Esempio di configurazione di Secure SIP Trunk tra CUCM e VCS

Sommario

Introduzione

In questo documento viene descritto come configurare una connessione SIP (Session Initiation Protocol) sicura tra Cisco Unified Communications Manager (CUCM) e Cisco TelePresence Video Communication Server (VCS).

CUCM e VCS sono strettamente integrati. Poiché gli endpoint video possono essere registrati su CUCM o sul VCS, è necessario che tra i dispositivi esistano trunk SIP.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Communications Manager
- Cisco TelePresence Video Communication Server
- Certificati

Componenti usati

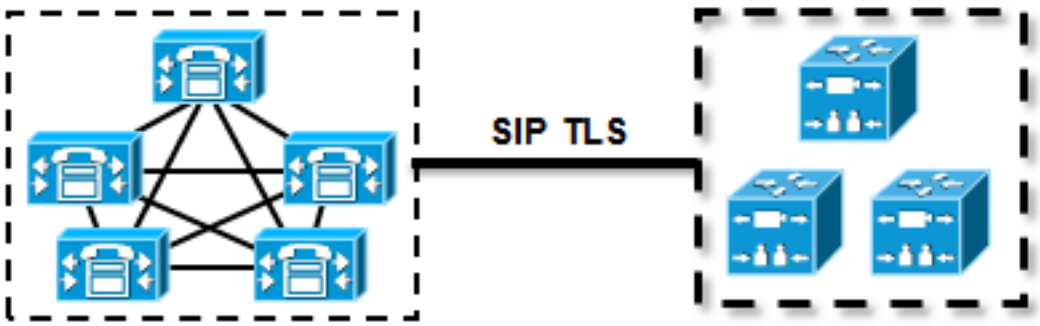
Il documento può essere consultato per tutte le versioni software o hardware. In questo esempio vengono utilizzati il software Cisco VCS versione X7.2.2 e CUCM versione 9.x.

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

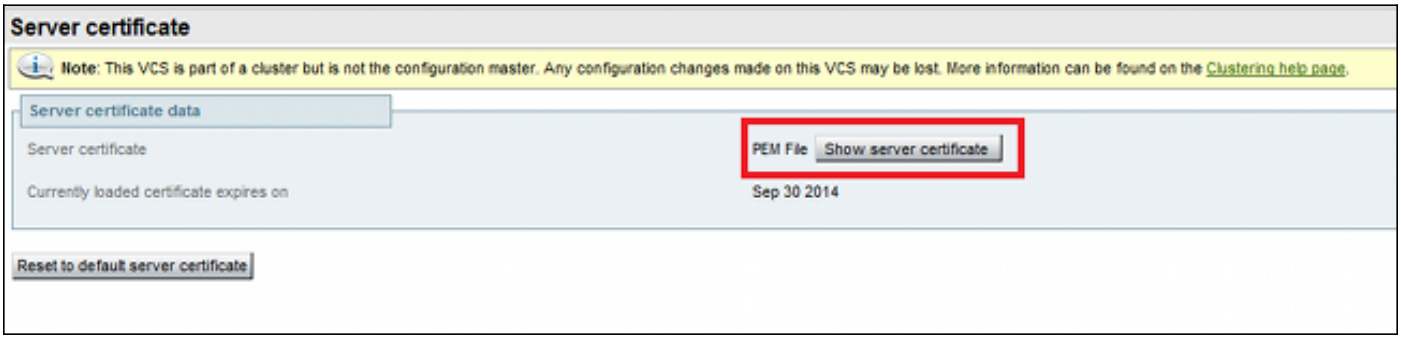
Verificare che i certificati siano validi, aggiungere i certificati ai server CUCM e VCS in modo che considerino attendibili i rispettivi certificati, quindi stabilire il trunk SIP.

