

Configura cluster di comunicazioni unificate

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Certificato SAN multiserver CallManager](#)

[Risoluzione dei problemi](#)

[Note avvertenze](#)

Introduzione

In questo documento viene descritto come configurare un cluster di comunicazioni unificato con l'utilizzo di certificati SAN multiserver con firma CA (Certification Authority).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Communications Manager (CUCM)
- CUCM IM e Presence versione 10.5

Prima di provare la configurazione, verificare che i seguenti servizi siano attivi e funzionanti:

- Servizio Web di amministrazione della piattaforma Cisco
- Servizio Cisco Tomcat

Per verificare questi servizi su un'interfaccia Web, selezionare **Cisco Unified Serviceability Page Services > Network Service > Select a server** (Servizi di rete unificati Cisco > Seleziona server). Per verificarli nella CLI, immettere il comando **utils service list**.

Se SSO è abilitato nel cluster CUCM, è necessario disabilitarlo e riabilitarlo.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Premesse

In CUCM versione 10.5 e successive, questa richiesta di firma del certificato (CSR) dell'archivio attendibile può includere il nome alternativo del soggetto (SAN) e i domini alternativi.

1. Tomcat - CUCM e IM&P
2. Cisco CallManager - Solo CUCM
3. Protocollo CUP-XMPP (Cisco Unified Presence-Extensible Messaging and Presence Protocol) - Solo IM&P
4. CUP-XMPP Server-to-Server (S2S) - Solo IM&P

In questa versione è più semplice ottenere un certificato firmato dalla CA. La CA deve firmare un solo CSR anziché il requisito di ottenere un CSR da ogni nodo del server e quindi ottenere un certificato firmato dalla CA per ogni CSR e gestirli singolarmente.

Configurazione

Passaggio 1.

Accedere all'amministrazione del sistema operativo (OS) del server di pubblicazione e selezionare Protezione > Gestione certificati > Genera CSR.

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose* tomcat

Distribution* cs-ccm-pub.\[redacted].com

Common Name* cs-ccm-pub.\[redacted].com

Multi-server(SAN)

Subject Alternate Names (SANs)

Parent Domain [redacted].com

Key Length* 2048

Hash Algorithm* SHA256



Generate Close

*- indicates required item.

Passaggio 2.

Scegliere SAN multiserver in Distribuzione.

Generate Certificate Signing Request

 Generate  Close

Status



Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*	tomcat
Distribution*	cs-ccm-pub.v[redacted].com
Common Name*	cs-ccm-pub.v[redacted].com Multi-server(SAN)
Subject Alternate Names (SANs)	
Parent Domain	[redacted].com
<hr/>	
Key Length*	2048
Hash Algorithm*	SHA256

Generate

Close





*- indicates required item.

Viene eseguito il popolamento automatico dei domini SAN e del dominio padre.

Verificare che tutti i nodi del cluster siano elencati per Tomcat: tutti i nodi CUCM e IM&P per CallManager: sono stati elencati solo i nodi CUCM.

Generate Certificate Signing Request

 Generate  Close

Status



Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*

Distribution*

Common Name*

Subject Alternate Names (SANs)

Auto-populated Domains

cs-ccm-pub.com
cs-ccm-sub.com
cs-imp.com

Parent Domain

Other Domains

--

No file selected.

Please import .TXT file only.
For more information please refer to the notes in the Help Section

Key Length*

Hash Algorithm*





*- indicates required item.

Passaggio 3.

Fare clic su Genera e una volta generato il CSR, verificare che tutti i nodi elencati nel CSR siano visualizzati anche nell'elenco CSR esportato.

Generate Certificate Signing Request

 Generate  Close

Status



Success: Certificate Signing Request Generated



CSR export operation successful on the nodes [cs-ccm-sub.com, cs-ccm-pub.com, cs-imp.com].

In Gestione certificati, la richiesta SAN viene generata:

Certificate List (1 - 15 of 15)						
Find Certificate List where Certificate begins with tomcat Find Clear Filter + -						
Certificate ^	Common Name	Type	Key Type	Distribution	Issued By	
tomcat	115pub-ms-██████████	CSR Only	RSA	Multi-server(SAN)	--	
tomcat	115pub-ms-██████████	CA-signed	RSA	Multi-server(SAN)	██████████	

Passaggio 4.

Fare clic su **Download CSR**, quindi scegliere lo scopo del certificato e fare clic su **Download CSR**.

