

Konfigurieren eines von einer Zertifizierungsstelle signierten Multiserver-Betreffs als Alternativname in CVOS-Systemen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die Einrichtung eines Cisco Voice Operating System (CVOS)-System-Clusters mithilfe eines CA-SAN (Certificate Authority)-Signed Multi-Server Subject Alternate Name) mit Publisher-Subscriber-Architekturmodell beschrieben. Das CVOS-System deckt CUIC-, Finesse-, Livedata- und IdS-Systeme in UCCE-Umgebungen ab.

Beitrag von Venu Gopal Sane, Ritesh Desai Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Unified Contact Center Enterprise (UCCE) Version 12.5
- Cisco Package Contact Center Enterprise (PCCE) Version 12.5
- Cisco Finesse v12.5
- Cisco Unified Intelligence Center v12.5

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Verwaltung des CVOS-Betriebssystems (Certificate Management, Zertifikatsverwaltung).

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Bei SAN-Zertifikaten mit mehreren Servern muss nur ein CSR für einen Cluster von Knoten von der

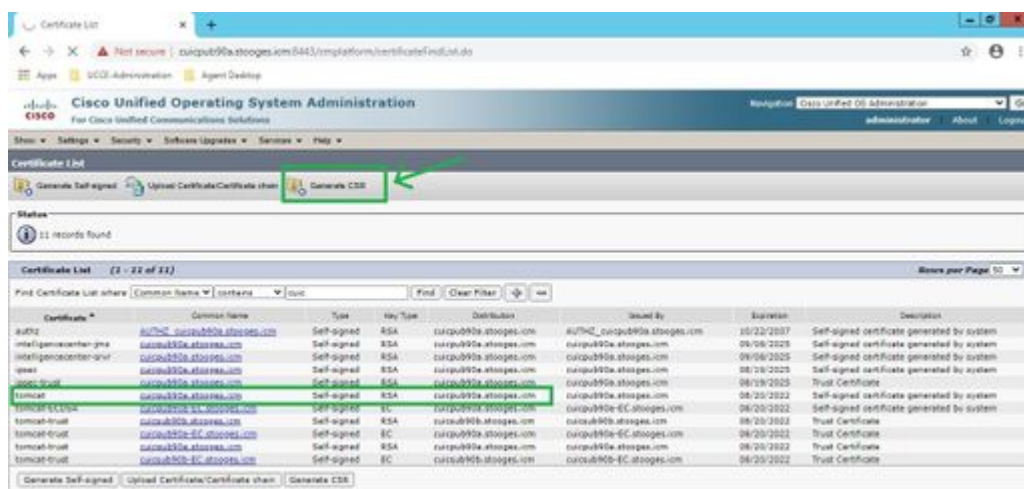
Zertifizierungsstelle signiert werden, und nicht ein CSR von jedem Serverknoten des Clusters, der dann ein Zertifikat mit CA-Signatur für jeden CSR erhält und einzeln verwaltet.

Stellen Sie vor der Konfiguration sicher, dass die folgenden Services verfügbar und funktionsfähig sind:

