

Défaillances de la licence ASA Smart dues à des problèmes de certificat

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Problème](#)

[Syslogs et sortie de débogage](#)

[Solution](#)

[Vérifier](#)

[Modification du certificat CA racine - Octobre 2018](#)

[Plates-formes 4100/9300 exécutant ASA](#)

[Étapes de résolution](#)

[Installations logicielles ASA nécessitant la conformité aux normes FIPS \(Federal Information Processing Standards\)](#)

[Informations connexes](#)

Introduction

Ce document décrit comment déterminer les échecs de licences Smart ASA qui sont dus à un échec de connexion de certificat.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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

Ce document décrit comment traiter une modification qui s'est produite en mars 2016 et en octobre 2018, dans laquelle les serveurs Web qui hébergent tools.cisco.com ont été migrés vers un certificat d'autorité de certification (CA) racine différent. Après cette migration, certains périphériques ASA (Adaptive Security Appliance) ne parviennent pas à se connecter au portail Smart Software Licensing Portal (hébergé sur tools.cisco.com) lorsqu'ils enregistrent un jeton d'identification ou lorsqu'ils tentent de renouveler les autorisations actuelles. Il a été déterminé qu'il s'agissait d'un problème lié au certificat. Plus précisément, le nouveau certificat qui est présenté à l'ASA est signé par une autorité de certification intermédiaire différente de celle attendue par l'ASA et a été préchargé.

Problème

Lorsqu'une tentative d'enregistrement d'un ASAv sur le portail de licences logicielles Smart échoue, l'enregistrement échoue avec un échec de connexion ou de communication. Les commandes `show license registration` et `call-home test profile license` affichent ces résultats.

```
<#root>
```

```
ASAv#
```

```
show license registration
```

```
Registration Status: Retry In Progress.  
Registration Start Time: Mar 22 13:25:46 2016 UTC  
Registration Status: Retry In Progress.  
Registration Start Time: Mar 22 13:25:46 2016 UTC  
Last Retry Start Time: Mar 22 13:26:32 2016 UTC.  
Next Scheduled Retry Time: Mar 22 13:45:31 2016 UTC.  
Number of Retries: 1.  
Last License Server response time: Mar 22 13:26:32 2016 UTC.  
Last License Server response message:
```

```
Communication message send response error
```

```
<#root>
```

```
ASAv#
```

```
call-home test profile License
```

```
INFO: Sending test message to DDCEService  
ERROR: Failed:
```

```
CONNECT_FAILED(35)
```

Cependant, ASAv peut résoudre tools.cisco.com et se connecter sur le port TCP 443 avec une requête ping TCP.

Syslogs et sortie de débogage

La sortie Syslog sur ASA v après une tentative d'enregistrement peut montrer ceci :

<#root>

[%ASA-3-717009](#): Certificate validation failed. No suitable trustpoints found to validate certificate serial number: 250CE8E030612E9F2B89F7058FD, subject name: cn=VeriSign Class 3 Public Primary Certification Authority - G5,ou=(c) 2006 VeriSign\, Inc. - For authorized use only,ou=VeriSign Trust Network,o=VeriSign\, Inc.,c=US, issuer name: ou=Class 3 Public Primary Certification Authority,o=VeriSign\, Inc.,c=US .

[%ASA-3-717009](#): Certificate validation failed. No suitable trustpoints found to validate certificate serial number: 513FB9743870B73440418699FF, subject name:

cn=Symantec Class 3 Secure Server CA - G4

,ou=Symantec Trust Network,o=Symantec Corporation,c=US, issuer name: cn=VeriSign Class 3 Public Primary Certification Authority - G5,ou=(c) 2006 VeriSign\, Inc. - For authorized use only,ou=VeriSign Trust Network, o=VeriSign\, Inc.,c=US .

