CA 署名付き複数サーバ サブジェクト代替名を含むユニファイド コミュニケーション クラスタ セットアップの設定例

目次

概要

この資料に認証局 （CA）の使用の統合された通信 クラスタを設定する方法を-署名されたマルチサーバ認証対象代替名（SAN）記述されています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Communications Manager（CUCM）
- CUCM IM および存在バージョン 10.5

この設定を試みる前に、これらのサービスをアップし、機能しています確認して下さい:

- Cisco プラットフォーム管理上の Web サービス
- Cisco Tomcat Service

Webインターフェイスのこれらのサービスを、ナビゲートは **Cisco Unified サービサビリティ ページ サービス > ネットワークサービス**に確認するために **> サーバを選択します。** それらを CLI で確認するために、**utils Service リスト** コマンドを入力して下さい。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

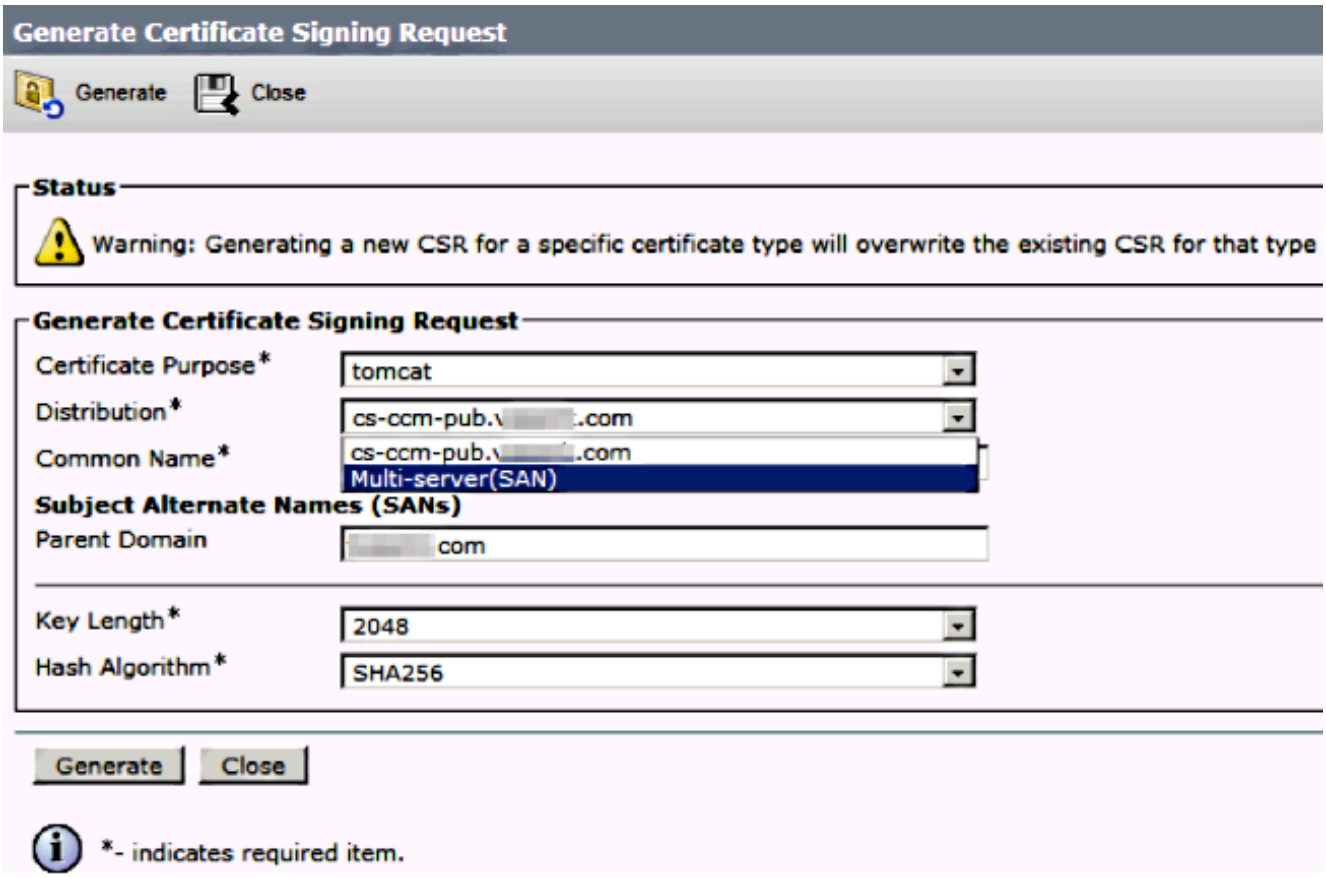
CUCM バージョン 10.5 および それ 以降では、この信頼ストア 証明書署名要求（CSR）要求は SAN および互い違いドメインを含むことができます。