Esempio di rete



Ottieni certificato VCS

Per impostazione predefinita, tutti i sistemi VCS vengono forniti con un certificato temporaneo. Nella pagina Admin, passare a **Manutenzione > Gestione certificati > Certificato server**. Fare clic su **Mostra certificato server**. Verrà visualizzata una nuova finestra con i dati non elaborati del certificato:



Questo è un esempio dei dati non elaborati del certificato:

```
-----BEGIN CERTIFICATE-----
MIIDHzCCAoigAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmjFDMEEGA1UECgw6VGVt
cG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTFlMy1hNTE4LTAwNTA1
Njk5NWI0YjFDMEEGA1UECww6VGVtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYw
LTI5YTAtMTFlMy1hNTE4LTAwNTA1Njk5NWI0YjEOMAwGA1UEAwwFY2lzY28wHhcN
MTMwOTMwMDcxNzIwWhcNMTQwOTMwMDcxNzIwWjCBmjFDMEEGA1UECgw6VGVtcG9y
YXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTFlMy1hNTE4LTAwNTA1Njk5
NWI0YjFDMEEGA1UECww6VGVtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5
YTAtMTFlMy1hNTE4LTAwNTA1Njk5NWI0YjEOMAwGA1UEAwwFY2lzY28wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPipL0I/
L21fyyjoO5qv9lzDCgy7PFZPxkD1d/DNLIgp1jjUqdfFV+64r8OkESwBO+4DFlut
tWZLQ1uKzzdsmvZ/b41mEtosElHNxH7rDYQsqdRA4ngNDJVlOgVFCEV4c7ZvAV4S
E8m9YNY9AgMBAAGjczBxMAkGA1UdEwQCMAAwJAYJYIZIAYb4QgENBBcWFVRlbXBv
cmFyeSBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU+knGYkeeiWqAjORhzQqRCHba+nEw
HwYDVR0jBBgwFoAUpHCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKoZIhvcNAQEFBQAD
gYEAZklIMSfi49p1jIYqYdOAIjOiashYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S
p1SyT4ilU5uiY0DD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6WL6hsj+90GAsI/TGthQ2n7yUWPl6CevopbJe1iA=
-----END CERTIFICATE-----
```

Èpossibile decodificare il certificato e visualizzarne i dati utilizzando OpenSSL sul PC locale o un decodificatore di certificati online come SSL Shopper:

Genera e carica certificato autofirmato VCS

Poiché ogni server VCS dispone di un certificato con lo stesso nome comune, è necessario inserire nuovi certificati nel server. È possibile scegliere di utilizzare certificati autofirmati o certificati firmati dall'Autorità di certificazione (CA). Per i dettagli di questa procedura, vedere la guida alla creazione e all'uso del certificato Cisco TelePresence con Cisco VCS Deployment.

In questa procedura viene descritto come utilizzare il software VCS stesso per generare un certificato autofirmato e caricarlo:

1. Accedere come utente root a VCS, avviare OpenSSL e generare una chiave privata:

```
~ # openssl
OpenSSL> genrsa -out privatekey.pem 1024
Generating RSA private key, 1024 bit long modulus
.................................++++++
.............++++++
e is 65537 (0x10001)
```

2. Utilizzare questa chiave privata per generare una richiesta di firma del certificato (CSR):

```
OpenSSL> req -new -key privatekey.pem -out certcsr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BE
State or Province Name (full name) [Some-State]:Vlaams-Brabant
Locality Name (eg, city) []:Diegem
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:radius.anatomy.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
OpenSSL> exit
```

