Exemple de configuration de Cisco Secure SRST

Contenu

Introduction

Ce document fournit un exemple de configuration pour la téléphonie sécuritaire à distance survivable Cisco (SRST).

Sécurisez les Téléphones IP de Cisco qui se trouvent aux sites distants et qui sont reliés aux Routeurs de passerelle peuvent communiquer sécurisé au-dessus du WAN avec le Cisco CallManager. Mais si le lien WAN ou le Cisco CallManager descend, toute la transmission par les téléphones distants devient nonsecure. Afin de surmonter cette situation, les Routeurs de passerelle peuvent maintenant fonctionner en mode sécurisé SRST, qui lance quand le lien WAN ou le Cisco CallManager descend. Quand le lien WAN ou le Cisco CallManager est restauré, les reprises de Cisco CallManager sécurisent des capacités de gestion des appels.

SRST sécurisé fournit de nouvelles fonctionnalités de sécurité SRST telles que l'authentification, l'intégrité, et le cryptage de medias. L'authentification fournit l'assurance à un interlocuteur qu'un autre interlocuteur est qui il prétend être. L'intégrité fournit l'assurance que les données données ne sont pas modifiées entre les entités. Le cryptage implique la confidentialité, ainsi il signifie que personne ne peut lire les données excepté le destinataire destiné. Ces fonctionnalités de sécurité permettent l'intimité pour des communications voix SRST et se protègent contre des violations et

l'usurpation d'identité de sécurité voix.

La Sécurité SRST est réalisée quand :

- Des périphériques d'extrémité sont authentifiés avec des Certificats.
- La signalisation est authentifiée et chiffrée avec le Transport Layer Security (TLS) pour le TCP.
- Un chemin sécurisé de medias est chiffré avec le Real-Time Transport Protocol sécurisé (SRTP).
- Des Certificats sont générés et distribués par un Autorité de certification (CA).

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

Conditions requises d'infrastructure de clé publique

- Réglez l'horloge, manuellement ou avec le Protocole NTP (Network Time Protocol). Ceci assure le synchronicity avec le Cisco CallManager.
- Activez l'ip http server (processeur de Cisco IOS®) avec la commande d'**ip http server**, sinon déjà activé. Référez-vous au serveur de certificat de Cisco IOS pour plus d'informations sur le déploiement d'Infrastructure à clés publiques (PKI).
- Si le serveur de certificat fait partie de votre configuration de démarrage, vous pouvez potentiellement voir ces messages pendant la procédure de démarrage :`% Failed to find Certificate Server's trustpoint at startup % Failed to find Certificate Server's cert.` Ces messages sont des messages d'information et indiquent une incapacité provisoire de configurer le serveur de certificat, parce que la configuration de démarrage n'est pas entièrement analysée encore. Les messages sont utiles afin de mettre au point, au cas où la configuration de démarrage serait corrompue. Vous pouvez vérifier l'état du serveur de certificat après la procédure de démarrage avec la commande de **show crypto pki server**.

Conditions requises SRST

- Des services sécurisés SRST ne peuvent pas être inscrits tandis que SRST est en activité. Désactivez par conséquent SRST avec l'**aucune** commande d'appel-gestionnaire-**retour**.
- Référez-vous aux medias et l'authentification et la fonctionnalité de chiffrement de signalisation pour des passerelles MGCP de Cisco IOS pour une liste de Téléphones IP, de Routeurs, de modules réseau, et de codecs pris en charge de Cisco pour SRST sécurisé.
- Référez-vous au micrologiciel du Cisco Unified SRST 4.0, aux Plateformes, à la mémoire, et aux Produits pris en charge de Voix pour les informations les plus à jour sur le nombre maximal de Téléphones IP de Cisco, le nombre maximal de nombres de répertoire (dn) ou de ports vocaux virtuels, et les mémoires réquises pour Cisco SRST.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Les Téléphones IP sécurisés de Cisco pris en charge dans SRST sécurisé doivent avoir des Certificats installés et le cryptage activé.
- Le routeur SRST doit avoir un certificat. Acertificate peut être généré par un tiers ou par l'Autorité de certification (CA) de Cisco IOS. Le Cisco IOS CA peut fonctionner sur la même passerelle que SRST.
- Des listes de confiance de certificat (CTLs) sur le Cisco CallManager doivent être activées. Pour des instructions complètes, référez-vous à la section *sécurisée configurante d'appels de Téléphonie sur IP de* medias et authentification de signalisation et à la fonctionnalité de chiffrement pour des passerelles MGCP de Cisco IOS.
- Le Cisco CallManager 4.1(2) ou plus tard doit être installé et doit prendre en charge la security mode (authentifiez et mode de chiffrement).
- Routeurs de passerelle que le passage SRST sécurisé doit prendre en charge des images de voix et de Cisco IOS de sécurité activée (une image logicielle cryptographique de de Â d'âÂ de k9 de Â d'âÂ). Deux images sont prises en charge : Services IP avancés, qui inclut un certain nombre de fonctionnalités de sécurité avancée, et services d'entreprise avancés, qui inclut le plein logiciel de Cisco IOS.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Restrictions