Pour plus d'informations, exécutez ces commandes de débogage pendant que vous tentez une autre inscription. Des erreurs Secure Socket Layer sont détectées.

```
debug license 255
debug license agent all
debug call-home all
debug ssl 255
```

Plus précisément, ce message est considéré comme faisant partie de cette sortie :

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify
failed@s3_cInt.c:1492
```

Dans la configuration ASA v par défaut, il y a un point de confiance appelé `_SmartCallHome_ServerCA` qui a un certificat chargé et émis pour le nom de sujet "cn=Verisign Class 3 Secure Server CA - G3".

<#root>

ASA v#

```
show crypto ca certificate
```


```
CA Certificate
  Status: Available
  Certificate Serial Number: 6ecc7aa5a7032009b8cebc2d491
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
```

```
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
  cn=VeriSign Class 3 Public Primary Certification Authority - G5
  ou=(c) 2006 VeriSign\, Inc. - For authorized use only
  ou=VeriSign Trust Network
  o=VeriSign\, Inc.
  c=US
Subject Name:

  cn=VeriSign Class 3 Secure Server CA - G3

  ou=Terms of use at https:// verisign /rpa (c)10
  ou=VeriSign Trust Network
  o=VeriSign\, Inc.
  c=US
OCSP AIA:
  URL: http://ocsp verisign
CRL Distribution Points:
  [1] http://crl verisign/pca3-g5.crl
Validity Date:
  start date: 00:00:00 UTC Feb 8 2010
  end   date: 23:59:59 UTC Feb 7 2020
Associated Trustpoints: _SmartCallHome_ServerCA
```

Cependant, dans les syslogs précédents, l'ASA indique qu'il obtient un certificat du portail Smart Software Licensing Portal signé par un intermédiaire appelé "cn=Symantec Class 3 Secure Server CA - G4".

 Remarque : les noms des sujets sont similaires, mais ils présentent deux différences : Verisign vs Symantec au début et G3 vs G4 à la fin.

Solution

ASAv doit télécharger un pool de confiance qui contient les certificats intermédiaires et/ou racine appropriés afin de valider la chaîne.

Dans les versions 9.5.2 et ultérieures, le pool de confiance de l'ASAv est configuré pour l'importation automatique à 22:00 heure locale du périphérique :

```
<#root>
```

```
ASAv#
```

```
sh run crypto ca trustpool
```

```
crypto ca trustpool policy
  auto-import
```

```
ASAv#
```

```
sh run all crypto ca trustpool
```

```
crypto ca trustpool policy
```

```
revocation-check none
cr1 cache-time 60
cr1 enforcenextupdate
auto-import
auto-import url http://www.cisco.com/security/pki/trs/ios_core.p7b
auto-import time 22:00:00
```

S'il s'agit d'une installation initiale et que les recherches DNS (Domain Name System) et la connectivité Internet n'ont pas encore été activées, l'importation automatique n'a pas réussi et doit être effectuée manuellement.

Sur les versions antérieures, telles que 9.4.x, l'importation automatique trustpool n'est pas configurée sur le périphérique et doit être importée manuellement.

Quelle que soit la version, cette commande importe le pool de confiance et les certificats appropriés :

```
<#root>
```

```
ASAv#
```

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

```
Root file signature verified.
```

```
You are about to update the current trusted certificate pool
```

```
with the 17145 byte file at http://www.cisco.com/security/pki/trs/ios_core.p7b
```

```
Do you want to continue? (y/n)
```

```
Trustpool import:
```

```
  attempted: 14
```

```
  installed: 14
```

```
  duplicates: 0
```

```
  expired: 0
```

```
  failed: 0
```

Vérifier

Une fois que le pool de confiance est importé soit par la commande manuelle, soit après 22h00, heure locale, cette commande vérifie qu'il y a des certificats installés dans le pool de confiance :

```
<#root>
```

```
ASAv#
```

```
show crypto ca trustpool policy
```

```
14 trustpool certificates installed
```

```
Trustpool auto import statistics:
```

```
  Last import result: FAILED
```


```
  Next scheduled import at 22:00:00 UTC Wed Mar 23 2016
```

```
Trustpool Policy
```

```
  Trustpool revocation checking is disabled
```

```
  CRL cache time: 60 seconds
```

```
CRL next update field: required and enforced
Automatic import of trustpool certificates is enabled
Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
Download time: 22:00:00
Policy Overrides:
  None configured
```

 Remarque : dans la sortie précédente, la dernière importation de mise à jour automatique a échoué car le DNS n'était pas opérationnel la dernière fois qu'il a tenté automatiquement, de sorte qu'il affiche toujours le dernier résultat d'importation automatique comme ayant échoué. Cependant, une mise à jour manuelle du pool de confiance a été exécutée et a réussi à mettre à jour le pool de confiance (c'est pourquoi il affiche 14 certificats installés).

Une fois le pool de confiance installé, la commande d'enregistrement de jeton peut être exécutée à nouveau afin d'enregistrer l'ASAv avec le portail de licences logicielles Smart.