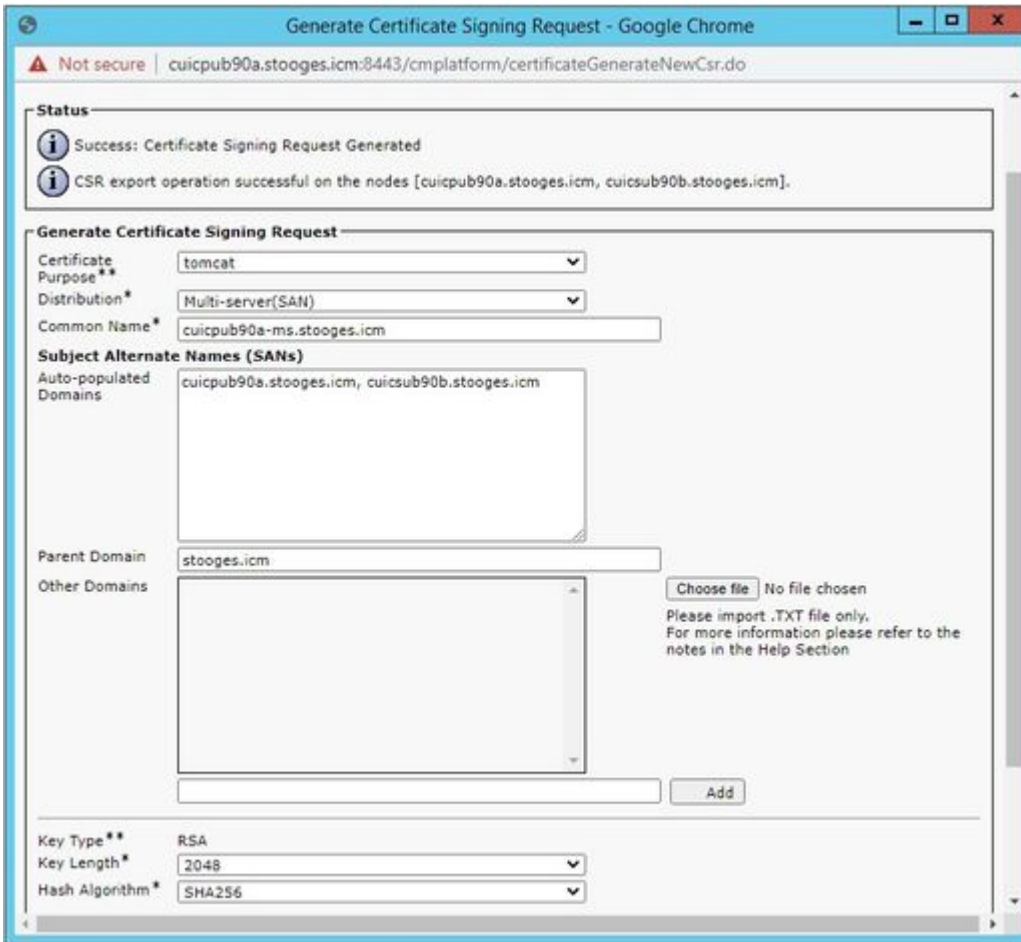
- Cisco Tomcat Service
- Benachrichtigung über Änderung des Cisco Zertifikats
- Überwachung auf Ablauf von Cisco Zertifikaten

Konfigurieren

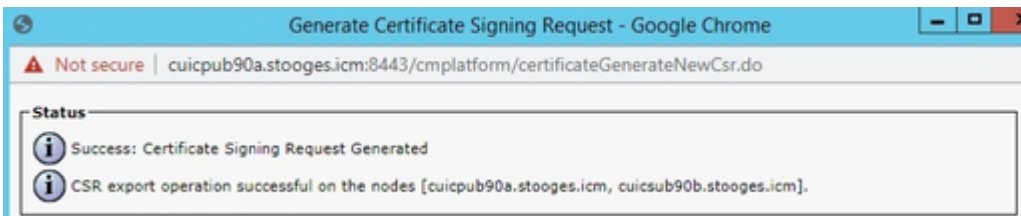
Schritt 1: Melden Sie sich bei der Betriebssystemverwaltung an, und navigieren Sie zu **Security > Certificate Management > Generate CSR (Sicherheit > Zertifikatsverwaltung > CSR generieren)**, wie im Abbild dargestellt.