1. Tomcat
2. Cisco CallManager（CCM）
3. Cisco Unified 存在拡張可能なメッセージングおよび存在プロトコル（CUP-XMPP）
4. CUP-XMPP サーバー間（S2S）

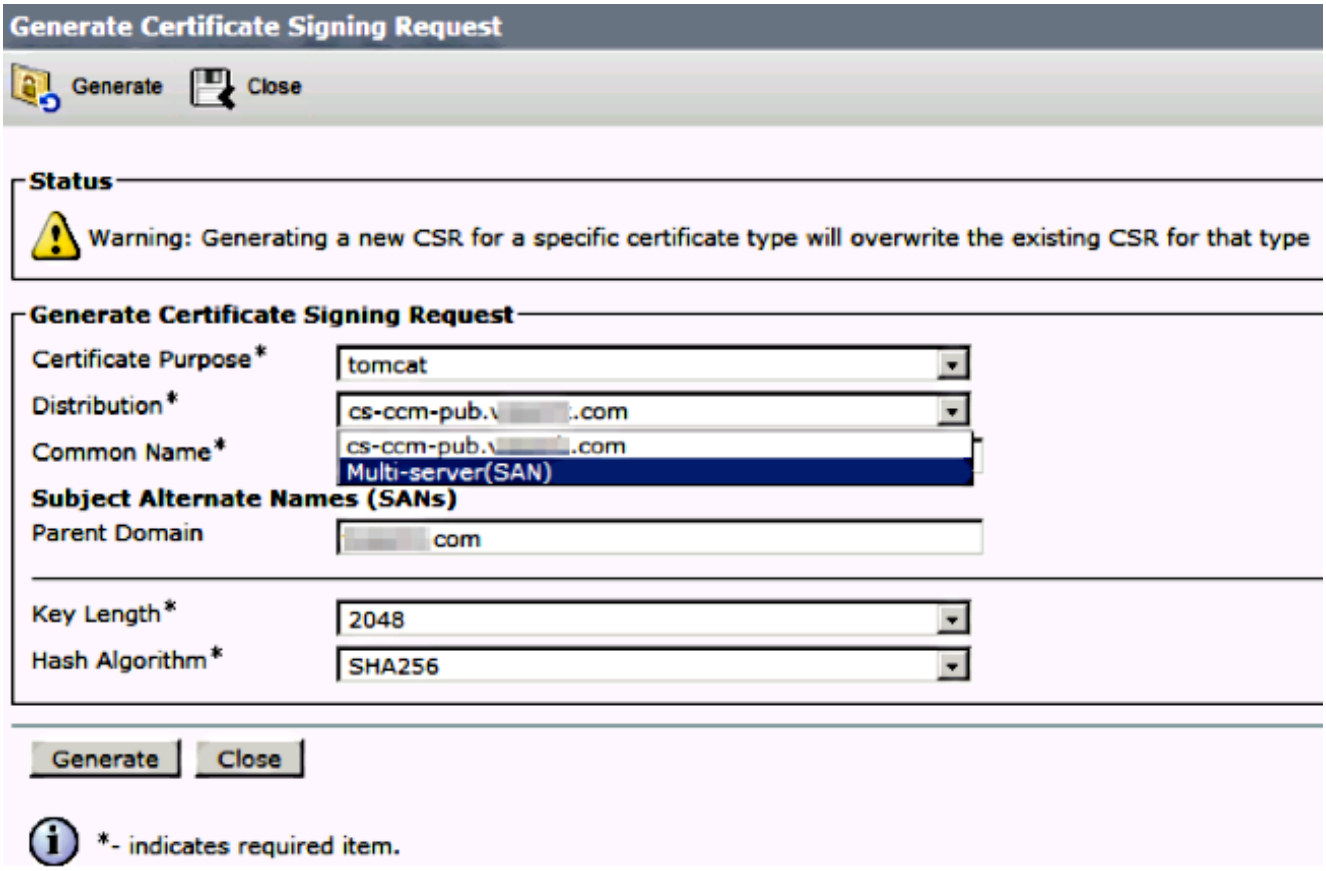
それはこのバージョンの CA署名付き証明書を得やすいです。 次に 1 CSR だけ各 Server ノードからの CSR を得、各 CSR のための CA署名付き証明書を得、それらをそれぞれ管理するために要件よりもむしろ CA によって署名するために必要となります。