```
<#root>
```

```
ASAv#
```

```
license smart register idtoken id_token force
```

Si l'ASAv a déjà été enregistré sur le portail de gestion des licences Smart Software, mais que les renouvellements d'autorisation ont échoué, ces tentatives peuvent également être effectuées manuellement.

```
<#root>
```

```
ASAv#
```

```
license smart renew auth
```

Modification du certificat CA racine - Octobre 2018

Le certificat d'autorité de certification racine pour tools.cisco.com a été modifié le vendredi 5 octobre 2018.

Les versions 9.6(2) et ultérieures de l'appliance ASAv actuellement déployée et l'appliance ASA exécutant Firepower 2100 ne peuvent pas être affectées par cette modification si la communication vers http://www.cisco.com/security/pki/trs/ios_core.p7b n'est pas autorisée. Il existe une fonction d'importation automatique de certificat qui est activée par défaut sur toutes les plates-formes ASA sous licence Smart mentionnées ci-dessus. La sortie de « show crypto ca trustpool » contient le certificat « QuoVadis Root CA 2 » :

CA Certificate

Fingerprint: 5e397bddf8baec82e9ac62ba0c54002b

Issuer Name:

cn=QuoVadis Root CA 2

o=QuoVadis Limited

c=BM

Subject Name:

cn=QuoVadis Root CA 2

o=QuoVadis Limited

c=BM

Pour les nouveaux déploiements, vous pouvez exécuter la commande « crypto ca trustpool import default » et télécharger l'ensemble de certificats Cisco par défaut qui contient le certificat QuoVadis. Si cela ne fonctionne pas, vous pouvez installer le certificat manuellement :

```
asa(config)# crypto ca trustpoint QuoVadisRootCA2
asa(config-ca-trustpoint)# enrollment terminal
asa(config-ca-trustpoint)# crl configure
asav(config-ca-crl)# crypto ca authenticate QuoVadisRootCA2
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

-----BEGIN CERTIFICATE-----

```
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAKGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZG1zIEExpbW10ZWQxGzAZBgNVBAMTE1F1b1ZhZG1zIFJv
b3QgQ0EgMjAeFw0wNjExMjQzODIzMDBaFw0zMTExMjQzODIzMzNaMEUxCzAJBgNV
BAYTAKJNMkRwYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYy
BAYTAKJNMkRwYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYy
YWRpcyBSb290IENBIDwggIiMAOGCsqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpL1A0ALa8DKYrwd4HIrkwZhr0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKiFvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yk1vc/u1srHh01wtZn/qtmUIttKGAr79dgv8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbB1DePSHFjIuwXZQeVi kvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9X0va7R+zdRcAi tMOeGylZUtQofX1b0Q07dsE/He3fbE+Ik/OXX1
ksOR1YqI0JDs3G3eicJ1cZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUR5R/7mp/i
Ucw6UwxI5g69ybR2B1LmEROFcmMDBOAEInsgGQLodKcfts1WZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/z0hD7osFRXq17PSorW+8oyWHhQPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFWdwzqLID9ujWc90tb+fVuI
yV77zGHci zN300QyNQ1iBJIWIENieJ0f70yHj+0sdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAF8wCwYDVR0PBAQDAgEGMBOGA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMZzB1gBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEwRTEL
MAKGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZG1zIEExpbW10ZWQxGzAZBgNVBAMT
E1F1b1ZhZG1zIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4Kfk2f
B1uornFdLwUvZ+YTRYPENvbzcmYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae4219NLmeyhP3ZRPx3UIHmFLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2B1
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WPKjaJw1acvvFYfzbnB4vsKqBusFU16Y8Zs10Q80m/DSHck+JDSV6IZUaUt10Ha
B0+pUNqQjZRG4T7w1POQADj10+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIpM0661V6bYCZJPVSAfv417CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQ1fe6yJvmjqIBxdZmv31h8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkG3Go3XZZenMfvJ2II4pEZXLXId26F0KC13GBUZGpn/Z9Yr9y
4a0THcyKJ1oJONDO1w2AFrR4pTqHTI2KpdVG1/IsELm8VCLAABpQ570su9t+Oza
8e0x79+Rj1QqCyXBjhnEUhAFZdwCEOrCMc0u
```

