTncaQwywa8WV0yUR0J8
osicfebUTVSvQpmowQTCd5zWSOTOEeAqgJnwQ3DPP3Zr0UxJqyRewg2C/Uaoq2yT
zGJSQnWS+Jr6Xl6ysGHlHx+5fwmY6D36g39HaaECAwEAAaOCAYIwggF+MBIGA1Ud
EwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFHSFgMBmx9833s+9KTeqAx2+7c0XMB8G
A1UdIwQYMBaAFE4iVCAYlebjbuYP+vq5Eu0GF485MA4GA1UdDwEB/wQEAwIBhjAd
```

```
BgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwdgYIKwYBBQUHAQEEajBoMCQG
CCsGAQUFBzABhhhodHRwOi8vb2NzcC5kaWdpY2VydC5jb20wQAYIKwYBBQUHMAKG
NGh0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RH
Mi5jcnQwQgYDVR0fBDswOTA3oDWgM4YxaHR0cDovL2NybDMuZGlnaWNlcnQuY29t
L0RpZ2lDZXJ0R2xvYmFsUm9vdEcyLmNybDA9BgNVHSAENjA0MAsGCWCGSAGG/WwC
ATAHBgVngQwBATAIBgZngQwBAgEwCAYGZ4EMAQICMAgGBmeBDAECAzANBgkqhkiG
9w0BAQsFAAOCAQEAkPFwyyiXaZd8dP3A+iZ7U6utzWX9upwGnIrXWkOH7U1MVl+t
wcW1BSAuWdH/SvWgKtiwla3JLko716f2b4gp/DA/JIS7w7d7kwcsr4drdjPtAFVS
slme5LnQ89/nD/7d+MS5EHKBCQRfz5eeLjJ1js+aWNJXMX43AYGyZmOpGrFmCW3R
bpD0ufovARTFXFZkAdl9h6g4U5+LXUZtXMYnhIHUfoyMo5tS58aI7Dd8KvvwVVo4
chDYABPPTHPbqjc1qCmBaZx2vN4Ye5DUys/vZwP9BFohFrH/6j/f3IL16/RZkiMN
JCqVJUzKoZHm1Lesh3Sz8W2jmdv51b2EQJ8HmA==
-----END CERTIFICATE-----
```

3. Entrez le jeton API dans l'interface de ligne de commande ISR4k à l'aide de la commande :

```
parameter-map type umbrella global
token XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

4. Voici l'exemple de configuration minimale sur ISR4k :

```
interface GigabitEthernet0/0/0
ip address 192.168.50.249 255.255.255.252
ip nat outside
umbrella out

interface GigabitEthernet0/0/1.10
encapsulation dot1Q 10
ip address 192.168.8.254 255.255.255.0
ip nat inside
umbrella in odns_v10_5
```