設定

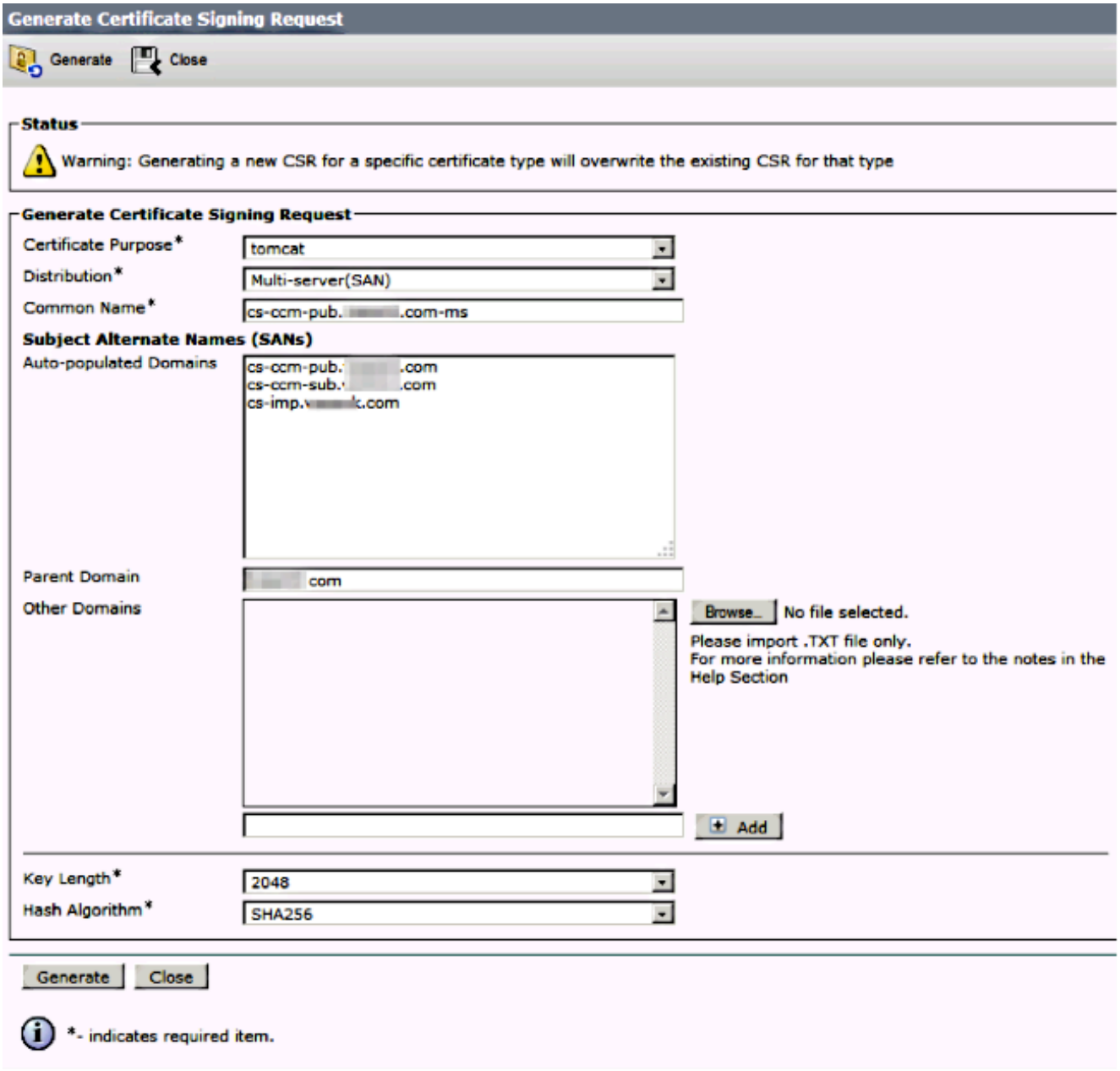
1. Operating System（OS）管理にログイン し、**セキュリティ > Certificate Management > 生成する CSR** にナビゲート して下さい。