Restrictions générales

- Les caractéristiques de logiciel cryptographiques (de Â d'âÂ de k9 de Â d'âÂ) sont sous des contrôles d'exportation. Ce produit contient les caractéristiques cryptographiques et est sujet aux Etats-Unis et à des lois locales de pays régissant l'importation, l'exportation, le transfert, et l'utilisation. La livraison des produits cryptographiques Cisco n'implique pas la tiers autorité pour importer, exporter, distribuer, ou utiliser le cryptage. Les importations, les exportateurs, les distributeurs, et les utilisateurs sont responsables de la conformité aux États-Unis et aux lois locales de pays. À l'aide de ce produit vous acceptez de se conformer aux lois et réglementations applicables. Si vous ne pouvez pas se conformer aux États-Unis et aux lois locales, renvoyez ce produit immédiatement.Un résumé des lois des États-Unis régissant des produits cryptographiques Cisco peut être trouvé à :http://www.cisco.com/wwl/export/crypto/tool/Si vous avez besoin davantage de d'assistance, svp contactez-nous en envoyant le courrier électronique à export@cisco.com.
- Quand un appel chiffré sécurisé du Real-Time Transport Protocol (SRTP) est fait entre les points finaux de téléphone IP de Cisco ou à partir d'un téléphone IP de Cisco à un point d'extrémité de passerelle, une icône de verrouillage est affichée sur les Téléphones IP. Le verrouillage indique la Sécurité seulement pour le tronçon IP de l'appel. Le degré de sécurité du tronçon PSTN n'est pas impliqué.
- SRST sécurisé est pris en charge seulement à portée d'un routeur unique.

Fonctions non prises en charge et logiciel en mode sécurisé SRST

- Versions antérieures à 4.1(2) de Cisco CallManager
- Musique d'attente sécurisée (MoH)
- Transcodage ou Conférences sécurisé
- Sécurisez H.323 ou SIROTEZ
- Hot Standby Router Protocol (HSRP)

Appels pris en charge en mode sécurisé SRST

Seulement des communications voix sont prises en charge en mode sécurisé SRST. Spécifiquement, ces communications voix sont prises en charge :

- Appel de base
- Appel en avant (occupé, pas de réponse, tous)
- Ligne partagée (Téléphones IP)
- Transfert d'appel (consultez et l'aveugle)
- Tenez et reprenez

Informations générales

Retour de libellé de Téléphones IP de Cisco pendant le SRST

Les versions de Cisco SRST plus tôt que le Logiciel Cisco IOS version 12.3(14)T ne peuvent pas prendre en charge les connexions sécurisées ou avoir la sécurité activée. Si un routeur SRST n'est pas capable de SRST sécurisé comme du Â de modeâÂ de retour c'est-à-dire, il ne peut pas se terminer une prise de contact de TLS avec le du Â de Cisco CallManagerâÂ que son certificat n'est pas ajouté au fichier de configuration du téléphone IP de Cisco. L'absence d'un certificat de routeur SRST fait utiliser le téléphone IP de Cisco la transmission nonsecure (de libellé) quand en mode de retour SRST. La capacité à la détecter et le retour en mode de libellé est établie dans le micrologiciel de téléphone IP de Cisco. Référez-vous aux medias et l'authentification et la fonctionnalité de chiffrement de signalisation pour des passerelles MGCP de Cisco IOS pour plus d'informations sur le mode de libellé.

Routeurs et le TLS Protocol SRST

La version 1.0 de Transport Layer Security (TLS) fournit les canaux sécurisés de TCP entre les Téléphones IP de Cisco, les Routeurs sécurisés SRST, et le Cisco CallManager. Le processus de TLS commence quand le téléphone IP de Cisco établit une connexion de TLS quand il s'inscrit au Cisco CallManager. Si le Cisco CallManager est configuré au retour à SRST, la connexion de TLS entre les Téléphones IP de Cisco et le routeur sécurisé SRST est également établie. Si le lien WAN ou le Cisco CallManager échoue, le Contrôle d'appel retourne au routeur SRST.

Routeurs et PKI SRST

Le transfert des Certificats entre un routeur SRST et un Cisco CallManager est obligatoire pour la fonctionnalité sécurisée SRST. Des commandes d'Infrastructure à clés publiques (PKI) sont utilisées pour générer, importer, et exporter les Certificats pour SRST sécurisé. Les Certificats pour chaque téléphone IP pris en charge de Cisco sont affichés dans cette table.