The screenshot shows the Cisco Unified Operating System Administration interface. At the top, there is a navigation menu with options like Show, Settings, Security, Software Upgrades, Services, and Help. Below this, the 'Certificate List' section is visible, with a 'Download CSR' button highlighted in a red box. Below the main interface, a 'Download Certificate Signing Request' dialog box is open. It contains a warning icon and the message: 'Certificate names not listed below do not have a corresponding CSR'. There is a dropdown menu for 'Certificate Purpose*' with 'tomcat' selected. At the bottom of the dialog, there are 'Download CSR' and 'Close' buttons. A note at the bottom left of the dialog states: '*- indicates required item.'

È possibile utilizzare la CA locale o una CA esterna come VeriSign per ottenere la firma del CSR (file scaricato nel passaggio precedente).

In questo esempio viene illustrata la procedura di configurazione per una CA basata su Microsoft Windows Server. Se si utilizza una CA diversa o una CA esterna, andare al passaggio 5.

Accedere a <https://<windowsserveripaddress>/certsrv/>

Scegliere **Richiedi certificato > Richiesta avanzata di certificati**.

Copiare il contenuto del file CSR nel campo Richiesta certificato con codifica Base 64 e fare clic su **Invia**.

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Inviare la richiesta CSR come illustrato di seguito.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded
certificate request
(CMC or
PKCS #10 or
PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBIjCCAGCgAqAgEgMCAgEgDgYFAAIBATAKIDQaw
BANDQwckBqVwIAIYFQOZEFEXK9j1zE0BkGALTE
cy11Ez0t0FV1LnLnCjFuay5jEj1c0Bk0TFRBq9V
NB11ZK5WEG2Rd128652QWNB1HdAJY1JW7T1K
NTYyqR1NG00C3q9R1nDQFRAQTAAN1R0w8uggER
< >
```

Additional Attributes:

Attributes

< >

Submit >

Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Your Request Id is 32.

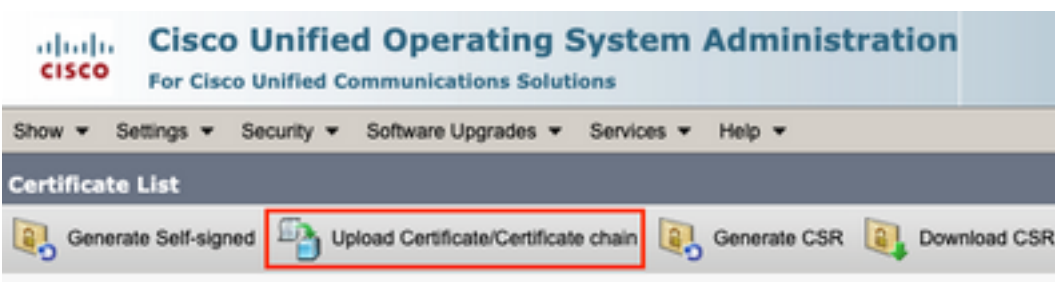
Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with this web browser within 10 days to retrieve your certificate

Passaggio 5.

Nota: prima di caricare un certificato Tomcat, verificare che SSO sia disabilitato. Se è attivata, l'SSO deve essere disattivato e riattivato una volta completato il processo di rigenerazione dei certificati Tomcat.

Con il certificato firmato, caricare i certificati CA come tomcat-trust. Innanzitutto il certificato radice e quindi il certificato intermedio, se esistente.



Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* tomcat-trust

Description(friendly name)

Upload File Choose File certchain.p7b

Upload Close

Passaggio 6.

Caricare ora il certificato firmato CUCM come Tomcat e verificare che tutti i nodi del cluster siano elencati in "Operazione di caricamento certificato riuscita" come mostrato nell'immagine:

Upload Certificate/Certificate chain

Upload Close

Status

i Certificate upload operation successful for the nodes cs-ccm-pub.com,cs-ccm-sub.com,cs-imp.com.

i Restart Cisco Tomcat Service for the nodes cs-ccm-pub.com,cs-ccm-sub.com,cs-imp.com using the CLI "utils service restart Cisco Tomcat".

Upload Certificate/Certificate chain

Certificate Purpose* tomcat

Description(friendly name) Self-signed certificate

Upload File Browse... No file selected.

Upload Close

i *- indicates required item.

La SAN multiserver è elencata in Gestione certificati come mostrato nell'immagine:

ipsec-trust	cs-com-pub.10000.com	Self-signed	cs-com-pub.10000.com	cs-com-pub.10000.com	04/18/2019	Trust Certificate
ITLRecovery	ITLRECOVERY.cs-com-pub.vasank.com	Self-signed	ITLRECOVERY.cs-com-pub.10000.com	ITLRECOVERY.cs-com-pub.10000.com	04/18/2019	Self-signed certificate generated by system
tomcat	cs-com-pub.10000.com.ms	CA-signed	Multi-server(SAN)	v10000-DC1-CA	12/19/2015	Certificate Signed by v10000-DC1-CA
tomcat-trust	cs-com-pub.10000.com.ms	CA-signed	Multi-server(SAN)	v10000-DC1-CA	12/19/2015	Trust Certificate
tomcat-trust	gs-com-pub.10000.com	Self-signed	gs-com-pub.10000.com	gs-com-pub.10000.com	04/21/2019	Trust Certificate
tomcat-trust	VeriSign Class 3 Secure Server CA - G3	CA-signed	VeriSign_Class_3_Secure_Server_CA_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/08/2020	Trust Certificate
tomcat-trust	dc1-com-pub.10000.com	Self-signed	dc1-com-pub.10000.com	dc1-com-pub.10000.com	04/17/2019	Trust Certificate
tomcat-trust	dc1-com-pub.10000.com	Self-signed	dc1-com-pub.10000.com	dc1-com-pub.10000.com	04/18/2019	Trust Certificate
tomcat-trust	v10000-DC1-CA	Self-signed	v10000-DC1-CA	v10000-DC1-CA	04/29/2064	Root CA
TVS	cs-com-pub.vasank.com	Self-signed	cs-com-pub.10000.com	cs-com-pub.10000.com	04/18/2019	Self-signed certificate generated by system

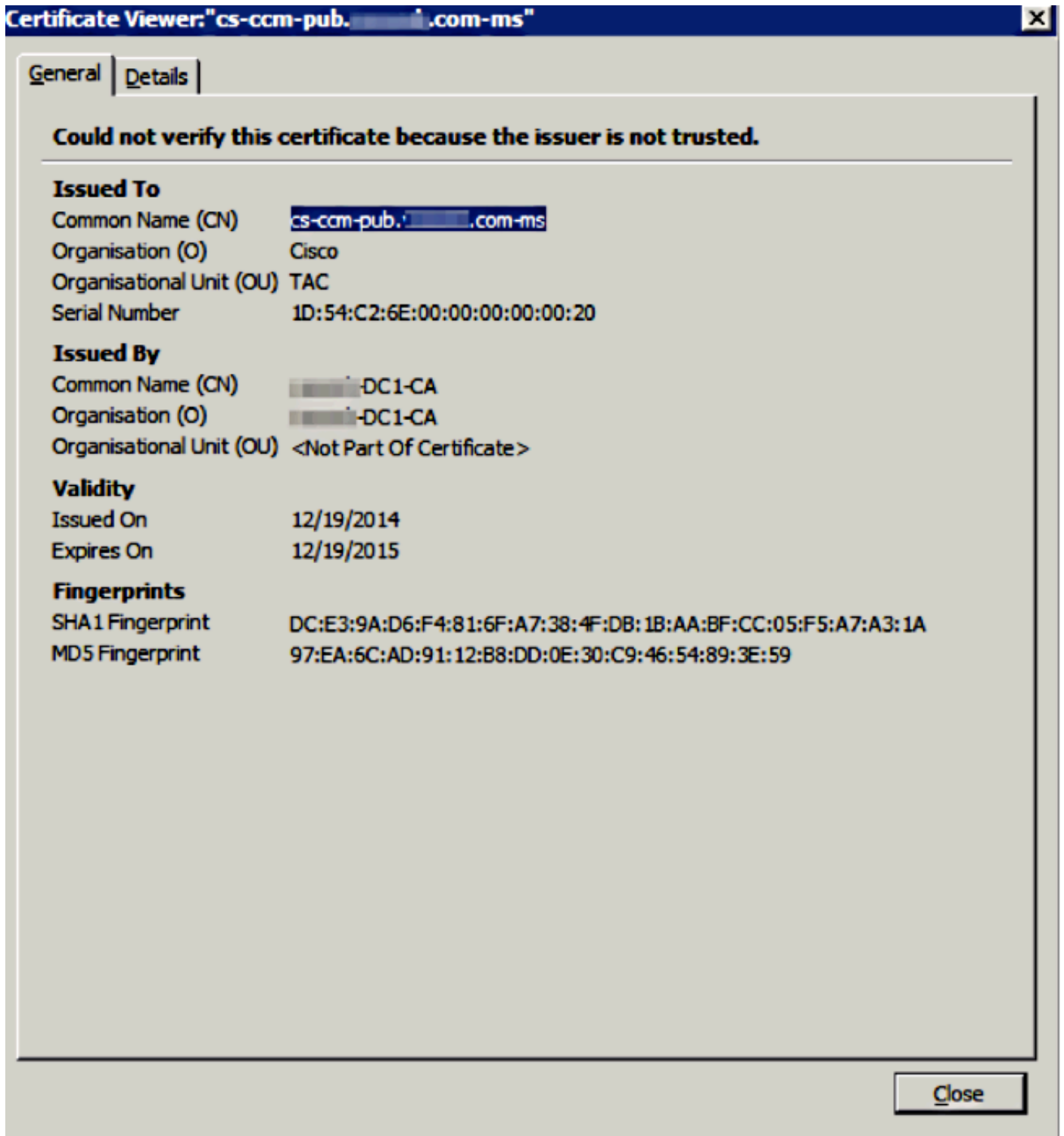
Passaggio 7.

Riavviare il servizio Tomcat su tutti i nodi nella lista SAN (prima il server di pubblicazione e quindi gli abbonati) tramite CLI con il comando: **utils service restart Cisco Tomcat**.