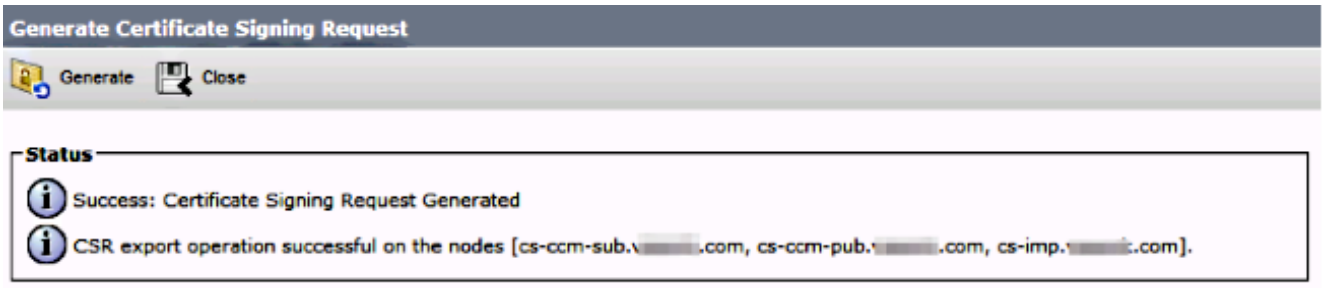
2. ディストリビューションの**マルチサーバ SAN を**選択して下さい。



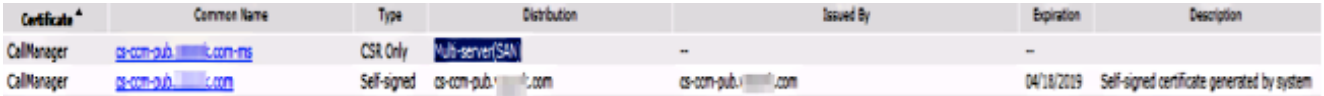
それ autopopulates SAN ドメインおよび親 ドメイン。



それが生成されれば、これは下記のものを表示します:



証明書管理では、SAN 要求は生成されます:



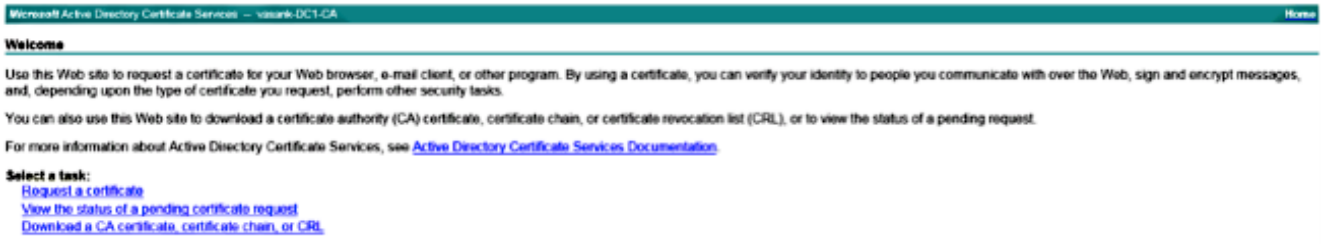
Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
CallManager	cs-ccm-pub .com-ms	CSR Only	Multi-server(SAN)	--	--	
CallManager	cs-ccm-pub .com	Self-signed	cs-ccm-pub .com	cs-ccm-pub .com	04/18/2019	Self-signed certificate generated by system

