Installa certificato radice su bordi SDWAN

Sommario

Introduzione

Questo documento descrive come installare un certificato radice in SD-WAN Edge con strumenti diversi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Software Cisco Catalyst Defined Wide Area Network (SD-WAN)
- Certificati
- Linux Basic

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

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

Problema

Un certificato digitale è un file elettronico che certifica l'autenticità di un dispositivo, server o utente tramite l'utilizzo della crittografia e dell'infrastruttura a chiave pubblica (PKI). L'autenticazione

digitale dei certificati consente alle organizzazioni di garantire che solo i dispositivi e gli utenti attendibili possano connettersi alle proprie reti.

L'identità dei router hardware vEdge viene fornita da un certificato di dispositivo firmato da Avnet, generato durante il processo di produzione e masterizzato nel chip TPM (Trusted Platform Module). I certificati radice Symantec/DigiCert e Cisco sono precaricati nel software per garantire l'attendibilità dei certificati dei componenti di controllo. I certificati radice aggiuntivi devono essere caricati manualmente, distribuiti automaticamente da SD-WAN Manager o installati durante il processo di provisioning automatizzato.

Uno dei problemi più comuni in SD-WAN è l'errore Control Connections a causa di un certificato non valido. Il problema può essere dovuto al fatto che il certificato non è mai stato installato oppure è stato danneggiato.

Per convalidare la legenda dell'errore Control Connection, usare il 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.
BIDNTVRFD  - 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.
CTORGNMMIS - Certificate Org name mismatch.           SSLNFAIL  - Failure to create new SSL context.
DCONFAIL   - DTLS connection failure.                 STNMODETD - Teardown extra vBond in STUN server
DEVALC     - Device memory Alloc failures.            SYSIPCHNG - System-IP changed
DHSTMO     - DTLS HandShake Timeout.                  SYSPRCH   - 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 Gl Peer.  TXCHTOBD  - Failed to send challenge to BoardID.
DUPSER     - Duplicate Serial Number.                 UNMSGBDRG - Unknown Message type or Bad Register
DUPSYSIPDEL- Duplicate System IP.                     UNAUTHEL  - 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.
MGRTBLCKD  - 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     PEER     PEER             SITE       DOMAIN PEER             PRIVATE  PEER             PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID         ID     PRIVATE IP       PORT     PUBLIC IP        PORT
-------------------------------------------------------------------------------------------------------
vbond    dtls     -                0          0      10.10.10.1       12346    10.10.10.1       12346   pu
vbond    dtls     -                0          0      10.10.10.2       12346    10.10.10.2       12346   pu
```

Alcune cause comuni dell'etichetta di errore CRTVERFL sono:

- Ora di scadenza del certificato.
- Root-ca è diverso.
  - Se viene eseguito un aggiornamento della CA radice nei controller.
  - Viene utilizzata un'autorità di certificazione (CA) diversa da Cisco e i dispositivi richiedono l'installazione manuale della CA radice.
- Modifica dell'autorità di certificazione nella sovrapposizione.

Nota: per ulteriori informazioni sugli errori delle connessioni di controllo, visitare il sito Risoluzione dei problemi relativi alle connessioni SD-WAN.

Il file CA radice deve essere esattamente lo stesso in tutti i componenti della sovrapposizione. Esistono due modi per verificare che il file della CA radice in uso non sia quello corretto

1. Esaminare le dimensioni del file. Questa operazione risulta utile nelle situazioni in cui la CA radice ha subito un aggiornamento.

<#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. Il secondo e più affidabile modo per verificare che il file sia esattamente lo stesso del file di origine è con il comando md5sum root-ca.crt vshell. Una volta fornito l'md5, confrontare il risultato di entrambi i componenti Controller e 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: come il comando md5sum root-ca.crt vshell viene utilizzato per verificare l'integrità dei file, in quanto praticamente qualsiasi modifica apportata a un file causa una differenza nell'hash MD5.

Soluzione

La catena di certificati radice di un dispositivo può essere installata con più strumenti. Esistono due modi per installarlo con i comandi di Linux.

Creazione di una root-ca con il comando Linux CAT in vShell

Nota: questa procedura è valida per i file CA radice che non hanno righe vuote all'interno del contenuto, per le situazioni con righe vuote è stata utilizzata la procedura dell'editor Linux vi.

Passaggio 1. Ottenere e copiare il file root-ca.crt da validator.

La CA radice è la stessa in tutti i controller e può essere copiata da uno qualsiasi di essi nel

percorso /usr/share/viptela/.

<#root>

vBond#

vshell

vBondvBond:~$

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

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJO23tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

Passaggio 2. Creare il file root-ca.crt nel vedge.

Da vshell, passare a /home/admin o /home/<nomeutente> e creare il file root-ca.crt.

<#root>

vEdge#

vshell

vEdge:~$

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

```
> -----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJO23tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
```

```
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
>
vEdge:~$
```

Passaggio 3. Convalidare il completamento.

<#root>

```
vEdge:~$
```

cat root-ca.crt

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
vEdge:~$
```

Nota: è importante verificare che il file sia completo. In caso contrario, eliminare il file con il comando rm root-ca.crt vshell e crearlo nuovamente dal Passaggio 2.

Uscire da vshell e continuare con la sezione.

<#root>

```
vEdge:~$
```

exit

Creazione di una CA radice con VI Text Editor in vShell

Passaggio 1. Ottenere e copiare il file root-ca.crt da validator.

La CA radice è la stessa in tutti i controller e può essere copiata da uno qualsiasi di essi nel percorso /usr/share/viptela/.

<#root>

vBond#

vshell

vBond:~$

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

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

Passaggio 2. Creare il file root-ca.crt nel vedge.

Da vshell, passare a /home/admin o /home/<nomeutente> e creare il file root-ca.crt.

<#root>

vEdge#

vshell

vEdge:~$

cd /usr/share/viptela/

vEdge:~$

pwd

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

Dopo aver fatto clic su Invio, viene visualizzato il prompt dell'editor.

Passaggio 3. Accedere alla modalità di inserimento

- Digitare i e incollare il contenuto del certificato dal passaggio 1. Scorrere verso il basso e verificare che il certificato sia completo.

Passaggio 4. Evita la modalità di inserimento e salva il certificato.

- Premere ESC.
- Digitare :wq! seguito da invio per salvare le modifiche e uscire dall'editor.

<#root>

vEdge:/usr/share/viptela$

cat root-ca.crt

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJO23tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5NO6tRn/Arr0PO7gi+s3i+zO16zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

Passaggio 5. Convalidare il completamento.

<#root>

vEdge:~$

cat root-ca.crt

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJO23tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5NO6tRn/Arr0PO7gi+s3i+zO16zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
vEdge:~$
```

Nota: è importante verificare che il file sia completo. In caso contrario, eliminare il file con il comando rm root-ca.crt vshell e crearlo nuovamente dal Passaggio 2.

Uscire da vshell e continuare con la sezione.

<#root>

vEdge:~$

exit

Installare il certificato

Passaggio 1. Installare il certificato CA radice con il comando request root-cert-chain install <percorso>.

<#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
```

Passaggio 2. Verificare che sia installato con il 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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).