

ユニファイドコミュニケーションクラスタの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[確認](#)

[CallManagerマルチサーバSAN証明書](#)

[トラブルシューティング](#)

[既知の注意事項](#)

概要

このドキュメントでは、認証局(CA)署名付きマルチサーバSAN証明書を使用してユニファイドコミュニケーションクラスタを設定する方法について説明します。

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 and Presenceバージョン10.5

この設定を開始する前に、次のサービスが稼働していることを確認してください。

- Cisco Platform Administrative Webサービス
- Cisco Tomcat サービス

Webインターフェイスでこれらのサービスを確認するには、[Cisco Unified Serviceability Page Services] > [Network Service] > [Select a server] に移動します。CLIでこれらを確認するには、`utils service list`コマンドを入力します。

CUCMクラスタでSSOが有効になっている場合は、SSOを無効にして再度有効にする必要があります。

使用するコンポーネント

このドキュメントの内容は、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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

CUCMバージョン10.5以降では、この信頼ストア証明書署名要求(CSR)にサブジェクト代替名(SAN)と代替ドメインを含めることができます。

1. Tomcat:CUCMおよびIM&P
2. Cisco CallManager:CUCMのみ
3. Cisco Unified Presence-Extensible Messaging and Presence Protocol(CUP-XMPP) - IM&Pのみ
4. CUP-XMPPサーバ間(S2S):IM&Pのみ

このバージョンでは、CA署名付き証明書を取得する方が簡単です。CAが署名する必要があるCSRは1つだけです。各サーバノードからCSRを取得し、CSRごとにCA署名付き証明書を取得して、それらを個別に管理する必要はありません。

設定

ステップ 1:

パブリッシャのオペレーティングシステム(OS)管理にログインし、[Security] > [Certificate Management] > [Generate CSR]に移動します。

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.

ステップ 2 :

DistributionでMulti-Server SANを選択します。

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.

SANドメインと親ドメインが自動入力されます。

クラスタのすべてのノードがTomcat用にリストされていることを確認します。CallManager用のすべてのCUCMおよびIM&Pノードがリストされます。CUCMノードのみがリストされます。

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* Multi-server(SAN)

Common Name* cs-ccm-pub.com-ms

Subject Alternate Names (SANs)

Auto-populated Domains

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

Parent Domain:com

Other Domains

No file selected.
Please import .TXT file only.
For more information please refer to the notes in the Help Section

Key Length* 2048

Hash Algorithm* SHA256

 *- indicates required item.

ステップ 3 :

[generate]をクリックし、CSRが生成されたら、CSRにリストされているすべてのノードが [Successful CSR exported]リストにも表示されていることを確認します。

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].

証明書管理では、SAN要求が生成されます。

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)

ステップ 4 :

[Download CSR] をクリックし、証明書の目的を選択して、[Download CSR] をクリックします。

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Show Settings Security Software Upgrades Services Help

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR **Download CSR**

Download Certificate Signing Request

Download CSR Close

Status

Warning: Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

Certificate Purpose* tomcat

Download CSR Close

*- indicates required item.

ローカルCAまたはVeriSignなどの外部CAを使用して、CSR (前の手順でダウンロードしたファイル) に署名を付けることができます。

この例では、Microsoft Windows ServerベースのCAの設定手順を示します。別のCAまたは外部CAを使用している場合は、手順5に進みます。

https://<windowsserveripaddress>/certsrv/にログインします

[Request a Certificate] > [Advanced Certificate Request] を選択します。
CSRファイルの内容を[Base-64-encoded certificate request]フィールドにコピーし、[Submit] をクリックします。

Microsoft Active Directory Certificate Services -- vasank-DC1-CA Home

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](#)