-----END CERTIFICATE-----

quit

INFO: Certificate has the following attributes:
Fingerprint: 5e397bdd f8baec82 e9ac62ba 0c54002b
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Plates-formes 4100/9300 exécutant ASA

Ce problème a affecté certains 4100/9300 sur le terrain qui exécutent ASA qui s'appuie sur Firepower eXtensible Operating System (FXOS) pour fournir des informations sur les licences Smart :

Unité concernée :

<#root>

```
FP9300-1-A-A-A /license # show license all
```

Smart Licensing Status

=====

Smart Licensing is ENABLED

Registration:

Status: REGISTERED

Smart Account: TAC Cisco Systems, Inc.

Virtual Account: CALO

Export-Controlled Functionality: Allowed

Initial Registration: SUCCEEDED on Jul 01 18:37:38 2018 UTC

Last Renewal Attempt: FAILED on Oct 09 17:32:59 2018 UTC

Failure reason: Failed to authenticate server

Étapes de résolution

Pour résoudre le problème, vous devez créer un nouveau point de confiance et entrer les données de certificat dans FXOS :

<#root>

```
FPR-2-A /license # scope security
```

```
FPR-2-A /security # enter trustpoint QuoVadisRootCA2
```

```
FPR-2-A /security/trustpoint* # set certchain
```

Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.

Trustpoint Certificate Chain: (THIS PART NEEDS TO BE COPY/PASTED)

>

-----BEGIN CERTIFICATE-----

MIIIFtzCCA5+gAwIBAgICBQkwdQYJKoZIhvcNAQEFBQAwRTElMAkGA1UEBhMCQk0x


```
GTAXBgNVBAoTEFF1b1ZlZG1zIEExpbW10ZWQxGzAZBgNVBAMTE1F1b1ZlZG1zIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODIzMDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAKJNMkRwFwYDVQQKExBRdW9WYWRpcyBMAw1pdGVkMRswGQYDVQQDExJRdW9W
YWRpcyBSb290IENBIDlwggIiMAOGCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpL1A0ALa8DKYrWd4HIRkVhR0In6spRlXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yk1vc/u1srHh01wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUwD4gXmuVbB1DePSHFjIuwXZQeVikvfj8ZaCuWw419eagGrDPmF60Tp
+ARz8un+XJiM9X0va7R+zdRcAitMOeGylZUtQofX1b0QQ7dsE/He3fbE+Ik/OXX1
ks0R1YqI0JDs3G3eicJlZcZaLdQP9nL9bFqyS2+r+eXyt66/3FsvbzSUR5R/7mp/i
Ucw6UwXI5g69ybr2B1LmEROfcmMDBOAEInsgGQLodKcfts1WZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXby0D/5YDXC20g
/z0hD7osFRXq17PSorW+8oyWHhQPHWykYTe5hnMz15eWniN9ggRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFWdwzqLID9ujWc90tb+fVuI
yV77zGHciZn300QyNQ1iBJIWIENieJ0f70yHj+0sdWwIDAQBo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAF8wCwYDVR0PBAQDAgEGMBOGA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMZzB1gBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAKGA1UEBMCk0xGTAXBgNVBAoTEFF1b1ZlZG1zIEExpbW10ZWQxGzAZBgNVBAMT
E1F1b1ZlZG1zIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4Kfk2f
B1uornFdLwUvZ+YTRYPENvbzWcYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae4219NLmeyhP3ZRPx3UIHmFLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2B1
FF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WPKjaJW1acvvyFyzznB4vsKqBU5fU16Y8Zs10Q80m/DShcK+JDSV6IZUaUt10Ha
B0+pUnQjZRG4T7w1POQADj10+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIoZc
hLsib9D45MY56QSIpM0661V6bYCZJPVsAfv417CUw+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQ1fe6yJvmjqIBxdZmv31h8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3GoI3XZzenMfvJ2II4pEZXNLxId26F0KC13GBUzGpn/Z9Yr9y
4a0THcyKJ1oJONDO1w2AFrR4pTqHTI2KpdVG1/IsELm8VCLAABpQ570su9t+Oza
8e0x79+rj1QqCyXBjHnEUhAFZdwCEOrCMc0u
-----END CERTIFICATE-----
>ENDOFBUF
```