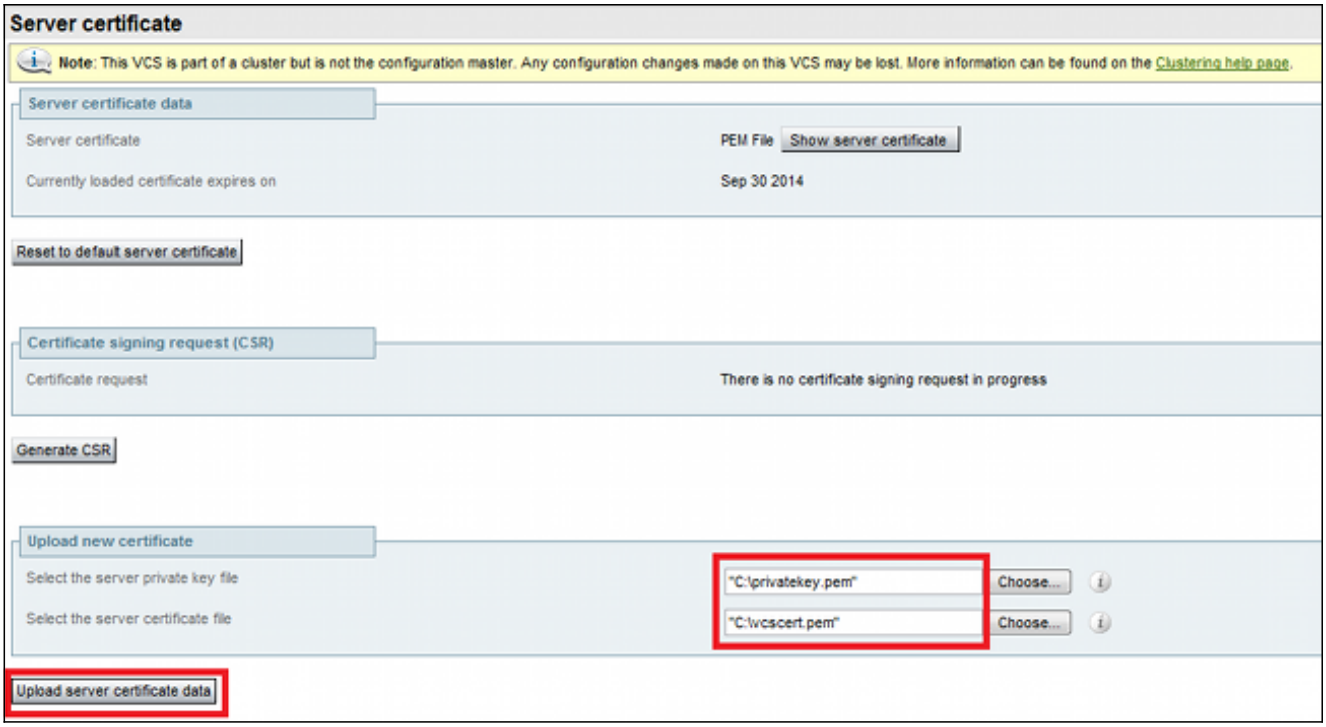
3. Genera il certificato autofirmato:

```
~ # openssl x509 -req -days 360 -in certcsr.pem -signkey privatekey.pem -out vcscert.pem
Signature ok
subject=/C=BE/ST=Vlaams-Brabant/L=Diegem/O=Cisco/OU=TAC/CN=radius.anatomy.com
Getting Private key
~ #
```

4. Confermare che i certificati sono ora disponibili:

```
~ # ls -ltr *.pem
-rw-r--r-- 1 root root 891 Nov 1 09:23 privatekey.pem
-rw-r--r-- 1 root root 664 Nov 1 09:26 certcsr.pem
-rw-r--r-- 1 root root 879 Nov 1 09:40 vcscert.pem
```

5. Scaricare i certificati con WinSCP e caricarli nella pagina Web in modo che il software VCS possa utilizzarli; sono necessari sia la chiave privata che il certificato generato:



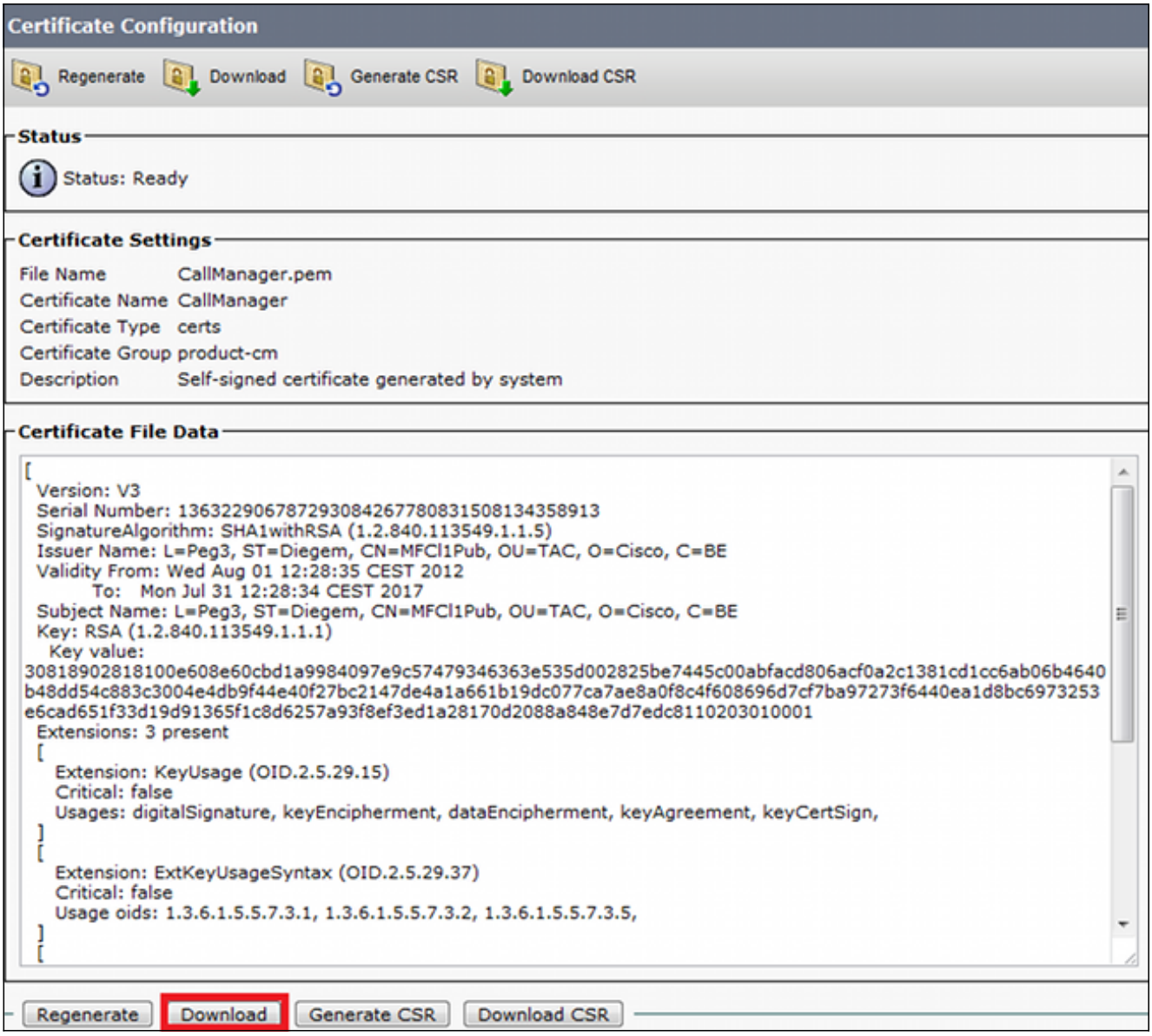
6. Ripetere questa procedura per tutti i server VCS.

Aggiungi certificato autofirmato dal server CUCM al server VCS

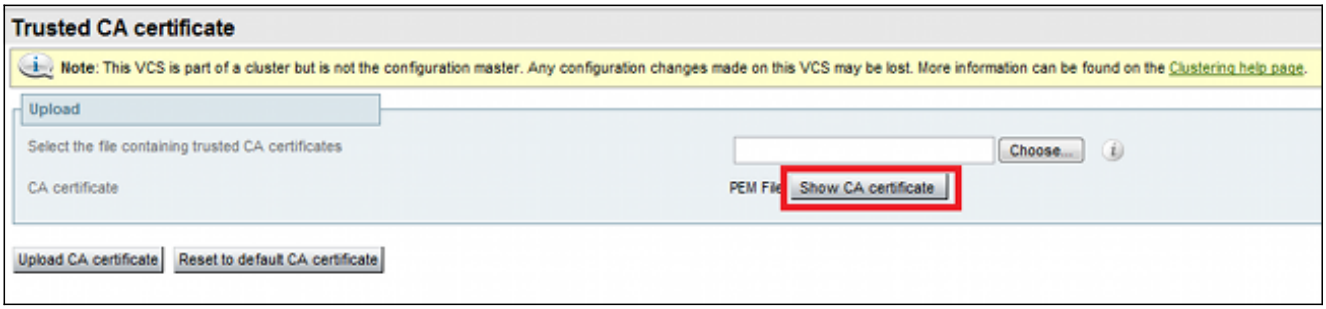
Aggiungere i certificati dai server CUCM in modo che il software VCS li consideri attendibili. In questo esempio vengono utilizzati i certificati autofirmati standard di CUCM; CUCM genera certificati autofirmati durante l'installazione in modo che non sia necessario crearli come nel software VCS.

