Genera CSR e applica certificati a CMS

Sommario

Introduzione

In questo documento viene descritto come generare una richiesta di firma di certificato (CSR) e caricare certificati firmati in Cisco Meeting Server (CMS).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base del server CMS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Putty o software simile
- CMS 2.9 o versione successiva

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.

Genera CSR

È possibile generare CSR in due modi, uno per generare il CSR direttamente sul server CMS dall'interfaccia della riga di comando (CLI) con accesso amministrativo, l'altro per farlo con l'autorità di certificazione (CA) esterna di terze parti, ad esempio Open SSL.

In entrambi i casi, affinché i servizi CMS funzionino correttamente, è necessario che la CSR venga generata con la sintassi corretta.

Passaggio 1. Struttura della sintassi

```
pki csr <key/cert basename> <CN:value> [OU:<value>] [O:<value>] [ST:<-value>] [C:<value>] [subjectAltNa
```

- <key/cert basename> è una stringa che identifica la nuova chiave e il nome del CSR. Può contenere caratteri alfanumerici, trattini o caratteri di sottolineatura. Campo obbligatorio.
- <CN:value> è il nome comune. Nome di dominio completo (FQDN) che specifica la posizione esatta del server nel DNS (Domain Name System). Campo obbligatorio.
- [OU:<value>] è l'unità organizzativa o il nome del reparto. Ad esempio, Supporto, IT, Tecnico, Finanza. Questo campo è facoltativo.
- [O:<valore>] è il nome dell'organizzazione o della società. Di solito il nome legalmente registrato di una società. Questo campo è facoltativo.
- [ST:<valore>] è la provincia, la regione, la contea o lo stato. Ad esempio, Buckinghamshire California. Questo campo è facoltativo.
- [C:<valore>] è il Paese. Codice ISO (International Organization for Standardization) di due lettere relativo al paese in cui si trova l'organizzazione. Ad esempio, US, GB, FR. Questo campo è facoltativo.
- [subjectAltName:<valore>] è il nome alternativo del soggetto (SAN). In base alla RFC 2459 (X509 versione 3), i certificati SSL (Secure Sockets Layer) possono specificare più nomi che il certificato deve corrispondere. Questo campo consente al certificato generato di coprire più domini. Può contenere indirizzi IP, nomi di dominio, indirizzi e-mail, nomi host DNS normali e così via, separati da virgole. Se è specificato, è necessario includere anche il CN nell'elenco. Sebbene si tratti di un campo facoltativo, è necessario compilare il campo SAN per consentire ai client XMPP (Extensible Messaging and Presence Protocol) di accettare un certificato. In caso contrario, nei client XMPP verrà visualizzato un errore di certificato.

Passaggio 2. Genera CSR Callbridge, Smpp, Webadmin e Webbridge

1. Accedere alla CLI di CMS con Putty e accedere con l'account admin.
2. Eseguire i comandi successivi per creare CSR per ogni servizio necessario in CMS. È inoltre possibile creare un singolo certificato con un carattere jolly (*.com) o con il nome di dominio completo (FQDN) del cluster come CN, FQDN di ogni server CMS e, se necessario, unire l'URL.

Servizio	Comando
Webadmin	pki csr <cert name> CN:<server FQDN>
Webbridge	pki csr <cert name> CN:<Server FQDN> subjectAltName:<Join Url>,<XMPP domain>
Callbridge CURVA Bilanciamento del carico	pki csr <cert name> CN:<Server FQDN's>

3. Se il sistema CMS è di tipo cluster, eseguire i comandi successivi.

Servizio	Comando
Callbridge CURVA Bilanciamento del carico	pki csr <cert name> CN:<cluster FQDN> subjectAltName:<Peer FQDN's>
XMPP	pki csr <cert name> CN:<Cluster FQDN> subjectAltName:<XMPP Domain>,<Peer FQDN's>

Passaggio 3. Genera CSR cluster di database e utilizza CA incorporata per firmarli

A partire dalla versione 2.7 di CMS, è necessario disporre di certificati per il cluster di database. Nella versione 2.7 è stata inclusa una CA incorporata che può essere utilizzata per firmare i certificati del database.