3. ローカル CA かそれを署名されて得るために VeriSign のような外部 CA を使用できます。この例は Microsoft Windows サーバーベース CA のためのコンフィギュレーションのステッ

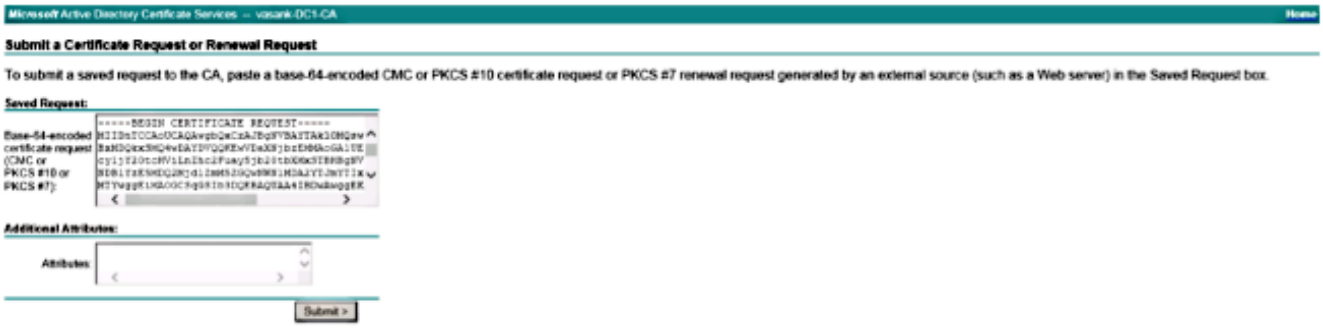
プを説明したものです。

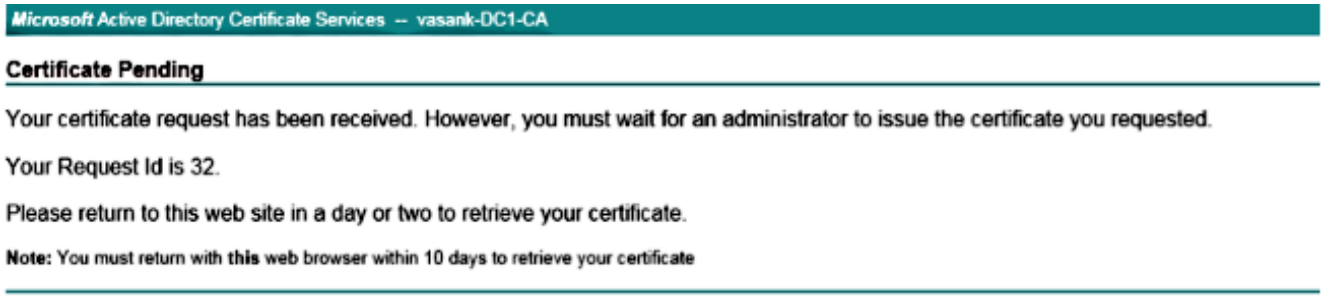
https:// <windowsserveripaddress>/certsrv/にログイン して下さい

