

Instalación del certificado raíz en los vEdge de SDWAN

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Solución](#)

[Crear root-ca con el comando Linux CAT en vShell](#)

[Crear root-ca con VI Text Editor en vShell](#)

[Instalar certificado](#)

Introducción

Este documento describe cómo instalar un certificado raíz en vEdges SD-WAN con diferentes herramientas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software (SD-WAN) Cisco Catalyst
- Certificados
- Linux básico

Componentes Utilizados

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.

- Cisco Catalyst SD-WAN Validator 20.6.3
- Cisco vEdge 20.6.3

Problema

Un certificado digital es un archivo electrónico que certifica la autenticidad de un dispositivo, servidor o usuario mediante el uso de criptografía e infraestructura de clave pública (PKI). La autenticación de certificados digitales ayuda a las organizaciones a garantizar que solo los dispositivos y usuarios de confianza puedan conectarse a sus redes.

La identidad de los routers de hardware vEdge la proporciona un certificado de dispositivo firmado por Avnet, generado durante el proceso de fabricación y grabado en el chip del Módulo de plataforma segura (TPM). Los certificados raíz de Symantec/DigiCert y Cisco están precargados en el software de confianza para los certificados de los componentes de control. Los certificados raíz adicionales deben cargarse manualmente, distribuirse automáticamente mediante el administrador de SD-WAN o instalarse durante el proceso de aprovisionamiento automatizado.

Uno de los problemas más comunes en SD-WAN es la falla de Control Connections debido a un certificado no válido. Esto ocurre porque el certificado nunca se instaló o porque está dañado.

Para validar la leyenda de error Conexión de control, utilice el comando EXEC show control connections-history.

<#root>

vEdge #

```
show control connections-history
```

Legend for Errors

ACSRREJ	- Challenge rejected by peer.	NOVMCFG	- No cfg in vmanage for device.
BDSGVERFL	- Board ID Signature Verify Failure.	NOZTPEN	- No/Bad chassis-number entry in ZTP.
BIDNTPR	- Board ID not Initialized.	OPERDOWN	- Interface went oper down.
BIDNTRFD	- Peer Board ID Cert not verified.	ORPTMO	- Server's peer timed out.
BIDSIG	- Board ID signing failure.	RMGSPR	- Remove Global saved peer.
CERTEXPRD	- Certificate Expired	RXTRDWN	- Received Teardown.
CRTREJSER	- Challenge response rejected by peer.	RDSIGFBD	- Read Signature from Board ID failed.
CRTVERFL	- Fail to verify Peer Certificate.		
SERNTPRES	- Serial Number not present.		
CTORGNMIS	- Certificate Org name mismatch.	SSLNFAIL	- Failure to create new SSL context.
DCONFAL	- DTLS connection failure.	STNMODETD	- Teardown extra vBond in STUN server
DEVALC	- Device memory Alloc failures.	SYSIPCHNG	- System-IP changed
DHSTMO	- DTLS HandShake Timeout.	SYSRCH	- System property changed
DISCVBD	- Disconnect vBond after register reply.	TMRALC	- Timer Object Memory Failure.
DISTLOC	- TLOC Disabled.	TUNALC	- Tunnel Object Memory Failure.
DUPCLHELO	- Recd a Dup Client Hello, Reset GI Peer.	TXCHTOBD	- Failed to send challenge to BoardID.
DUPSER	- Duplicate Serial Number.	UNMSGBDRG	- Unknown Message type or Bad Register
DUPSYSIPDEL	- Duplicate System IP.	UNAUTHHEL	- Recd Hello from Unauthenticated peer
HAFAIL	- SSL Handshake failure.	VBDEST	- vDaemon process terminated.
IP_TOS	- Socket Options failure.	VECRTREV	- vEdge Certification revoked.
LISFD	- Listener Socket FD Error.	VSCRTREV	- vSmart Certificate revoked.
MGRTBLOCKD	- Migration blocked. Wait for local TMO.	VB_TMO	- Peer vBond Timed out.
MEMALCFL	- Memory Allocation Failure.	VM_TMO	- Peer vManage Timed out.
NOACTVB	- No Active vBond found to connect.	VP_TMO	- Peer vEdge Timed out.
NOERR	- No Error.	VS_TMO	- Peer vSmart Timed out.
NOSLPRCRT	- Unable to get peer's certificate.	XTVMTRDN	- Teardown extra vManage.
NTPRVMINT	- Not preferred interface to vManage.	XTVSTRDN	- Teardown extra vSmart.
STENTRY	- Delete same tloc stale entry.		

PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PRIVATE PORT	PEER PUBLIC IP	PUBLIC PORT
vbond	dtls	-	0	0	10.10.10.1	12346	10.10.10.1	12346
vbond	dtls	-	0	0	10.10.10.2	12346	10.10.10.2	12346

Algunas causas comunes de la etiqueta de error CRTVERFL son:

- La hora de vencimiento del certificado.
- Root-ca es diferente.
 - Si una actualización de root-ca ocurre en los controladores.
 - Se utiliza una autoridad certificadora (CA) diferente de Cisco y los dispositivos necesitan la instalación manual de root-ca.
- Cambio de autoridad certificadora en la superposición.



Nota: Para obtener más información sobre los errores de Control Connections, visite [Troubleshoot SD-WAN Control Connections](#).

El archivo root-ca debe ser exactamente el mismo en todos los componentes de la superposición. Hay dos formas de validar que el archivo root-ca en utilizado no es el correcto

1. Revise el tamaño del archivo, esto es útil en situaciones en las que la raíz-ca tenía una actualización.

<#root>

```
vBond:/usr/share/viptela$ ls -l
total 5
-rw-r--r-- 1 root root 294 Jul 23 2022 ISR900_pubkey.der
-rw-r--r-- 1 root root 7651 Jul 23 2022 TPMRootChain.pem
-rw-r--r-- 1 root root 16476 Jul 23 2022 ViptelaChain.pem
-rwxr-xr-x 1 root root 32959 Jul 23 2022 ios_core.pem

-rw-r--r-- 1 root root 24445 Dec 28 13:59 root-ca.crt
```

<#root>

```
vEdge:/usr/share/viptela$ ls -l
total 6
drwxr-xr-x 2 root root 4096 Aug 28 2022 backup_certs
-rw-r--r-- 1 root root 1220 Dec 28 13:46 clientkey.crt
-rw----- 1 root root 1704 Dec 28 13:46 clientkey.pem
-rw----- 1 root root 1704 Dec 28 13:46 proxy.key
-rw-r--r-- 1 root root 0 Aug 28 2022 reverse_proxy_mapping

-rw-r--r-- 1 root root 23228 Aug 28 2022 root-ca.crt
```

2. Segunda y más confiable manera de validar que el archivo es exactamente igual que el archivo de origen es con el comando `md5sum root-ca.crt vshell`. Una vez que se proporciona el md5, compare el resultado de los componentes Controller y Edge device.

```
<#root>
```

```
vBond:/usr/share/viptela$
```

```
md5sum root-ca.crt
```


```
a4f945b9a1f50f1fa68d539dcf2e54f2 root-ca.crt
```

```
<#root>
```

```
vEdge:/usr/share/viptela$
```

```
md5sum root-ca.crt
```


```
b36358d01b36254a54db2f8db2266ced root-ca.crt
```

 Nota: Como el comando `md5sum root-ca.crt vshell` se utiliza para verificar la integridad de los archivos, ya que prácticamente cualquier cambio en un archivo hace que el hash MD5 sea diferente.

Solución

La cadena de certificados raíz de un dispositivo se puede instalar con varias herramientas. Hay dos maneras de instalarlo con el uso de comandos de Linux.

Crear root-ca con el comando Linux CAT en vShell

 Nota: Este procedimiento se aplica a los archivos root-ca que no tienen líneas en blanco dentro del contenido, para situaciones con líneas en blanco usadas en Linux mediante el procedimiento del editor.

Paso 1. Obtenga y copie el archivo `root-ca.crt` del validador.

La raíz-ca es la misma en todos los controladores y se puede copiar de cualquiera de ellos en la ruta /usr/share/viptela/.

```
<#root>
```

```
vBond#
```

```
vsHELL
```

```
vBondvBond:~$
```

```
cat /usr/share/viptela/root-ca.crt
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAKGA1UEBhMCVVMxZzAVBGNVBAoTD1Z1cm1TaWduLCBjbmuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbiBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+r70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIeWi u5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAObgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQWEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGGUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHR21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7wNq
```

```
-----END CERTIFICATE-----
```

Paso 2. Cree el archivo root-ca.crt en el borde.

