Verificar falhas de Smart Licensing do ASA devido a problemas de certificado

Contents

Introduction

Este documento descreve como determinar falhas de ASA Smart Licensing que são causadas por uma falha de handshake de certificado.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve como lidar com uma alteração ocorrida em março de 2016 e outubro de 2018, na qual os servidores da Web que hospedam tools.cisco.com foram migrados para um certificado de Autoridade de Certificação (CA) raiz diferente. Após essa migração, alguns dispositivos ASA (Adaptive Security Appliance) não conseguem se conectar ao Smart Software Licensing Portal (que está hospedado em tools.cisco.com) quando registram um token de ID ou quando tentam renovar autorizações atuais. Isso foi determinado como um problema relacionado ao certificado. Especificamente, o novo certificado que é

apresentado ao ASA é assinado por uma CA intermediária diferente da que o ASA espera e foi pré-carregado.

Problema

Quando é feita uma tentativa de registrar um ASAv no Smart Software Licensing Portal, o registro falha com uma falha de conexão ou comunicação. Os comandos **show license registration** e **call-home test profile license** mostram essas saídas.

<#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)

No entanto, o ASAv pode resolver tools.cisco.com e conectar-se na porta TCP 443 com um ping TCP.

Syslogs e saída de depuração

A saída de syslog no ASAv após uma tentativa de registro pode mostrar isso:

<#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 .
```

Para obter mais informações, execute esses comandos de depuração enquanto tenta outro registro. Erros do Secure Socket Layer são vistos.

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

Especificamente, essa mensagem é vista como parte dessa saída:

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify
 failed@s3_clnt.c:1492
```

Na configuração padrão do ASAv, há um ponto confiável chamado _SmartCallHome_ServerCA que tem um certificado carregado e emitido para o nome do requerente "cn=Verisign Class 3 Secure Server CA - G3".

<#root>

ASAv#

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
```

No entanto, nos syslogs anteriores, o ASA indica que recebe um certificado do Smart Software Licensing Portal assinado por um intermediário chamado "cn=Symantec Class 3 Secure Server CA - G4".

> **Observação**: os nomes de assunto são semelhantes, mas têm duas diferenças: Verisign vs. Symantec no início e G3 vs. G4 no final.

Solução

O ASAv precisa fazer o download de um pool confiável que contenha os certificados intermediários e/ou raiz adequados para validar a cadeia.

Na versão 9.5.2 e posterior, o ASAv tem o pool confiável configurado para importar automaticamente às 22:00 hora local do dispositivo:

<#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
 crl cache-time 60
 crl enforcenextupdate
 auto-import
 auto-import url http://www.cisco.com/security/pki/trs/ios_core.p7b
 auto-import time 22:00:00
```

Se esta for uma instalação inicial, e as pesquisas do Sistema de Nome de Domínio (DNS) e a conectividade com a Internet ainda não estiverem ativas nesse momento, a importação automática não foi bem-sucedida e precisa ser concluída manualmente.

Em versões mais antigas, como a 9.4.x, a importação automática do pool confiável não está configurada no dispositivo e precisa ser importada manualmente.

Em qualquer versão, este comando importa o pool confiável e os certificados relevantes:

<#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
```

Verificar

Quando o pool confiável é importado pelo comando manual ou depois das 22:00 h, hora local, esse comando verifica se há certificados instalados no pool confiável:

```
<#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
```

> **Observação**: na saída anterior, a última importação de atualização automática falhou, pois o DNS não estava operacional na última tentativa automática, portanto, ele ainda mostra o último resultado da importação automática como falha. No entanto, uma atualização manual do pool confiável foi executada e atualizou com êxito o pool confiável (por isso ele mostra 14 certificados instalados).

Após a instalação do pool confiável, o comando token registration pode ser executado novamente para registrar o ASAv no Smart Software Licensing Portal.