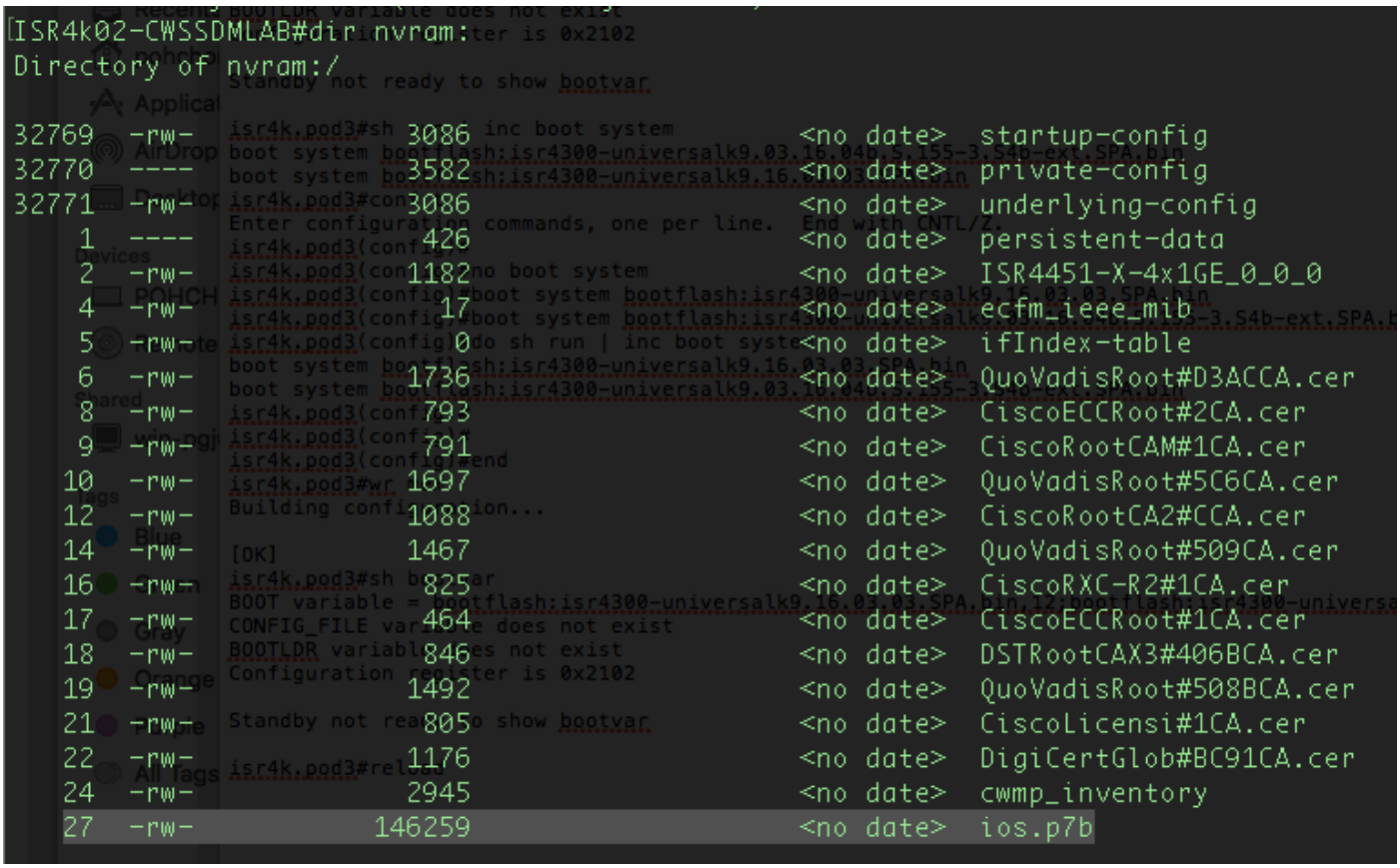
Informations supplémentaires:

- Assurez-vous de configurer la commande « umbrella out » avant la commande « umbrella in ».
- L'enregistrement ne peut réussir que lorsque le port 443 est dans un état ouvert et permet au trafic de traverser n'importe quel pare-feu existant.
- Dans l'ancienne version de Cisco IOS XE Denali, la commande OpenDNS est utilisée à la place d'Umbrella.

Vérification de l'importation du certificat et de l'enregistrement du périphérique