<---manually type this on a new line after the -----END OF CERTIFICATE----- line and press ENTER

Validez ensuite la modification, puis renouvelez la licence :

```
FPR-2-A /security/trustpoint* # comm
FPR-2-A /security/trustpoint # scope license
FPR-2-A /license # scope licdebug
FPR-2-A /license/licdebug # renew
```

Vous devez maintenant vérifier que la licence a été renouvelée :

<#root>

```
FP9300-1-A-A-A /license/licdebug # show license all
```

```
Smart Licensing Status
=====
```

```
Smart Licensing is ENABLED
```

Registration:

Status: REGISTERED
Smart Account: TAC Cisco Systems, Inc.
Virtual Account: CALO
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Jul 01 18:37:38 2018 UTC
Last Renewal Attempt: SUCCEEDED on Oct 09 17:39:07 2018 UTC
Next Renewal Attempt: Apr 07 17:39:08 2019 UTC
Registration Expires: Oct 09 17:33:07 2019 UTC

License Authorization:

Status: AUTHORIZED on Oct 09 17:39:12 2018 UTC
Last Communication Attempt: SUCCESS on Oct 09 17:39:12 2018 UTC
Next Communication Attempt: Nov 08 17:39:12 2018 UTC
Communication Deadline: Jan 07 17:33:11 2019 UTC

Installations logicielles ASA nécessitant la conformité aux normes FIPS (Federal Information Processing Standards)

Pour les plates-formes ASA qui nécessitent la conformité FIPS, l'importation du certificat QuoVadis Root CA 2 peut échouer pour non-conformité aux exigences de cryptographie de signature et ce message peut être affiché :

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate is not FIPS compliant.
% Error in saving certificate: status = FAIL

Comme solution de contournement pour les installations ASA conformes à la norme FIPS, importez le certificat intermédiaire HydrantID SSL ICA G2. Le certificat HydrantID SSL ICA G2 est affiché ci-dessous et est conforme aux exigences de l'algorithme de signature sha256WithRSAEncryption. Reportez-vous à la documentation présentée dans cet article afin de charger le certificat basé sur votre plate-forme :

-----BEGIN CERTIFICATE-----
MIIGxDCCBKyGAWIBAgIUdRcWd4PQQ361VsNX1G5FY7jr06wwDQYJKoZIhvcNAQEL
BQAwRTElMAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZlZG1zIEExpbW10ZWQxGzAZ
BgNVBAMTE1F1b1ZlZG1zIFJvb3QgQ0EgMjAeFw0xMzEyMTcxNDI1MTBaFw0yMzEy
MTcxNDI1MTBaMF4xCzAJBgNVBAYTA1VTMTAwLgYDVQQKEydIeWRyYW50SUQgKEF2
YWxhbmNoZSBDbG91ZCBDb3Jwb3JhdG1vbikxHTAbBgNVBAMTFEh5ZHJhbnRJRkBT
U0wgSUNBIEcyMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICGKCAgEA9p1Z0A9+
H+tgdlN+STF7bd0xvnOERYyjo8ZbKumzigNePSwbQYVWuso76GI843yjaX2rh0+
Jt0NVJM41jVctf9qwacVduR7CEi0qJgpAUJyZUuB9IpFWF1Kz1403Leh6URuRZ43
RzHaRmNtzkxttGBuOtAg+i10uwiGAo9VQLgd0N1qQFcrbp97/f08ZIQiPrbhLxCZ
fXkYi3mktZVRFXG62FHAuH1sLDXCKba3avDcUR7ykG4ZXcmp6k114UKa8JHOHPE
NYyr0R6oHELOGZMox1nQcFwuYMX9sJdAUU/9SQVXYA6u6Ytx1pZiC8qhXM1IE00T