Desde vshell, navegue hasta /home/admin o /home/<username> y cree el archivo root-ca.crt.

```
<#root>
```

```
vEdge#
```

```
vsHELL
```

```
vEdge:~$
```

```
cat <<" >> root-ca.crt
```

```
> -----BEGIN CERTIFICATE-----
```

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAKGA1UEBhMCVVMxZzAVBGNVBAoTD1Z1cm1TaWduLCBjbmuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbiBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+r70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIeWi u5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAObgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQWEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGGUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
```

```
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZaFC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
>
vEdge:~$
```


Paso 3. Validar que se ha completado.

```
<#root>
```

```
vEdge:~$
```

```
cat root-ca.crt
```

```
-----BEGIN CERTIFICATE-----
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTD1Zlcm1TaWduLCBjbmuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwHhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbjBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNhDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIeWiU5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZaFC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
vEdge:~$
```

 Nota: Es importante validar que el archivo esté completo; si no está completo, elimine el archivo con el comando `rm root-ca.crt` vshell y créelo nuevamente desde el Paso 2.

Salga de vshell y continúe con la Sección.

```
<#root>
```

```
vEdge:~$
```

```
exit
```

Crear root-ca con VI Text Editor en vShell

Paso 1. Obtenga y copie el archivo root-ca.crt del validador.

La raíz-ca es la misma en todos los controladores y se puede copiar de cualquiera de ellos en la ruta `/usr/share/viptela/`.

```

<#root>

vBond#
  vshell

vBond:~$
cat /usr/share/viptela/root-ca.crt

-----BEGIN CERTIFICATE-----
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yJELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTD1Zlcm1TaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwHhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbjBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIewi5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAObgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGGQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ228udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----

```

Paso 2. Cree el archivo root-ca.crt en el borde.

Desde vshell, navegue hasta /home/admin o /home/<username> y cree el archivo root-ca.crt.

```

<#root>

vEdge#
  vshell

vEdge:~$
  cd /usr/share/viptela/

vEdge:~$
  pwd

/home/admin
vEdge:~$ vi root-ca.crt

```

Una vez que haga clic en Intro, aparecerá el mensaje del editor.

Paso 3. Entrar en modo de inserción

- Tipo: i y pegue el contenido del certificado del paso 1. Desplácese hacia abajo y confirme que el certificado está completo.

Paso 4. Salga del modo de inserción y guarde el certificado.

- Presione la tecla ESC.
- Escriba :wq! seguido de enter para guardar los cambios y salir del editor.

```
<#root>
```

```
vEdge:/usr/share/viptela$
```

```
cat root-ca.crt
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZjZAVBgnVBAoTD1Z1cm1TaWduLCBjbmuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbjBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIeWi u5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGGUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
```

```
-----END CERTIFICATE-----
```

Paso 5. Validar que se ha completado.

```
<#root>
```

```
vEdge:~$
```


```
cat root-ca.crt
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZjZAVBgnVBAoTD1Z1cm1TaWduLCBjbmuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbjBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIeWi u5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGGUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
```

```
-----END CERTIFICATE-----
```

```
vEdge:~$
```

 Nota: Es importante validar que el archivo esté completo; si no está completo, elimine el archivo con el comando `rm root-ca.crt` vshell y créelo nuevamente desde el Paso 2.

Salga de vshell y continúe con la Sección.

```
<#root>
vEdge:~$
exit
```

Instalar certificado

Paso 1. Instale el certificado root-ca con el comando `request root-cert-chain install <path>`.

```
<#root>
vEdge#
request root-cert-chain install /home/admin/root-ca.crt

Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/PKI.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```

Paso 2. Valide que esté instalado con el comando `show control local-properties`.

```
<#root>
vEdge#
show control local-properties

personality vedge
organization-name organization-name
root-ca-chain-status Installed

certificate-status Installed
certificate-validity Valid
certificate-not-valid-before Apr 11 17:57:17 2023 GMT
certificate-not-valid-after Apr 10 17:57:17 2024 GMT
```

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).