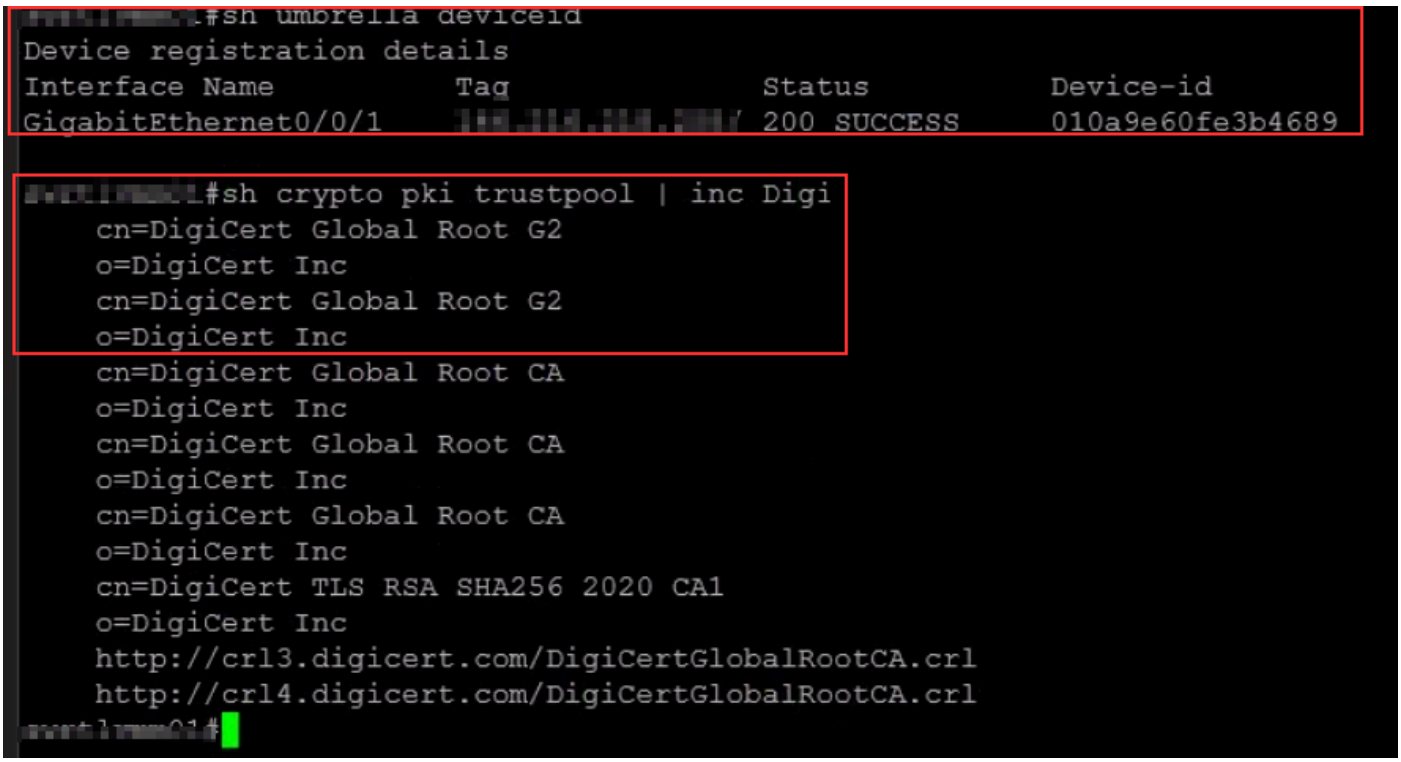
1. Vérifiez si le certificat CA a été correctement stocké sur le périphérique ISR4k :

- Si l'importation du certificat a été effectuée à l'aide de l'URL, émettez la commande `dir nvram:` pour vérifier que le certificat ios.p7b est correctement stocké dans la mémoire vive non volatile du périphérique.



115016968663

- Si l'importation du certificat a été effectuée à l'aide de la méthode copier/coller, exécutez la commande `show cry pki trustpool` et vérifiez le numéro de série et cn du certificat :



28552066223252

2. Pour vérifier que l'enregistrement de l'ISR4k a réussi, exécutez la commande `show umbrella device id`.

Exemple de sortie :