1. Eseguire la rimozione del cluster di database su tutti i core.
2. Nel database primario eseguire pki selfsigned dbca CN. Esempio:Pki selfsigned dbca CN:tplab.local
3. Sul server primario, eseguire pki csr dbserver CN:cmscore1.example.com subjectAltName. Esempio:cmscore2.example.com,cmscore3.example.com.
4. Nel database primario creare un certificato per il database clientpki csr dbclient CN:postgres.
5. Sul server primario, utilizzare dbca per firmare dbserver certpki con firma dbserver dbca.
6. Sul server primario, utilizzare dbca per firmare il certificato dbclient pki certificato dbclient

dbca.

7. Copiare il file dbclient.crt in tutti i server che devono connettersi a un nodo di database
8. Copiare il file dbserver.crt in tutti i server collegati al database (nodi che costituiscono il cluster di database).
9. Copiare il file dbca.crt in tutti i server.
10. Sul server database primario, eseguire i certificati cluster di database dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt. Viene utilizzato il file dbca.crt come ca-cert radice.
11. Nel server database primario eseguire il comando cluster di database localnode a.
12. Eseguire l'inizializzazione del cluster di database nel server database primario.
13. Nel server database primario eseguire lo stato del cluster di database. Vedere Nodi: (me): primario connesso.
14. In tutti gli altri core aggiunti al cluster di database, eseguire dbserver.key dbserver.crt dbclient.key dbclient.crt dbclient.crt dbca.crt.
15. In tutti i core connessi al cluster di database, ovvero che non si trovano nel percorso di un database, eseguire i certificati del cluster di database dbclient.key cbclient.crt dbca.crt.

- Sui core collegati (collocati in un database):
    - eseguire **cluster di database localnode a**.
    - eseguire l'**operazione di join del cluster di database**.

- ON core connessi (non situati nello stesso percorso di un database):
    - esegui **cluster di database localnode a**.
        - esegui **connessione cluster di database**.

Passaggio 4. Verifica dei certificati firmati

- La validità del certificato (data di scadenza) può essere verificata con l'ispezione del certificato, eseguire il comando **pki inspect <nomefile>**.
- È possibile verificare che un certificato corrisponda a una chiave privata, eseguire il comando **pki match <keyfile> <certificate file>**.
- Per verificare che un certificato sia firmato dalla CA e che il bundle di certificati possa essere utilizzato per verificarlo, eseguire il comando **pki verify <cert> <certificate bundle/Root CA>**.

Passaggio 5. Applicazione di certificati firmati a componenti su server CMS

- Per applicare i certificati a Webadmin, eseguire i comandi seguenti:

webadmin disable webadmin certs <keyfile> <certificate file> <certificate bundle/Root CA> webadmin enable

- Per applicare i certificati a Callbridge, eseguire i comandi seguenti:

callbridge certs <keyfile> <certificate file> <certificate bundle/Root CA> callbridge restart

- Per applicare i certificati a Webbridge, eseguire i comandi seguenti:

webbridge disable webbridge certs <keyfile> <certificate file> <certificate bundle/Root CA> webbridge enable

- Per applicare i certificati a XMPP, eseguire i comandi seguenti:

xmpp disable xmpp certs <keyfile> <certificate file> <certificate bundle/Root CA> xmpp enable

- Per applicare i certificati al database o sostituire i certificati scaduti nel cluster di database corrente, eseguire i comandi seguenti:

database cluster remove (on all servers, noting who was primary before beginning) database cluster certs <server_key> <server_certificate> <client_key> <
database cluster initialize (only on primary node)
database cluster join <FQDN or IP of primary> (only on slave node)
database cluster connect <FQDN or IP of primary> (only on nodes that are not part of the database cluster)

