Determinación de errores de licencias inteligentes de ASA debido a problemas de certificados

Contenido

Introducción

Este documento describe cómo determinar los errores de ASA Smart Licensing que se deben a un error de protocolo de enlace de certificado.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe cómo abordar un cambio que ocurrió en marzo de 2016 y octubre de 2018, en el que los servidores web que alojan tools.cisco.com se migraron a un certificado raíz de autoridad de certificación (CA) diferente. Después de esa migración, algunos dispositivos ASA (Adaptive Security Appliance) no pueden conectarse al portal de licencias de software inteligente (alojado en tools.cisco.com) cuando registran un token de ID o mientras intentan renovar las autorizaciones actuales. Se determinó que se

trataba de un problema relacionado con el certificado. Específicamente, el nuevo certificado que se presenta al ASA está firmado por una CA intermedia diferente de la que el ASA espera y se ha precargado.

Problema

Cuando se intenta registrar un ASAv en el portal de licencias de software inteligente, el registro falla debido a un error de conexión o comunicación. Los comandos **show license registration** y **call-home test profile license** muestran estos resultados.

```
<#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)
```

Sin embargo, ASAv puede resolver tools.cisco.com y conectarse al puerto TCP 443 con un ping TCP.

Syslogs y salida de depuración

La salida de Syslog en el ASAv después de un intento de registro puede mostrar lo siguiente:

```
<#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 obtener más información, ejecute estos comandos debug mientras intenta realizar otro registro. Se observan errores de Secure Socket Layer.

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

Específicamente, este mensaje se ve como parte de ese resultado:

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

En la configuración predeterminada de ASAv, hay un punto de confianza llamado _SmartCallHome_ServerCA que tiene un certificado cargado y emitido con el nombre de sujeto "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
```

Sin embargo, en los registros del sistema anteriores, el ASA indica que obtiene un certificado del portal de licencias de software inteligente firmado por un intermediario llamado "cn=Symantec Class 3 Secure Server CA - G4".

> **Nota**: Los nombres de los sujetos son similares, pero tienen dos diferencias: Verisign frente a Symantec al principio y G3 frente a G4 al final.

Solución

ASAv necesita descargar un conjunto de confianza que contenga los certificados raíz o intermedios adecuados para validar la cadena.

En la versión 9.5.2 y posteriores, ASAv tiene el conjunto de confianza configurado para la importación automática a las 10:00 PM hora local del 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
```

Si se trata de una instalación inicial y las búsquedas del sistema de nombres de dominio (DNS) y la conectividad a Internet no se han realizado todavía en ese momento, la importación automática no se ha realizado correctamente y debe completarse manualmente.

En versiones anteriores, como la 9.4.x, la importación automática del grupo de confianza no está configurada en el dispositivo y debe importarse manualmente.

En cualquier versión, este comando importa el conjunto de confianza y los 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
```

Verificación

Una vez que el grupo de confianza es importado por el comando manual o es después de las 10:00 PM hora local, este comando verifica que hay certificados instalados en el grupo de confianza:

<#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
```

> **Nota**: En el resultado anterior, la última importación de actualización automática falló porque DNS no estaba operativo la última vez que se intentó automáticamente, por lo que sigue mostrando el último resultado de importación automática como erróneo. Sin embargo, se ejecutó una actualización manual del conjunto de confianza que se actualizó correctamente (por lo que muestra 14 certificados instalados).

Una vez instalado el conjunto de confianza, el comando de registro de token se puede ejecutar nuevamente para registrar el ASAv con el portal de licencias de software inteligente.

<#root>

```
ASAv#
```

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

Si ASAv ya estaba registrado en el portal de licencias de software inteligente, pero las renovaciones de autorización fallaron, también se pueden intentar manualmente.

<#root>

ASAv#

license smart renew auth

Cambio del certificado de la CA raíz: octubre de 2018

El certificado de la CA raíz para tools.cisco.com fue cambiado el viernes, 5 de octubre de 2018.

Este cambio no puede afectar a la versión 9.6(2) y posteriores del ASAv implementado actualmente ni a la versión del ASA que ejecuta Firepower 2100 si no se permite la comunicación con http://www.cisco.com/security/pki/trs/ios_core.p7b. Existe una función de importación automática de certificados que está habilitada de forma predeterminada en todas las plataformas ASA Smart Licensed mencionadas anteriormente. La salida de â€˜show crypto ca trustpoolâ€™ contiene el 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 las nuevas implementaciones, puede ejecutar el comando "crypto ca trustpool import default" y descargar el paquete de certificados predeterminado de Cisco que contiene el certificado de QuoVadis. Si esto no funciona, puede instalar el 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 que ejecutan ASA

Este problema ha afectado a unos 4100/9300 en el campo que ejecutan ASA, que se basa en Firepower eXtensible Operating System (FXOS) para proporcionar información sobre licencias inteligentes:

Unidad afectada:

<#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

Pasos de resolución

Para resolver, debe crear un nuevo punto de confianza e introducir los datos del certificado en 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

A continuación, realice el cambio y renueve la licencia:

```
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
```

Ahora debe comprobar que se ha renovado la licencia:

<#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
```

Instalaciones de software ASA que requieren el cumplimiento de los estándares federales de procesamiento de la información (FIPS)

Para las plataformas basadas en ASA que requieren cumplimiento de FIPS, la importación del certificado de CA 2 raíz de QuoVadis puede fallar por no cumplir con los requisitos criptográficos de la firma y se puede mostrar este mensaje:

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

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

Como solución alternativa para las instalaciones ASA compatibles con FIPS, importe el certificado intermedio HydrantID SSL ICA G2. A continuación, se muestra el certificado HydrantID SSL ICA G2 y cumple con los requisitos del algoritmo de firma sha256WithRSAEncryption, consulte la documentación que se muestra en este artículo para cargar el certificado basado en su 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-----
```

Información Relacionada

- **Asistencia técnica y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).