```
admin:
admin:utils service restart Cisco Tomcat
Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

Verifica

Accedere a <http://<fqdnofccm>:8443/ccmadmin> per verificare che venga utilizzato il nuovo certificato.



Certificato SAN multiserver CallManager

È possibile seguire una procedura simile per il certificato CallManager. In questo caso, i domini popolati automaticamente sono solo nodi CallManager. Se il servizio Cisco CallManager non è in esecuzione, è possibile scegliere di mantenerlo nell'elenco SAN o rimuoverlo.

Avviso: questo processo influisce sulla registrazione e sull'elaborazione delle chiamate. Assicurati di pianificare una finestra di manutenzione per qualsiasi lavoro con i certificati CUCM/TVS/ITL/CAPF.

Prima di firmare il certificato SAN per CUCM, verificare che:

- Il telefono IP è in grado di considerare attendibile il servizio di verifica dell'attendibilità (TVS). È possibile verificare questa condizione accedendo a qualsiasi servizio HTTPS dal telefono. Ad esempio, se l'accesso alla directory aziendale funziona, significa che il telefono considera attendibile il servizio TVS.
- Verificare se il cluster è in modalità non protetta o mista.

Per determinare se si tratta di un cluster a modalità mista, scegliere **Amministrazione Cisco Unified CM > Sistema > Parametri Enterprise > Modalità di protezione cluster (0 = Non protetto; 1 = Modalità mista)**.

Avviso: se il cluster è in modalità mista prima del riavvio dei servizi, è necessario aggiornare l'elenco di certificati attendibili (CTL): [Token](#) o [Token](#).

Dopo aver installato il certificato rilasciato dalla CA, è necessario riavviare il successivo elenco di servizi nei nodi abilitati:

- Cisco Unified Serviceability > Strumenti > Control Center - Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Strumenti > Control Center - Feature Services > Cisco CallManager
- Cisco Unified Serviceability > Strumenti > Control Center - Feature Services > Cisco CTIM Manager
- Cisco Unified Serviceability > Strumenti > Control Center - Servizi di rete > Cisco Trust Verification Service

Risoluzione dei problemi

Questi registri possono aiutare il Technical Assistance Center di Cisco a identificare eventuali problemi relativi alla generazione e al caricamento di CSR SAN multiserver con firma CA.

- API Cisco Unified OS Platform
- Cisco Tomcat
- Registri di CertMgr piattaforma IPT
- [Processo di rinnovo del certificato](#)

Note avvertenze

- ID bug Cisco [CSCur97909](#) - Il caricamento del certificato multiserver non elimina i certificati autofirmati nel database
- ID bug Cisco [CSCus47235](#) - CUCM 10.5.2 non può essere duplicato nella SAN per CSR
- ID bug Cisco [CSCup28852](#) - ripristino del telefono ogni 7 minuti a causa dell'aggiornamento del certificato quando si usa il certificato multiserver

Se esiste già un certificato per più server, si consiglia di eseguire la rigenerazione nei seguenti scenari:

- Modifica nome host o dominio. Quando si modifica un nome host o un dominio, i certificati vengono rigenerati automaticamente come autofirmati. Per passare a una firma CA, è necessario seguire i passaggi precedenti.
- Se è stato aggiunto un nuovo nodo al cluster, è necessario generare un nuovo CSR per

includere il nuovo nodo.

- Quando un sottoscrittore viene ripristinato e non è stato utilizzato alcun backup, il nodo può disporre di nuovi certificati autofirmati. Per includere il sottoscrittore può essere necessario un nuovo CSR per il cluster completo. (Richiesta di miglioramento) ID bug Cisco [CSCuv75957](#) per aggiungere questa funzionalità.)

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).