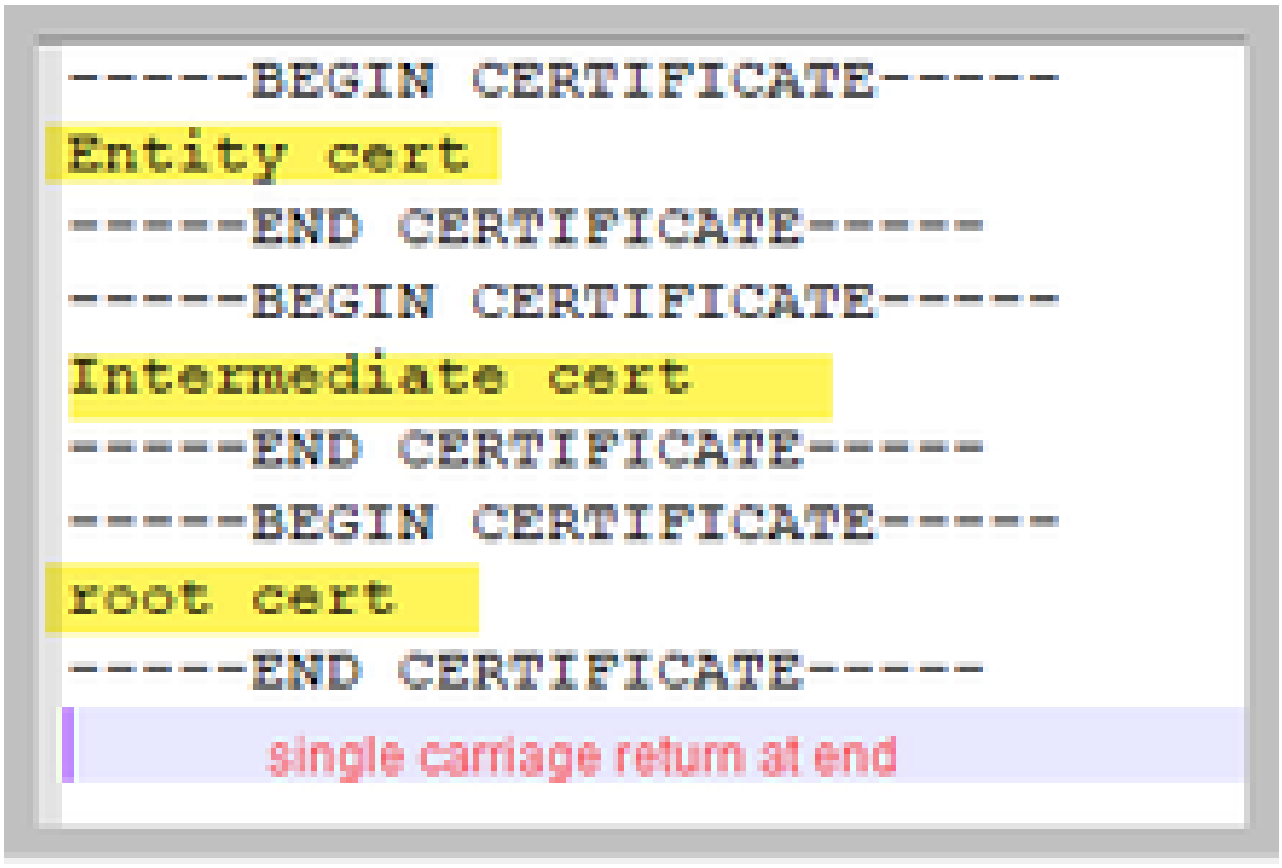
- Per applicare i certificati a TURN, eseguire i comandi seguenti:

turn disable turn certs <keyfile> <certificate file> <certificate bundle/Root CA> turn enable

Catene e pacchetti di certificati attendibili

A partire da CMS 3.0, è necessario utilizzare le catene di certificati o le catene complete. Inoltre, è importante per qualsiasi servizio che riconosca la modalità di creazione dei certificati quando si creano i pacchetti.

Quando si crea una catena di certificati, come richiesto per il bridge Web 3, è necessario crearla come illustrato nell'immagine, con il certificato di entità in primo piano, gli intermedi al centro, la CA radice in basso, quindi un singolo ritorno a capo.



Ogni volta che si crea un fascio, il certificato deve avere un solo ritorno a capo alla fine.

I bundle CA sarebbero gli stessi mostrati nell'immagine, ma, ovviamente, non ci sarebbe nessun certificato di entità.