Q9+q5ppffSUDMC4V/5IF5A6snKVP78M8qd/RMVswcjMUMEnov+wykwCbDLD+IReM
A57XX+HojN+8XF7L9Jwge3z3Z1MwL7E54W3cI7f6cx05DVwoKxkd2jRIg37oqS1
SU3z/bA9UXjHcT1/6BoLho2p9rWm6o1jANPeQuLHyGJ3hc19N8nDo2IATp70k1GP
kd1qhIgrdkki7gBpanMOK98hKMPdQgs+NY4DkaMJqfrHzWR/CYkdyUCivFaepaFS
K78+jVu1oCMOFOnucPXL2fQa3VQn+69+7mA324frjwZj9NzrHjd0a5UP7waPpd9W
2jZoj4b+g+1+XU1SQ+9DWiuZtvfDw++k0BMCAwEAa0CAZEwggGNMBIGA1UdEwEB
/wQIMAYBAf8CAQAweAYDVR0gBHEwbzAIBgZngQwBAgEwCAYGZ4EMAQICMA4GDCsG
AQQBv1gAAmQBAjBJBgwrBgEEAb5YAAOHBAAwOTA3BggrBgEFBQcCARYraHR0cDov
L3d3dy5oeWRyYW50aWQuY29tL3N1cHBvcnQvcmlvbnNpdG9yeTBvBggrBgEFBQcB
AQRmMGQwKgYIKwYBBQUHAGGhmhOdHA6Ly9vY3NwLnF1b3ZhZG1zZ2xvYmFsLmNv
bTA2BggrBgEFBQcwoAoYqHR0cDovL3RydXN0LnF1b3ZhZG1zZ2xvYmFsLmNvbS9x
dnJjYTIuY3J0MA4GA1UdDwEB/wQEAwIBBjAFBgNVHSMEGDAwGBQahGK8SEwzJQTU
7tD2A8QZRtGUazA5BgNVHR8EMjAwMC6gLKAqhiodHRwOi8vY3JsLnF1b3ZhZG1z
Z2xvYmFsLmNvbS9xdnJjYTIuY3J0MA4GA1UdDgQWBBSYarYtLr+nqp/299YJr9WL
V/mKtzANBqkqhkig9w0BAQsFAAOCAgEA1raik8EDDUkpAnIOaj09/r4dpj/Zry76
6SH1oYPo7eTGzpdanPMeGMuSmwdjUkFUPALuWwkaDERfz9xdyFL3N8CRg9mQhdtT
3aWQUv/iyXULXT87EgL3b8zzf8fhTS7r654m9WM2w7pFqfmx9qA1Fe9Xcv1ZrUu
9hph+/MfWMrUju+VPL5U7hZvUpg66mS3BaN15rsXv2+Vw6kQsQC/82iJLHvtYVL/
LwbNio18CsinDeyRE0J9w1YDqzcg5rhD0rtX4JEmBzq8yBRvHIB/023o/vIO5oxh
83Hic/2Xgwksf1DKS3/z5nTzhsUjPcpwkN6nHp6gmA8JBXoU1KQz4eYHJCq/ZyC+
BuY2vHpNx6101J5dmy7ps7J7d6mZXzguP3DQN84hjtFwJPqdf+/9RgLriXeFTqwe
snxbk2FsPhwxhiNOH98GSZVvG02v10uHLVaf9B+puYpoUiEqgm1WG5mWW1PxHstu
Ew9jBMcJ6wjQc8He9rSUMrhBr0HyhckdC99RgEvpcZpV2XL4nPPrTI2ki/c9xQb9
kmhVGonSXY5aP+hDC+Ht+bxmc4wN5x+vB02hak8Hh8jIUSTRx0sRfJozU0R9ysyP
EZAHFZ3Zivg2BaD4t0IS08/T2FDjG7PNUv0tgPAOKw2t94B+1evrSUhqJDU0Wf9c
9vkaKoPvX4w=
-----END CERTIFICATE-----

Informations connexes

- [Assistance technique et téléchargements Cisco](#)

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.