```
<#root>

ASAv#

license smart register idtoken id_token force
```

Se o ASAv já estava registrado no Smart Software Licensing Portal, mas as renovações de autorização falharam, elas também podem ser tentadas manualmente.

<#root>

ASAv#

license smart renew auth

Alteração do Certificado CA Raiz - outubro de 2018

O certificado CA raiz para tools.cisco.com foi alterado na sexta-feira, 5 de outubro de 2018.

A versão 9.6(2) e posterior do ASAv implantado atualmente e o ASA em execução do Firepower 2100 não podem ser afetados por essa alteração se a comunicação com http://www.cisco.com/security/pki/trs/ios_core.p7b não for permitida. Há um recurso de importação automática de certificado que é habilitado por padrão em todas as plataformas ASA Smart Licensed mencionadas anteriormente. A saída de â€˜show crypto ca trustpoolâ€™ contém o certificado â€˜QuoVadis Root CA 2â€™:

```
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
```

Para novas implantações, você pode emitir o comando "crypto ca trustpool import default" e baixar o pacote de certificação padrão da Cisco que contém o certificado QuoVadis. Se isso não funcionar, você poderá instalar o certificado manualmente:

```
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
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9W
YWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
```

```
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+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
```

Plataformas 4100/9300 executando ASA

Esse problema afetou cerca de 4100/9300s em campo que executam o ASA, que depende do Firepower eXtensible Operating System (FXOS) para fornecer informações de Smart Licensing:

Unidade afetada:

<#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

Etapas de Resolução

Para resolver, você precisa criar um novo ponto confiável e inserir os dados do certificado no 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-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9W
YWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
>ENDOFBUF
```

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

Em seguida, confirme a alteração e renove a licença:

```
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
```

Agora você deve verificar se o licenciamento foi renovado:

<#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
```

Instalações do software ASA que exigem conformidade com FIPS (Federal Information Processing Standards, padrões federais de processamento de informações)

Para plataformas baseadas em ASA que exigem conformidade com FIPS, a importação do certificado CA 2 raiz do QuoVadis pode falhar por não conformidade com os requisitos criptográficos de assinatura e esta mensagem pode ser exibida:

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

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

Como solução alternativa para instalações ASA compatíveis com FIPS, importe o certificado intermediário HydrantID SSL ICA G2. O certificado HydrantID SSL ICA G2 é mostrado a seguir e está em conformidade

com os requisitos do algoritmo de assinatura sha256WithRSAEncryption. Consulte a documentação mostrada neste artigo para carregar o certificado com base em sua plataforma:

```
-----BEGIN CERTIFICATE-----
MIIGxDCCBKygAwIBAgIUdRcWd4PQQ361VsNXlG5FY7jr06wwDQYJKoZIhvcNAQEL
BQAwRTELMAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZ
BgNVBAMTElF1b1ZhZGlzIFJvb3QgQ0EgMjAeFw0xMzEyMTcxNDI1MTBaFw0yMzEy
MTcxNDI1MTBaMF4xCzAJBgNVBAYTAlVTMTAwLgYDVQQKEydIeWRyYW50SUQgKEF2
YWxhbmNoZSBDbG91ZCBDb3Jwb3JhdGlvbikxHTAbBgNVBAMTFEh5ZHJhbnRJRCBT
U0wgSUNBIEcyMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA9p1ZOA9+
H+tgdln+STF7bdOxvnOERYyjo8ZbKumzigNePSwbQYVWuso76GI843yjaX2rhn0+
Jt0NVJM41jVctf9qwacVduR7CEi0qJgpAUJyZUuB9IpFWF1Kz14O3Leh6URuRZ43
RzHaRmNtzkxttGBuOtAg+ilOuwiGAo9VQLgdONlqQFcrbp97/fO8ZIqiPrbhLxCZ
fXkYi3mktZVRFKXG62FHAuH1sLDXCKba3avDcUR7ykG4ZXcmp6kl14UKa8JHOHPE
NYyr0R6oHELOGZMox1nQcFwuYMX9sJdAUU/9SQVXyA6u6YtxlpZiC8qhXM1IE00T
Q9+q5ppffSUDMC4V/5If5A6snKVP78M8qd/RMVswcjMUMEnov+wykwCbDLD+IReM
A57XX+HojN+8XFTL9Jwge3z3ZlMwL7E54W3cI7f6cxO5DVwoKxkdk2jRIg37oqSl
SU3z/bA9UXjHcTl/6BoLho2p9rWm6oljANPeQuLHyGJ3hc19N8nDo2IATp70klGP
kd1qhIgrdkki7gBpanMOK98hKMpdQgs+NY4DkaMJqfrHzWR/CYkdyUCivFaepaFS
K78+jVu1oCMOFOnucPXL2fQa3VQn+69+7mA324frjwZj9NzrHjd0a5UP7waPpd9W
2jZoj4b+g+l+XU1SQ+9DWiuZtvfDW++k0BMCAwEAAaOCAZEwggGNMBIGA1UdEwEB
/wQIMAYBAf8CAQAweAYDVR0gBHEwbzAIBgZngQwBAgEwCAYGZ4EMAQICMA4GDCsG
AQQBvlgAAmQBAjBJBgwrBgEEAb5YAAOHBAAwOTA3BggrBgEFBQcCARYraHR0cDov
L3d3dy5oeWRyYW50aWQuY29tL3N1cHBvcnQvcmVwb3NpdG9yeTByBggrBgEFBQcB
AQRmMGQwKgYIKwYBBQUHMAGGHmh0dHA6Ly9vY3NwLnF1b3ZhZGlzZ2xvYmFsLmNv
bTA2BggrBgEFBQcwAoYqaHR0cDovL3RydXN0LnF1b3ZhZGlzZ2xvYmFsLmNvbS9x
dnJjYTIuY3J0MA4GA1UdDwEB/wQEAwIBBjAfBgNVHSMEGDAWgBQahGK8SEwzJQTU
7tD2A8QZRtGUazA5BgNVHR8EMjAwMC6gLKAqhihodHRwOi8vY3JsLnF1b3ZhZGlz
Z2xvYmFsLmNvbS9xdnJjYTIuY3JsMB0GA1UdDgQWBBSYarYtLr+nqp/299YJr9WL
V/mKtzANBgkqhkiG9w0BAQsFAAOCAgEAlraik8EDDUkpAnIOajO9/r4dpj/Zry76
6SH1oYPo7eTGzpDanPMeGMuSmwdjUkFUPALuWwkaDERfz9xdyFL3N8CRg9mQhdtT
3aWQUv/iyXULXT87EgL3b8zzf8fhTS7r654m9WM2W7pFqfimx9qAlFe9XcVlZrUu
9hph+/MfWMrUju+VPL5U7hZvUpg66mS3BaN15rsXv2+Vw6kQsQC/82iJLHvtYVL/
LwbNio18CsinDeyRE0J9wlYDqzcg5rhD0rtX4JEmBzq8yBRvHIB/023o/vIO5oxh
83Hic/2Xgwksf1DKS3/z5nTzhsUIpCpwkN6nHp6gmA8JBXoUlKQz4eYHJCq/ZyC+
BuY2vHpNx6101J5dmy7ps7J7d6mZXzguP3DQN84hjtfwJPqdf+/9RgLriXeFTqwe
snxbk2FsPhwxhiNOH98GSZVvG02v10uHLVaf9B+puYpoUiEqgm1WG5mWW1PxHstu
Ew9jBMcJ6wjQc8He9rSUmrhBr0HyhckdC99RgEvpcZpV2XL4nPPrTI2ki/c9xQb9
kmhVGonSXy5aP+hDC+Ht+bxmc4wN5x+vB02hak8Hh8jIUStRxOsRfJozU0R9ysyP
EZAHFZ3Zivg2BaD4tOISO8/T2FDjG7PNUv0tgPAOKw2t94B+1evrSUhqJDU0Wf9c
9vkaKoPvX4w=
-----END CERTIFICATE-----
```

Informações Relacionadas

- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.