In questa procedura viene descritto come aggiungere un certificato autofirmato dal server CUCM al server VCS:

1. Scaricare il certificato CallManager.pem da CUCM. Accedere alla pagina Amministrazione del sistema operativo, selezionare **Security > Certificate Management**, quindi selezionare e scaricare il certificato CallManager.pem autofirmato:



2. Aggiungere il certificato come certificato CA attendibile nel software VCS.Sul software VCS, selezionare **Manutenzione > Gestione certificati > Certificato CA attendibile**, quindi selezionare **Mostra certificato CA**:



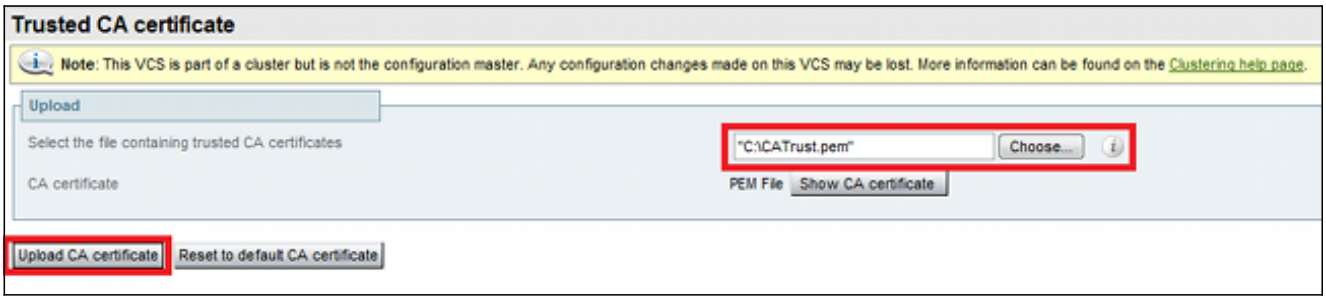
Verrà visualizzata una nuova finestra con tutti i certificati attualmente considerati attendibili.

3. Copiare tutti i certificati attualmente attendibili in un file di testo. Aprire il file CallManager.pem in un editor di testo, copiarne il contenuto e aggiungerlo alla fine dello stesso file di testo dopo i certificati attualmente attendibili:

```
CallManagerPub
======================
-----BEGIN CERTIFICATE-----
MIICmDCCAgGgAwIBAgIQZo7WOmjKYy9JP228PpPvgTANBgkqhkiG9w0BAQUFADBe
MQswCQYDVQQGEwJCRTEOMAwGA1UEChMFQ2lzY28xDDAKBgNVBAsTA1RBQzERMA8G
A1UEAxMITUZDbDFQdWIxDzANBgNVBAgTBkRpZWdlbTENMAsGA1UEBxMEUGVnMzAe
Fw0xMjA4MDExMDI4MzVaFw0xNzA3MzExMDI4MzRaMF4xCzAJBgNVBAYTAkJFMQ4w
DAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMREwDwYDVQQDEwhNRkNsMVB1YjEP
MA0GA1UECBMGRGllZ2VtMQ0wCwYDVQQHEwRQZWczMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDmCOYMvRqZhAl+nFdHk0Y2PlNdACglvnRFwAq/rNgGrPCiwTgc
0cxqsGtGQLSN1UyIPDAE5NufROQPJ7whR95KGmYbGdwHfKeuig+MT2CGltfPe6ly
c/ZEDqHYvGlzJT5srWUfM9GdkTZfHI1iV6k/jvPtGigXDSCIqEjn1+3IEQIDAQAB
o1cwVTALBgNVHQ8EBAMCArwwJwYDVR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMC
BggrBgEFBQcDBTAdBgNVHQ4EFgQUK4jYX6O6BAnLCalbKEn6YV7BpkQwDQYJKoZI
hvcNAQEFBQADgYEAkEGDdRdMOtX4ClhEatQE3ptT6L6RRAyP8oDd3dIGEOYWhA2H
Aqrw77loieva297AwgcKbPxnd5lZ/aBJxvmF8TIiOSkjy+dJW0asZWfei9STxVGn
NSr1CyAt8UJh0DSUjGHtnv7yWse5BB9mBDR/rmWxIRrlIRzAJDeygLIq+wc=
-----END CERTIFICATE-----
```

Se nel cluster CUCM sono presenti più server, aggiungerli tutti qui.

4. Salvare il file come CATrust.pem e fare clic su **Upload CA certificate** (Carica certificato CA) per caricare nuovamente il file sul software VCS:



Il software VCS considererà attendibili i certificati offerti da CUCM.