次に示すように、CSR要求を送信します。

Microsoft Active Directory Certificate Services -- vasank-DC1-CA Home

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-----
MIIBzQCCAQgAggBqBwCABQgBYDAtAKIOMQaw
BARDQwckp4vSA1PVOEzFEXK3)z0B6c-0ALTE
cy11E20t:0FV1L6L6c2Fuky5j618c06KTF8BqV
N6B1ZK5MIG2RQd1286N2iQv8B1H6AJYI:INTTIX
NTYyqR1NG00C3q8Tn1D0FRAQTAAN1K0N6uqgER
< >
```

Additional Attributes:

Attributes: < >

Microsoft Active Directory Certificate Services -- vasank-DC1-CA

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

ステップ 5 :

注:Tomcat証明書をアップロードする前に、SSOが無効になっていることを確認してください。SSOが有効になっている場合は、すべてのTomcat証明書の再生成プロセスが完了したら、SSOを無効にして再度有効にする必要があります。

証明書が署名された状態で、CA証明書をtomcat-trustとしてアップロードします。最初にルート証明書、次に中間証明書 (存在する場合) です。

 **Cisco Unified Operating System Administration**
For Cisco Unified Communications Solutions

Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate List

 Generate Self-signed  **Upload Certificate/Certificate chain**  Generate CSR  Download CSR

Upload Certificate/Certificate chain

 Upload  Close

Status

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

Upload Certificate/Certificate chain

Certificate Purpose* ▾

Description(friendly name)

Upload File certchain.p7b

手順 6 :

次の図に示すように、CUCM署名付き証明書をTomcatとしてアップロードし、クラスタのすべてのノードが[Certificate upload operation successful]に表示されていることを確認します。

Upload Certificate/Certificate chain

 Upload  Close

Status

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

Description(friendly name)

Upload File No file selected.

 *- indicates required item.

マルチサーバSANは、次の図に示すように[Certificate Management]に表示されます。

ipsecc-trust	cs-ccm-pub.com	Self-signed	cs-ccm-pub.com	cs-ccm-pub.com	04/18/2019	Trust Certificate
ITLRecovery	ITLRECOVERY cs-ccm-pub.com	Self-signed	ITLRECOVERY cs-ccm-pub.com	ITLRECOVERY cs-ccm-pub.com	04/18/2019	Self-signed certificate generated by system
tomcat	cs-ccm-pub.com-ms	CA-signed	Multi-server(SAN)DC1-CA	12/19/2015	Certificate Signed byDC1-CA
tomcat-trust	cs-ccm-pub.com-ms	CA-signed	Multi-server(SAN)DC1-CA	12/19/2015	Trust Certificate
tomcat-trust	cs-ccm-pub.com	Self-signed	cs-ccm-pub.com	cs-ccm-pub.com	04/21/2019	Trust Certificate
tomcat-trust	VerSign_Class_3_Secure_Server_CA_-_G3	CA-signed	VerSign_Class_3_Secure_Server_CA_-_G3	VerSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/08/2020	Trust Certificate
tomcat-trust	dc1-ccm-pub.com	Self-signed	dc1-ccm-pub.com	dc1-ccm-pub.com	04/17/2019	Trust Certificate
tomcat-trust	dc1-ccm-pub.com	Self-signed	dc1-ccm-pub.com	dc1-ccm-pub.com	04/18/2019	Trust Certificate
tomcat-trustDC1-CA	Self-signedDC1-CADC1-CA	04/29/2064	Root CA
TVS	cs-ccm-pub.com	Self-signed	cs-ccm-pub.com	cs-ccm-pub.com	04/18/2019	Self-signed certificate generated by system

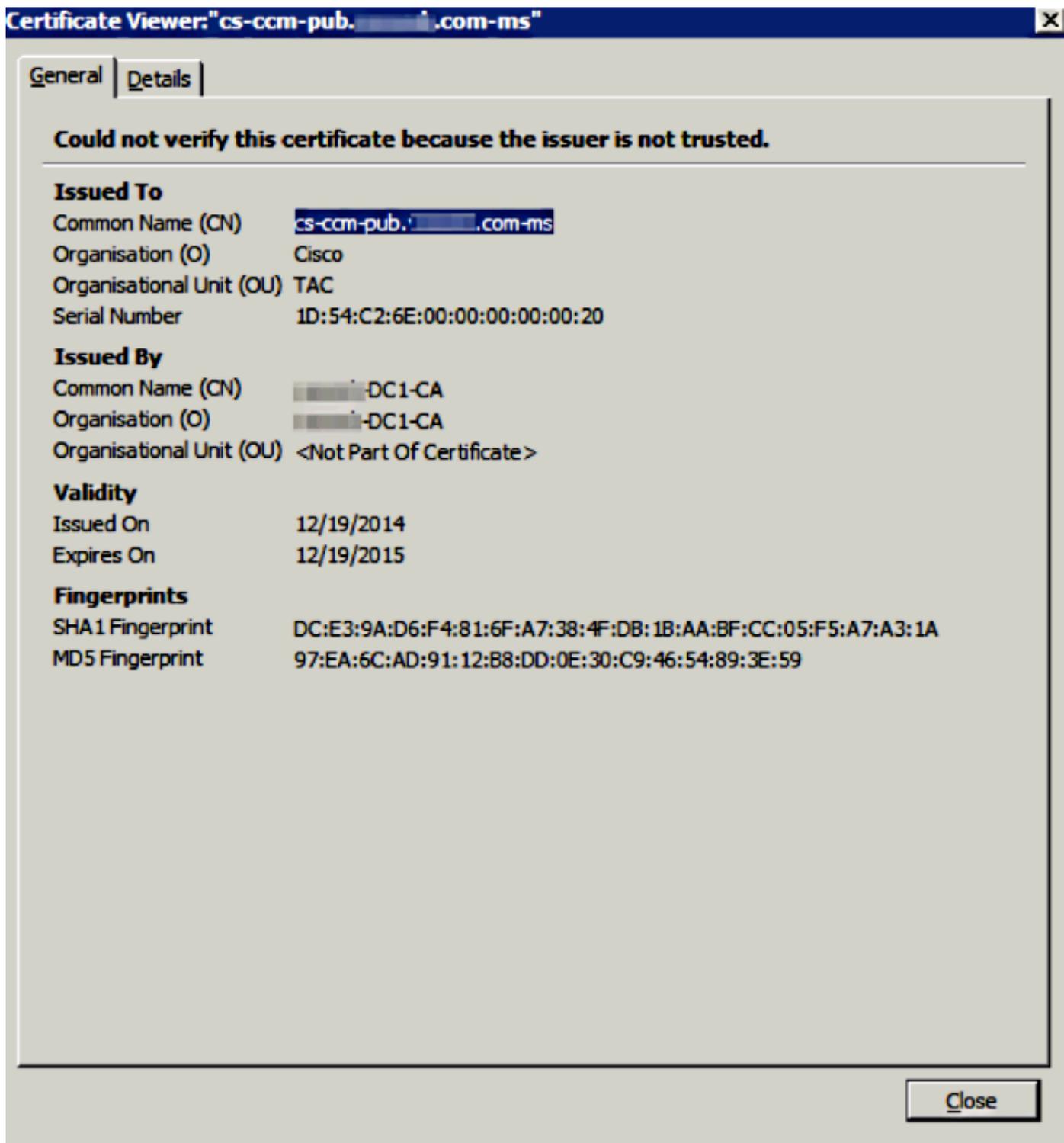
手順 7 :

CLIでutils service restart Cisco Tomcatコマンドを使用して、SANリスト内のすべてのノード（最初のパブリッシャとサブスクリバ）でTomcatサービスを再起動します。