証明書要求を『Request a certificate』 を選択 して下さい **> 進めました。**

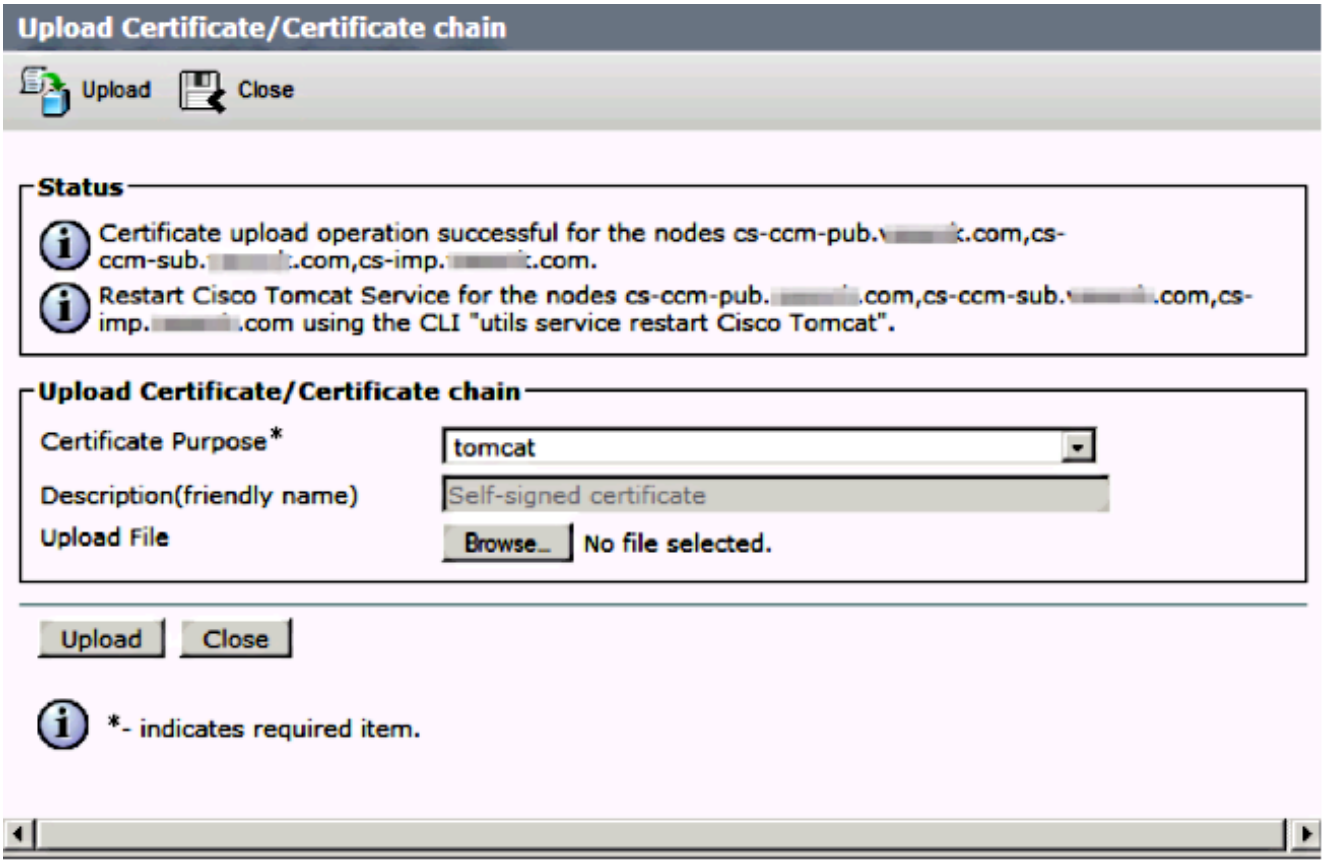


4. ここに示されているように CSR 要求を入れて下さい。

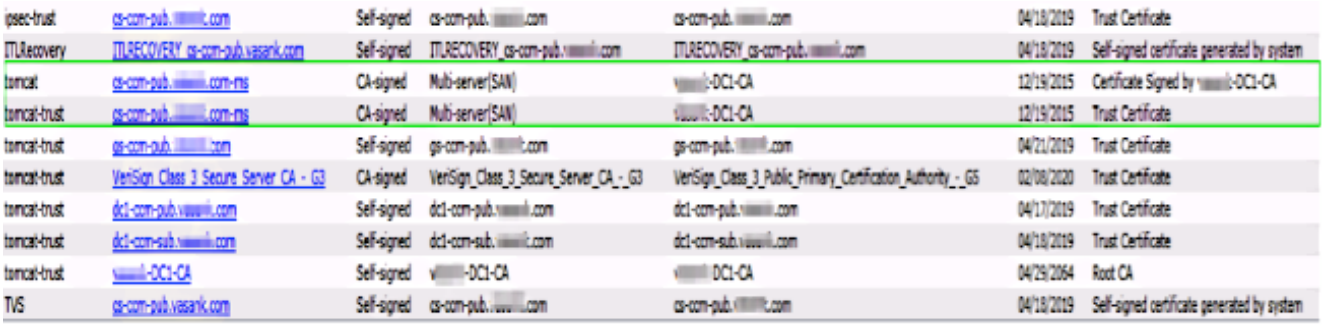