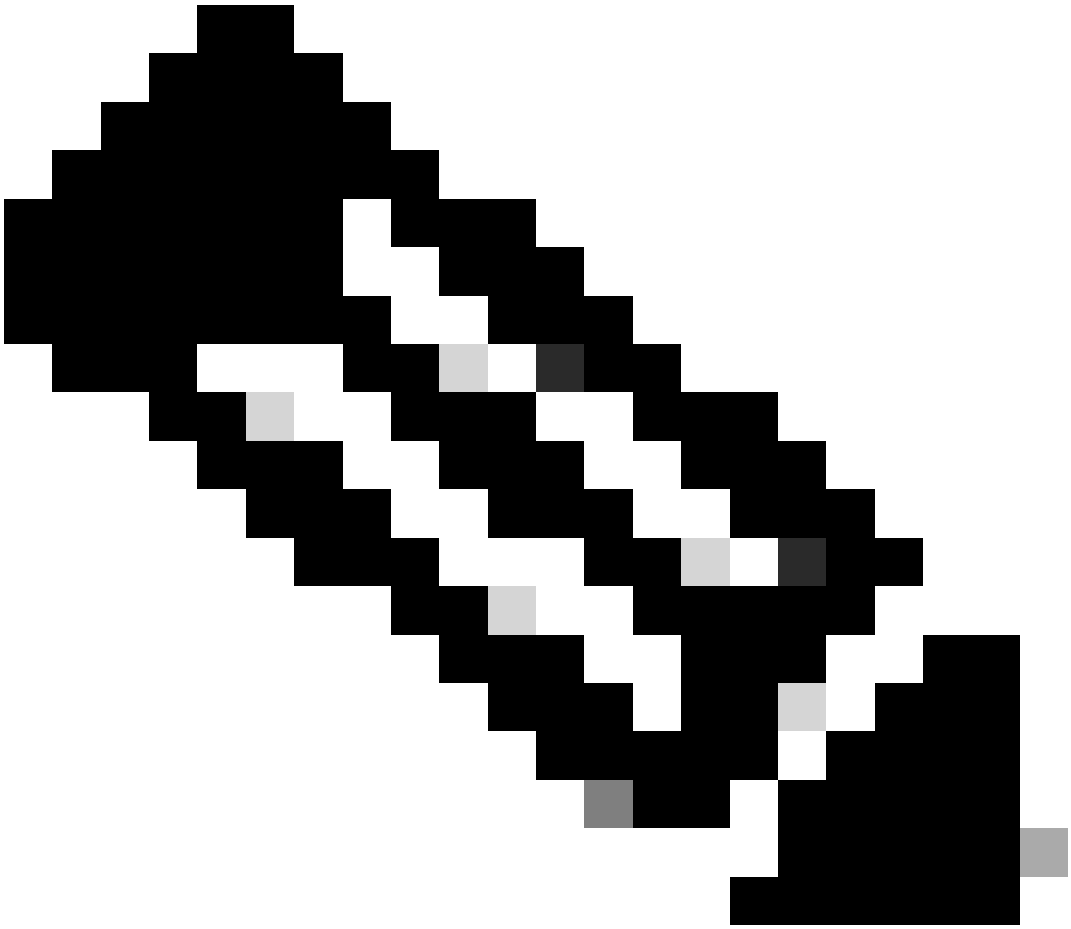
Risoluzione dei problemi

Se è necessario sostituire un certificato scaduto per tutti i servizi, ad eccezione dei certificati del database, il metodo più semplice consiste nel

caricare nuovi certificati con lo stesso nome dei certificati precedenti. In questo caso, sarà sufficiente riavviare il servizio e non sarà necessario riconfigurarlo.

Se si esegue **pki csr ...** e il nome del certificato corrisponde a una chiave corrente, il servizio verrà interrotto immediatamente. Se la produzione è in tempo reale e si creano in modo proattivo un nuovo CSR e una nuova Chiave, utilizzare un nuovo nome. È possibile rinominare il nome attualmente attivo prima di caricare il nuovo certificato nei server.

Se i certificati del database sono scaduti, è necessario verificare con **lo stato del cluster di database** chi è il database primario e, in tutti i nodi, eseguire il comando **database cluster remove**. Quindi è possibile utilizzare le istruzioni del Passaggio 3. Generare il CSR del cluster di database e utilizzare una CA incorporata per firmarli**.**



Nota: se è necessario rinnovare i certificati Cisco Meeting Manager (CMM), vedere il video successivo: Aggiornamento del certificato SSL di Cisco Meeting Management.

Informazioni correlate

- **Supporto tecnico Cisco e download**

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).