```
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:
```

確認

http://<fqdnofccm>:8443/ccmadminにログインして、新しい証明書が使用されていることを確認します。



CallManagerマルチサーバSAN証明書

CallManager証明書についても同様の手順を実行できます。この場合、自動入力ドメインはCallManagerノードだけです。Cisco CallManagerサービスが実行されていない場合は、SANリストに保持するか、削除するかを選択できます。

警告：このプロセスは、電話機の登録とコール処理に影響します。CUCM/TVS/ITL/CAPF証明書を使用して作業する場合は、必ずメンテナンスウィンドウをスケジュールしてください。

。

CUCMのCA署名付きSAN証明書の前に、次のことを確認します。

- IP PhoneはTrust Verification Service(TVS)を信頼できます。これは、電話機から任意のHTTPSサービスにアクセスすることで確認できます。たとえば、社内ディレクトリアクセスが機能する場合、電話機はTVSサービスを信頼することを意味します。
- クラスタが非セキュアモードか混合モードかを確認します。

混合モードクラスタかどうかを確認するには、[Cisco Unified CM Administration] > [System] > [Enterprise Parameters] > [Cluster Security Mode](0 == Non-Secure、1 == Mixed Mode)。

警告：サービスを再起動する前に混合モードクラスタを使用している場合は、CTLを[トークン](#)または[トークンレス](#)に更新する必要があります。

CAによって発行された証明書をインストールした後、有効になっているノードで次のサービスのリストを再起動する必要があります。

- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CallManager
- [Cisco Unified Serviceability] > [Tools] > [Control Center - Feature Services] > [Cisco CTIManager]
- [Cisco Unified Serviceability] > [Tools] > [Control Center - Network Services] > [Cisco Trust Verification Service]

トラブルシューティング

これらのログは、Cisco Technical Assistance Center(TAC)がマルチサーバSAN CSRの生成とCA署名付き証明書のアップロードに関連する問題を特定するのに役立ちます。

- Cisco Unified OS Platform API
- Cisco Tomcat
- IPTプラットフォーム CertMgr ログ
- [証明書の更新プロセス](#)

既知の注意事項

- Cisco Bug ID [CSCur97909](#) : マルチサーバ証明書をアップロードしても、DB内の自己署名証明書が削除されない
- Cisco Bug ID [CSCus47235](#) - CSRのためにCUCM 10.5.2がSANに複製されない
- Cisco Bug ID [CSCup28852](#) : マルチサーバ証明書を使用する場合の証明書の更新により、電話機が7分ごとにリセットされる

既存のマルチサーバ証明書がある場合は、次のシナリオで再生成が推奨されます。

- ホスト名またはドメインの変更。ホスト名またはドメインの変更が実行されると、証明書は自己署名として自動的に再生成されます。これをCA署名付きに変更するには、前の手順に従う必要があります。
- 新しいノードがクラスタに追加された場合は、新しいノードを含めるために新しいCSRを生成する必要があります。
- サブスクリバが復元され、バックアップが使用されなかった場合、ノードは新しい自己署名

名証明書を持つことができます。サブスクリバを含めるには、クラスタ全体の新しい CSRが必要になる場合があります。(拡張要求があります。Cisco Bug ID [CSCuv75957](#) この機能を追加します)。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。