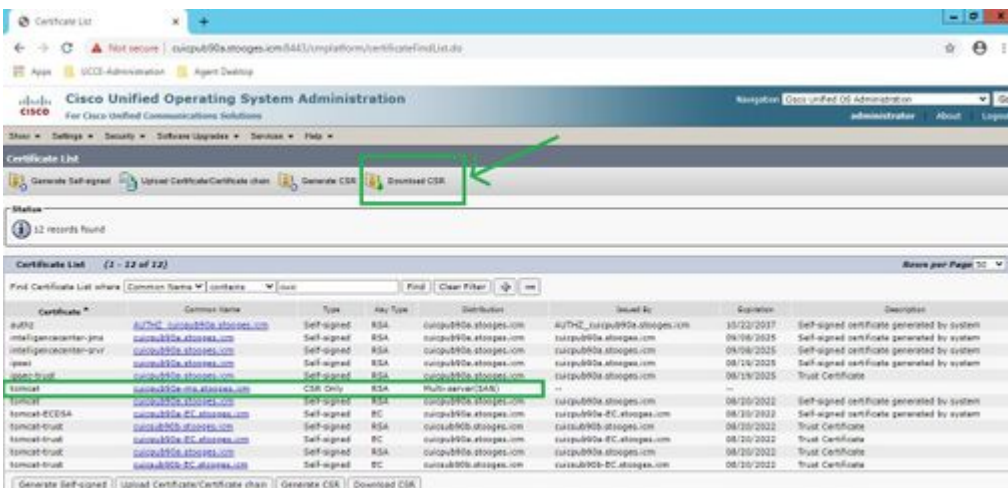
Schritt 2: Wählen Sie **Multi-Server SAN** in Distribution aus. Die SAN-Domänen und die übergeordnete Domäne werden automatisch aufgefüllt.



Schritt 3: Die erfolgreiche Generierung der CSR-Anfrage zeigt folgende Meldung an:



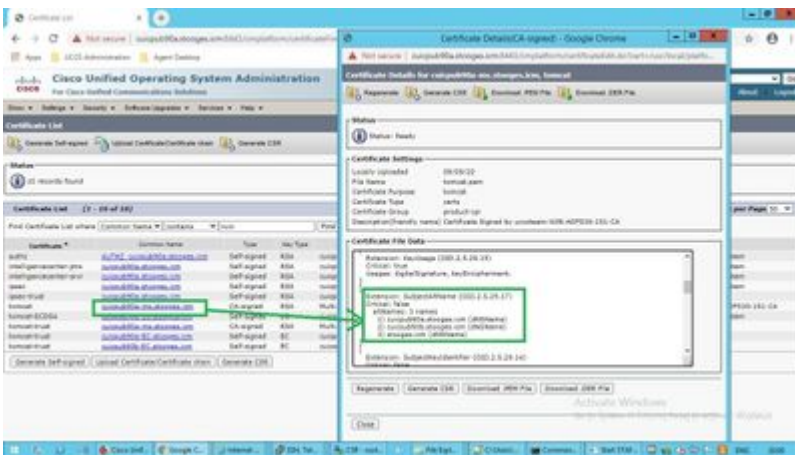
Schritt 4: Nach der erfolgreichen Generierung der CSR-Anfrage können Sie hier die generierte CSR-Anfrage sehen, die Sie herunterladen und zur Signatur an die Zertifizierungsstelle senden können.



Schritt 5: Laden Sie das CA-signierte Zertifikat als Typ tomcat in den Publisher-Knoten des Clusters auf der Seite für die Zertifikatsverwaltung hoch, und befolgen Sie die Anweisungen, die beim erfolgreichen Hochladen angezeigt werden.



Schritt 6: Nachdem die Datei erfolgreich hochgeladen wurde, überprüfen Sie die Zertifikatsliste, die das neue CA-signierte Zertifikat als Typ multi-SAN anzeigt.



Klicken Sie auf das neue Multi-SAN-Zertifikat, und überprüfen Sie, ob SubjectAltNames den Domännennamen und die FQDNs aller Cluster-Knoten anzeigt.

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Melden Sie sich bei der Seite "**cmplatform**" der Subscriber-Knoten an, und überprüfen Sie, ob das gleiche Multi-SAN-Zertifikat mit der Verwendung von <http://<any-node-fqdn>.8443/cmplatform> ausgefüllt ist.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Erfassen Sie diese Zertifikatsmanagement-Protokolle vom CLI-Zugriff, und öffnen Sie das Ticket beim Cisco TAC: **Datei erhalten Sie eine aktive Protokollplattform/log/cert***

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.