5. 認証を得れば、Tomcat 信頼として CA 認証をアップロードし、次に Tomcat として CA署名付き証明書をアップロードして下さい。



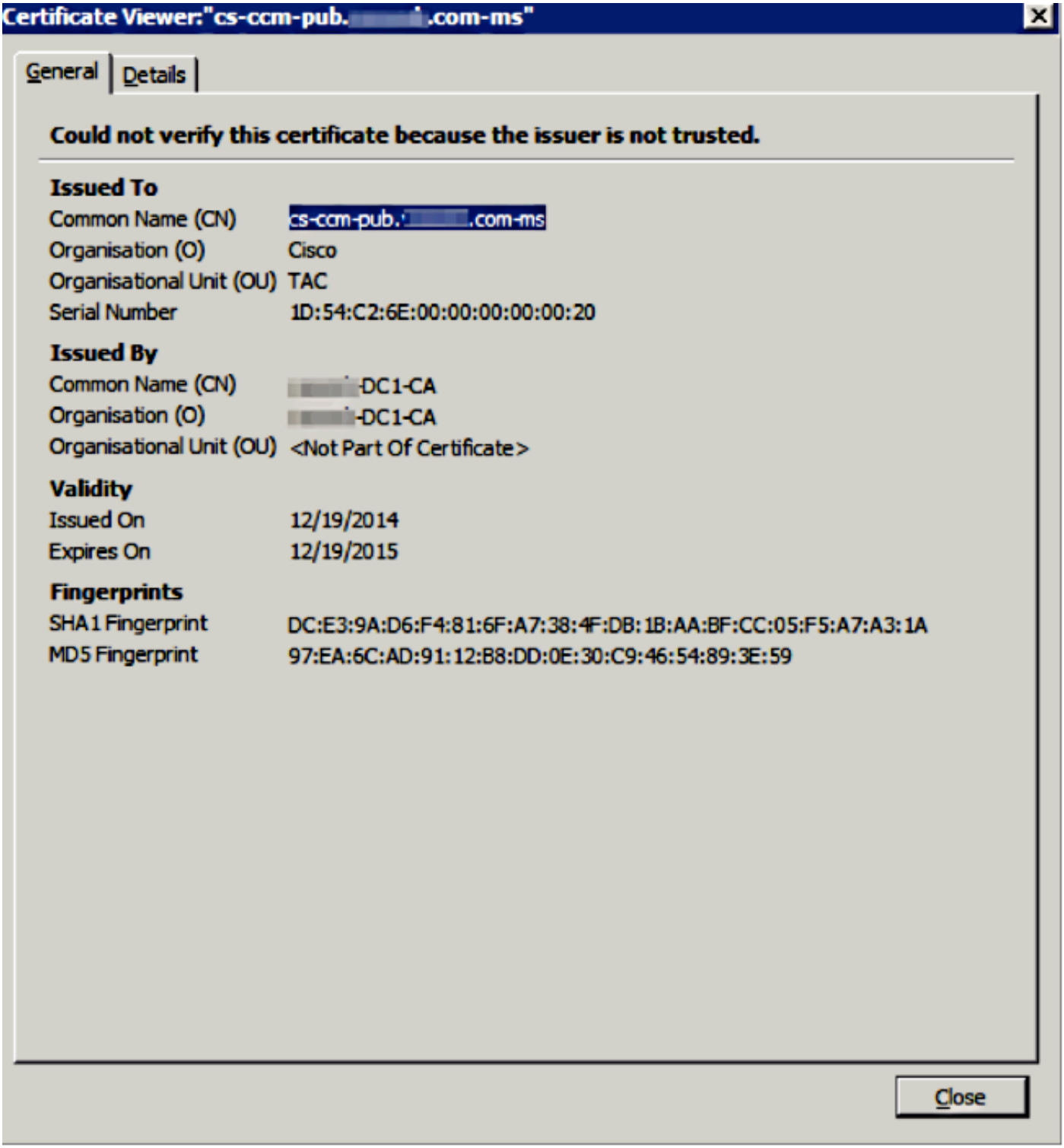
6. サービスを再起動されますアップロードされるノードを含む SAN リストのすべてのノードで確認して下さい。 証明書管理にリストされているマルチサーバ SAN を見ます。