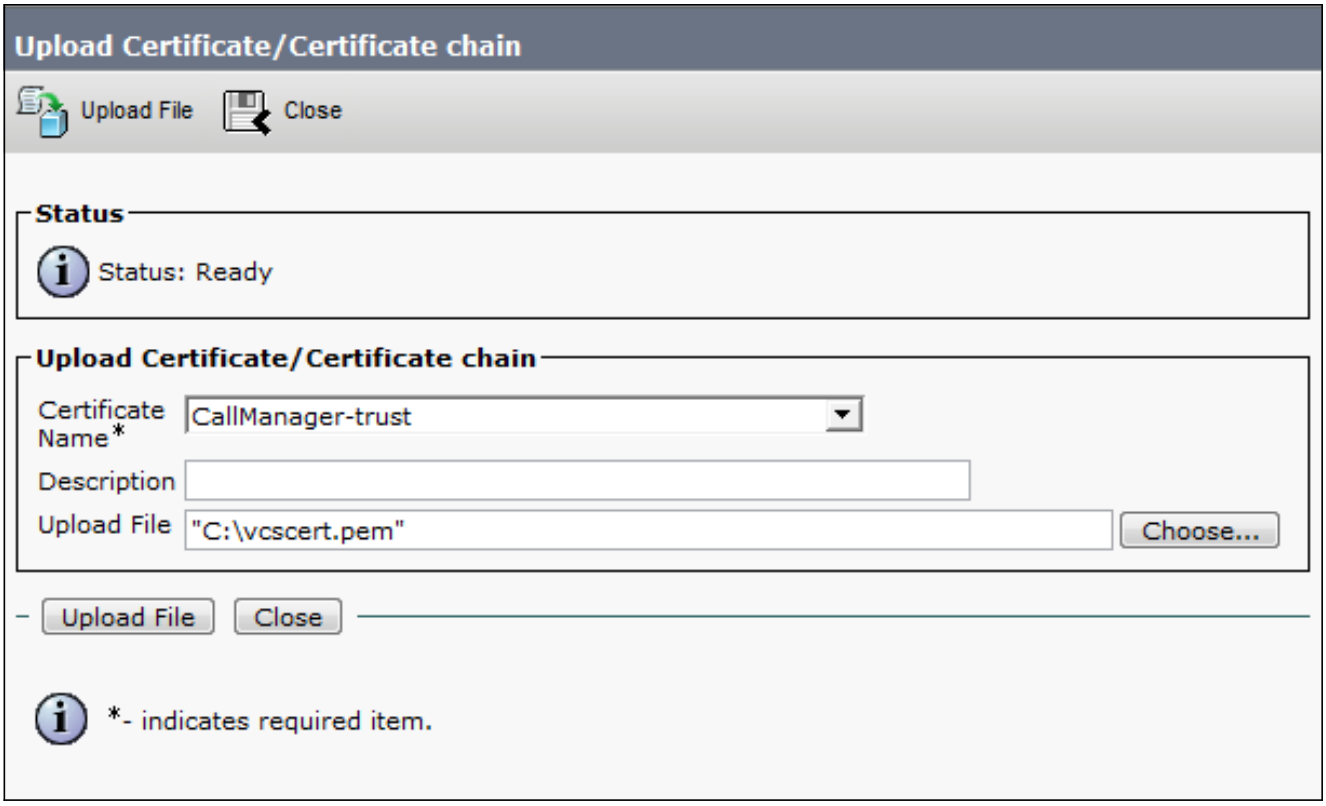
5. Ripetere questa procedura per tutti i server VCS.

Carica certificato dal server VCS al server CUCM

Il CUCM deve considerare attendibili i certificati offerti dal software VCS.

In questa procedura viene descritto come caricare il certificato VCS generato sul CUCM come certificato CallManager-Trust:

1. Nella pagina Amministrazione del sistema operativo, passare a **Protezione > Gestione certificati**, immettere il nome del certificato, individuare la posizione e fare clic su **Carica file**:



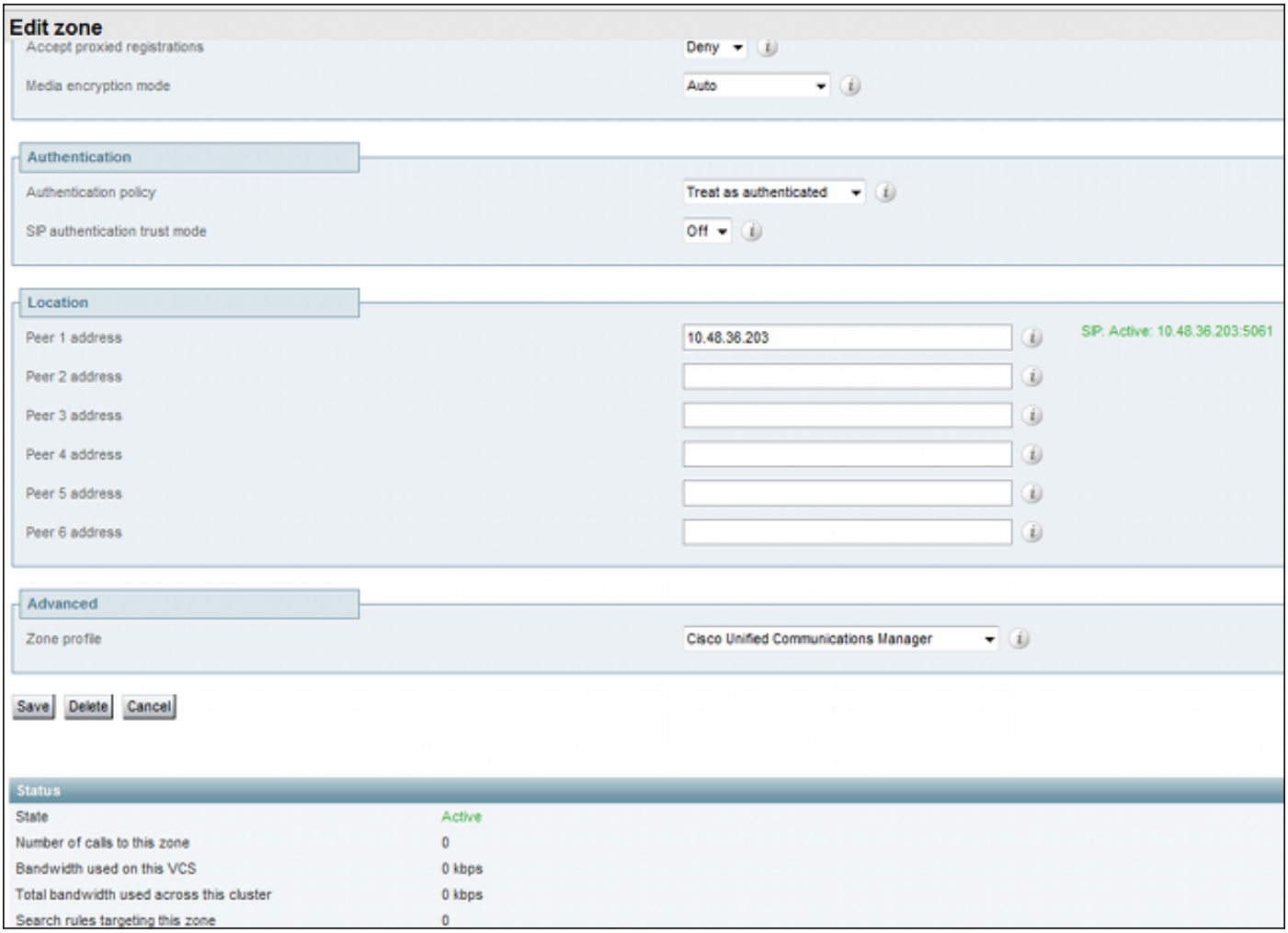
2. Caricare il certificato da tutti i server VCS. Eseguire questa operazione su ogni server CUCM che comunicherà con il software VCS; si tratta in genere di tutti i nodi che eseguono il servizio CallManager.

Connessione SIP

Una volta convalidati i certificati ed entrambi i sistemi si fidano a vicenda, configurare la zona adiacente su VCS e il trunk SIP su CUCM. Per i dettagli di questa procedura, vedere la guida alla distribuzione di Cisco TelePresence Cisco Unified Communications Manager con Cisco VCS (SIP Trunk).

Verifica

Verificare che la connessione SIP sia attiva nella zona adiacente su VCS:



Risoluzione dei problemi

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

Informazioni correlate

- Cisco TelePresence Guida all'installazione di Cisco Unified Communications Manager con Cisco VCS (SIP Trunk)
- Cisco TelePresence Video Communication Server Administrator Guide
- Cisco TelePresence - Creazione e uso di certificati con Cisco VCS - Guida all'implementazione
- Guida all'amministrazione del sistema operativo di Cisco Unified Communications
- Guida all'amministrazione di Cisco Unified Communications Manager
- Documentazione e supporto tecnico – Cisco Systems