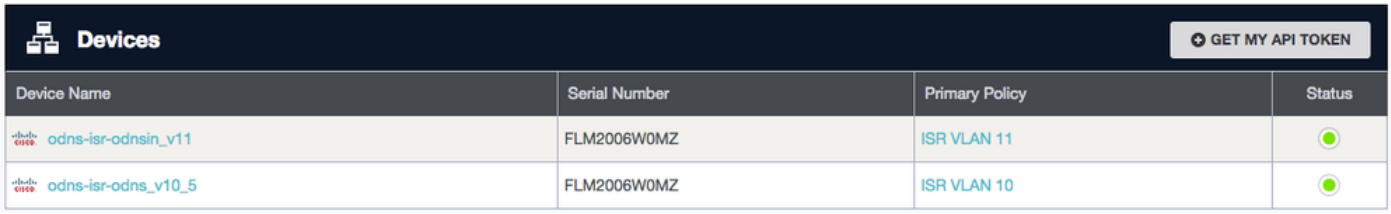
```
Device registration details

Interface Name                          Tag             Status       Device Id

interface GigabitEthernet0/0/1.10     odns_v10_5     200 SUCCES    010a04efd4e4bc14

interface GigabitEthernet0/0/1.11     odns_v11       200 SUCCES    010a04efd4e4xy15
```

Sortie du tableau de bord :



115016791766

Débogage et consignation

- Vérifiez la version ISR4k : `show version` ou `show platform` (requis pour Cisco IOS XE Denali 16.3 ou version ultérieure)
- Activer les journaux de débogage d'enregistrement des périphériques : "`debug umbrella device-registration`" puis "`show logging`" (pour désactiver - `no debug umbrella device-registration`)

Voici des exemples de journaux :

Certificat manquant :

```
Jun 13 04:05:32.639: %OPENDNS-3-SSL_HANDSHAKE_FAILURE: SSL handshake failed
```

Le certificat est installé et le périphérique est correctement enregistré :

```
*%PKI-6-TRUSTPOOL_DOWNLOAD_SUCCESS: Trustpool Download is successful
*%OPENDNS-6-DEV_REG_SUCCESS: Device id for interface/tag GigabitEthernet0/0/1/odns_v10_5 is 010a0e4bc14
```

Api.opendns.com n'est pas résoluble :

<#root>

*%UMBRELLA-3-DNS_RES_FAILURE:

Failed to resolve name api.opendns.com

Retry attempts:0

- Vérifiez la résolution DNS : Aucune commande « dig » ou « nslookup » n'est disponible sur ISR4k. Il est préférable d'utiliser « `ping hostname source interface #` » à partir de l'interface de ligne de commande ISR4k
- ISR avec VRF configuré : Sur l'interface, assurez-vous que « `ip name-server vrf <vrf_name> <dns_server_ip>` » est configuré et vérifiez avec « `ping vrf <vrf_name> api.opendns.com` »
- Assurez-vous que « ip dns server » est configuré : Cela permet d'interroger directement le routeur de service intégré.
- Pour désactiver DNSCrypt, entrez cette commande : `parameter-map type umbrella global > no dnscrypt`
- Vérification du domaine interne : exécutez la commande `show umbrella config` et recherchez le domaine local Regex, par exemple :
  - `show umbrella config` > Local Domain Regex parameter-map : contournement DNS
  - `Commande show run | be dns_bypass`
  - `show platform hardware qfp active feature dns-snoop-agent client hw-pattern-list`
- Impossible d'importer le certificat à l'aide de l'URL ou le certificat importé à l'aide du terminal est supprimé après redémarrage :

crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b

% Error: failed to open file.

% No certificates imported from http://www.cisco.com/security/pki/trs/ios.p7b.

Solution : téléchargez manuellement l'ensemble de certificats « ios.p7b » via curl et copiez-le dans la mémoire flash du routeur > Effacez le certificat existant du pool > Importez l'ensemble de certificats « ios.p7b » de la mémoire flash :

<#root>

Show run | sec crypto pki

crypto pki certificate pool

cabundle nvram:Trustpool15.cer

crypto pki trustpool clean

```
crypto pki trustpool import url flash:ios.p7b
Reading file from bootflash:ios.p7b
% PEM files import succeeded.
```

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.