ipsec-trust	cs-ccm-pub.[redacted].com	Self-signed	cs-ccm-pub.[redacted].com	cs-ccm-pub.[redacted].com	04/18/2019	Trust Certificate
ITLRecovery	ITLRECOVERY_cs-ccm-pub.vasank.com	Self-signed	ITLRECOVERY_cs-ccm-pub.[redacted].com	ITLRECOVERY_cs-ccm-pub.[redacted].com	04/18/2019	Self-signed certificate generated by system
tomcat	cs-ccm-pub.[redacted].com-ms	CA-signed	Multi-server(SAN)	[redacted]-DC1-CA	12/19/2015	Certificate Signed by [redacted]-DC1-CA
tomcat-trust	cs-ccm-pub.[redacted].com-ms	CA-signed	Multi-server(SAN)	[redacted]-DC1-CA	12/19/2015	Trust Certificate
tomcat-trust	cs-ccm-pub.[redacted].com	Self-signed	cs-ccm-pub.[redacted].com	cs-ccm-pub.[redacted].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-ccm-pub.[redacted].com	Self-signed	dc1-ccm-pub.[redacted].com	dc1-ccm-pub.[redacted].com	04/17/2019	Trust Certificate
tomcat-trust	dc1-ccm-sub.[redacted].com	Self-signed	dc1-ccm-sub.[redacted].com	dc1-ccm-sub.[redacted].com	04/18/2019	Trust Certificate
tomcat-trust	[redacted]-DC1-CA	Self-signed	[redacted]-DC1-CA	[redacted]-DC1-CA	04/29/2064	Root CA
TVS	cs-ccm-pub.vasank.com	Self-signed	cs-ccm-pub.[redacted].com	cs-ccm-pub.[redacted].com	04/18/2019	Self-signed certificate generated by system

確認

新しい認証が使用されるようにするために http://<fqdnofccm>:8443/ccmadmin に口グイン して下さい。



CallManager マルチサーバ SAN 認証

同じようなプロシージャは CallManager 認証のために続くことができます。 この場合、autopopulated ドメインは CallManager ノードすべてです。 それが動作しない場合、それを SAN リストから保存するか、またはそこにから取除くことを選択できます。

CA によって発行される認証をインストールした後すべてのノードの CallManagerサービスを再開して下さい。

CUCM のための CA 署名付き SAN 認証を得る前に、それを確認して下さい:

- IP Phone は信頼確認サービス (TV) を信頼できます。 これは電話から HTTPS サービスに

アクセスする場合確認することができます。 たとえば社内 ディレクトリ アクセスがはたらけば、電話が TV サービスを信頼することをそして意味します。
- それがセキュア クラスタである場合、新しい CTL ファイルが作成され、クラスタがリブートされるように Certificate trust list （ CTL ） クライアントが再実行されるようにして下さい。

トラブルシューティング

これらの口グは CA 署名付き Certficate のマルチサーバ SAN CSR 生成およびアップロードに関する問題を識別するために Cisco Technical Assistance Center を助ける必要があります。

- Cisco Unified OS プラットフォーム API
- Cisco Tomcat
- IPT プラットフォーム CertMgr ログ

既存のマルチサーバ Certifcate CUCM では、サーバのホスト名が変更すれば、認証を CA によって署名されて得ることを以前に説明されるようにマルチサーバ SAN CSR 要求を生成することを推奨します。