

Genera certificato firmato dall'Autorità di certificazione (CA) nel server di chiamata CVP per TLS (Transport Layer Security) SIP

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come generare un certificato CA firmato per il server di chiamata CVP (Customer Voice Portal) e come verificare il certificato del server di chiamata CVP. Dalla versione 11.6 di CVP, è supportata la comunicazione TLS SIP (Session Initiation Protocol).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CVP
- SIP

Componenti usati

Le informazioni di questo documento si basano su CVP 11.6.

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.

Configurazione

Passaggio 1. Trovare la password per il keystore.

Per individuare la password, passare a `c:\Cisco\CVP\conf\security.properties` nel server di chiamata CVP.

Questo file contiene la password per il keystore, necessaria per il funzionamento del keystore.

Passaggio 2. Creare una variabile temporanea per evitare di immettere ogni volta il valore della password del keystore.

Passare a **c:\Cisco\CVP\conf\security** ed eseguire questo comando:

```
set kt=c:\Cisco\CVP\jre\bin\keytool.exe -storepass 592(!aT@Hbt{[c)b7n6{Mj6J[0P4C~X2?4!zv~5(@2*12Dm97 -storetype JCEKS -keystore .keystore
```

Nota: Storepass deve essere sostituito con la password del keystore.

Passaggio 3. Rimuovere il certificato del server di chiamata esistente.

Passare a **c:\Cisco\CVP\conf\security** per trovare il certificato esistente. Eseguire questo comando per eliminare il certificato:

```
%kt% -delete -alias certificato_server_chiamate
```

Dopo l'eliminazione del certificato, è possibile utilizzare questo comando per verificare tutti i certificati nel server CVP:

```
%kt% -elenco
```

Per verificare se il certificato del server di chiamata è stato eliminato, eseguire questo comando:

```
%kt% -list | findstr callserver
```

Passaggio 4. Generare la coppia di chiavi. È necessario utilizzare una coppia di chiavi da 2048 bit.

Passare a **c:\Cisco\CVP\conf\security** ed eseguire questo comando:

```
%kt% -genkeypair -alias certificato_server_chiamate -v -keysize 2048 -keyalg RSA
```

Quando si esegue questo comando, vengono richieste le seguenti informazioni:

Nota: È necessario utilizzare il nome host del server come nome e cognome.

Qual è il vostro nome e cognome?

[Sconosciuto]: col115cvpcall02

Qual è il nome dell'unità organizzativa?

[Sconosciuto]: TAC

Qual è il nome dell'organizzazione?

[Sconosciuto]: Cisco

Indicare il nome della città o località.

[Sconosciuto]: Sydney

Qual è il nome della provincia?

[Sconosciuto]: NSW

Qual è il codice paese di due lettere per questo apparecchio?

[Sconosciuto]: AU

CN=col115cvpcall02, OU=TAC, O=Cisco, L=Sydney, ST=NSW, C=AU corretto?

[no]: sì

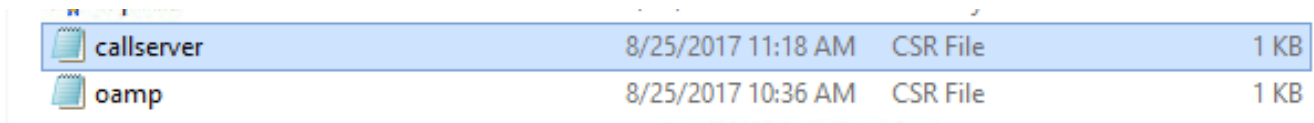
Passaggio 5. Generare la nuova richiesta di firma del certificato (CSR).

Passare a **c:\Cisco\CVP\conf\security** ed eseguire questo comando:

```
%kt% -certreq -alias certificato_server_chiamata -file server.csr
```

Passaggio 6. Firmare il CSR tramite CA interna o C di terze parti.

Per trovare questo file CSR, passare a **c:\Cisco\CVP\conf\security**:

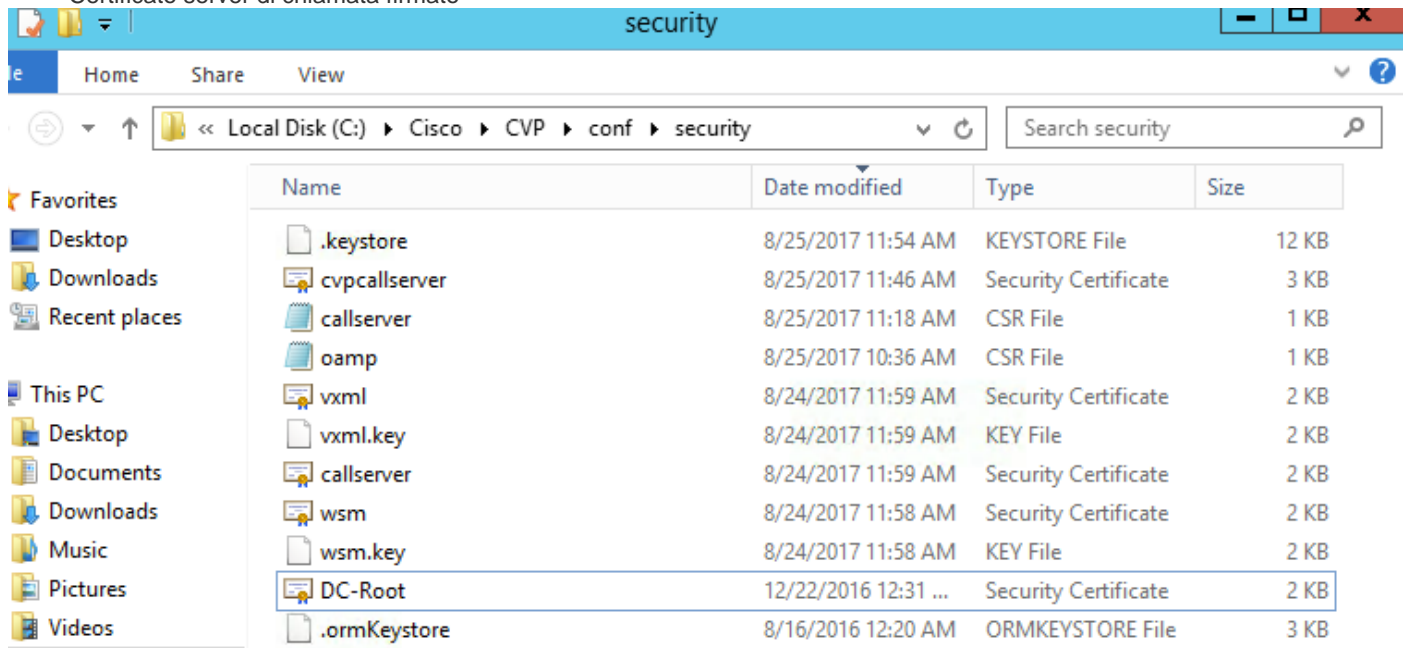


Name	Date modified	Type	Size
callserver	8/25/2017 11:18 AM	CSR File	1 KB
oamp	8/25/2017 10:36 AM	CSR File	1 KB

Passaggio 7. Installare la CA radice.

Due certificati vengono copiati in **c:\Cisco\CVP\conf\security**.

- Certificato CA radice
- Certificato server di chiamata firmato



Name	Date modified	Type	Size
.keystore	8/25/2017 11:54 AM	KEYSTORE File	12 KB
cvpcallserver	8/25/2017 11:46 AM	Security Certificate	3 KB
callserver	8/25/2017 11:18 AM	CSR File	1 KB
oamp	8/25/2017 10:36 AM	CSR File	1 KB
vxml	8/24/2017 11:59 AM	Security Certificate	2 KB
vxml.key	8/24/2017 11:59 AM	KEY File	2 KB
callserver	8/24/2017 11:59 AM	Security Certificate	2 KB
wsm	8/24/2017 11:58 AM	Security Certificate	2 KB
wsm.key	8/24/2017 11:58 AM	KEY File	2 KB
DC-Root	12/22/2016 12:31 ...	Security Certificate	2 KB
.ormKeystore	8/16/2016 12:20 AM	ORMKEYSTORE File	3 KB

Eseguire questo comando:

```
%kt% -import -v -trustcacerts -alias root -file DC-Root.cer
```

In questa esercitazione, il certificato CA radice è DC-Root.cer.

Passaggio 8. Installare il certificato del server di chiamata firmato dalla CA.

Andare sul sito **c:\Cisco\CVP\conf\security**

Eseguire questo comando:

```
%kt% -import -v -trustcacerts -alias callserver_certificate -file cvpcallserver.cer
```

In questa esercitazione il certificato del server di chiamata è cvpcallserver.cer.

Passaggio 9. Verificare il nuovo certificato installato

Per verificare il nuovo certificato installato, passare a **C:\Cisco\CVP\conf\security>**

Eseguire questo comando:

```
%kt% -list -v -alias callserver_certificate Nome alias:callserver_certificate
```

Nota: Il nome alias è un valore di sistema fisso. È necessario utilizzare `callserver_certificate`.

Esempio:

Data creazione: 25 ago 2017

Tipo voce: VoceChiavePrivata

Lunghezza catena certificati: 2

Certificate[1]:

Proprietario: CN=col115cvpcall02, OU=TAC, O=Cisco, L=Sydney, ST=NSW, C=AU

Emittente: CN=col115-COL115-CA, DC=col115, DC=org, DC=au

Numero di serie: 610000000e78c717ba3dd3dc2400000000000e

Valido da: Ven 25 ago 11:32:43 AEST 2017 fino a: Sab 25 ago 11:42:43 AEST 2018

Impronte digitali certificato:

Al termine di tutti questi passaggi, è stato installato il certificato firmato dall'autorità di certificazione per il server di chiamata. Questo certificato viene utilizzato quando viene stabilita la connessione TLS per il SIP.

Verifica

Questi due comandi possono essere utilizzati per elencare tutti i certificati o solo per chiamare i certificati del server:

```
%kt% - elenco
```

```
%kt% -list | findstr callserver
```

Questo comando può essere utilizzato per visualizzare i dettagli del certificato:

Nome alias: `callserver_certificato`

```
%kt% -list -v -alias certificato_server
```

Nome alias: `callserver_certificate`

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

[Guida alla configurazione di Cisco Unified Customer Voice Portal, versione 11.6\(1\)](#)