Tableau 1 - Téléphones IP et Certificats pris en charge de Cisco

Téléphone IP 7940 de Cisco	Téléphone IP 7960 de Cisco	Téléphone IP 7970 de Cisco
Le téléphone reçoit localement - le certificat significatif (LSC) de la fonction de proxy d'autorité de certification (CAPF) dans le format distingué des règles de codage (DER). Nom du fichier de certificat : 59fe77ccd.0 que le nom du fichier peut changer basé sur le nom du sujet de certificat CAPF et l'émetteur de certificat CAPF. Si le Cisco CallManager utilise un tiers fournisseur de certificat, il peut y avoir plusieurs .0 fichier (de deux à dix). Chaque .0 fichier du certificat doit être importé individuellement pendant la configuration. L'Inscription manuelle est prise en charge seulement.	Le téléphone reçoit localement - le certificat significatif (LSC) de la fonction de proxy d'autorité de certification (CAPF) dans le format distingué des règles de codage (DER). Nom du fichier de certificat : 59fe77ccd.0 que le nom du fichier peut changer basé sur le nom du sujet de certificat CAPF et l'émetteur de certificat CAPF. Si le Cisco CallManager utilise un tiers fournisseur de certificat, il peut y avoir plusieurs .0 fichier (de deux à dix). Chaque .0 fichier du certificat doit être importé individuellement pendant la configuration. L'Inscription manuelle est prise en charge seulement.	Le téléphone contient un certificat installé par fabrication (MIC) utilisé pour l'authentification de périphérique. Si Cisco 7970 implémente la MIC, deux fichiers du certificat publics sont nécessaires : • CiscoCA.pem (Cisco enracinent le CA, utilisé pour authentifi

		er le certificat) • a69d2e04.0, dans le format du Privacy Enhanced Mail (PEM) Si le Cisco CallManager utilise un tiers fournisseur de certificat, il peut y avoir plusieurs .0 fichier (de deux à dix). Chaque .0 fichier du certificat doit être importé individuellement pendant la configuration. L'Inscription manuelle

		est prise en charge seulement.

Serveur de qualifications de Cisco IOS sur les Routeurs sécurisés SRST

SRST sécurisé présente un serveur de qualifications qui fonctionne sur un routeur sécurisé SRST. Quand le client, Cisco CallManager, demande un certificat par le canal de TLS, le serveur de qualifications fournit le certificat de routeur SRST au Cisco CallManager. Le Cisco CallManager insère le certificat de routeur SRST dans le fichier de configuration de téléphone IP de Cisco et télécharge les fichiers de configuration aux téléphones. Le téléphone IP sécurisé de Cisco emploie le certificat pour authentifier le routeur SRST pendant les exécutions de retour. Le service de qualifications fonctionne sur le port TCP par défaut 2445.

Cinq nouvelles commandes Cisco IOS configurent le serveur de qualifications en mode d'appel-gestionnaire-retour et fournissent des capacités d'élimination des imperfections et de vérification de serveur :

- qualifications
- debug credentials
- source-address d'IP (qualifications)
- affichez les qualifications
- point de confiance (qualifications)

Établissement de SRST sécurisé au téléphone IP de Cisco

Ce diagramme affiche l'interworking du serveur de qualifications sur le routeur SRST, le Cisco CallManager, et le téléphone IP de Cisco, qui établit SRST sécurisé au téléphone IP de Cisco.

1. Le téléphone IP de Cisco configure le DHCP et obtient l'adresse du serveur TFTP.
2. Le téléphone IP de Cisco récupère un fichier CTL du serveur TFTP. Le fichier CTL contient les Certificats aux lesquels le téléphone est censé pour faire confiance.
3. Le téléphone IP de Cisco ouvre un canal et des registres de protocole de Transport Layer Security (TLS) au Cisco CallManager.

Les exportations de Cisco CallManager sécurisent les informations de routeur SRST et le certificat de routeur SRST au téléphone IP de Cisco. Le téléphone place le certificat dans sa configuration.

Une fois le téléphone a le certificat SRST, le routeur SRST est considéré sécurisé.

Si le téléphone IP de Cisco est configuré en tant que du Â d'authenticatedâÂ de du Â d'âÂ ou et Cisco CallManager du Â d'encryptedâÂ de du Â d'âÂ est configuré dans le mode mixte, le téléphone recherche un certificat SRST dans son fichier de configuration. S'il trouve un certificat SRST, il ouvre une connexion de réserve de TLS au port par défaut. Le port par défaut est le port TCP de téléphone IP de Cisco plus 443, qui est le port 2443 sur un routeur SRST. La connexion au routeur SRST se produit automatiquement, tant que il n'y a pas un Cisco CallManager secondaire et le SRST est configuré comme périphérique de sauvegarde.

Le Cisco CallManager doit être configuré dans le mode mixte, qui est son mode sécurisé.

En cas de panne BLÊME, le téléphone IP de Cisco commence l'enregistrement SRST. Le téléphone IP de Cisco s'inscrit au routeur SRST au port par défaut pour des communications protégées.

Configurez

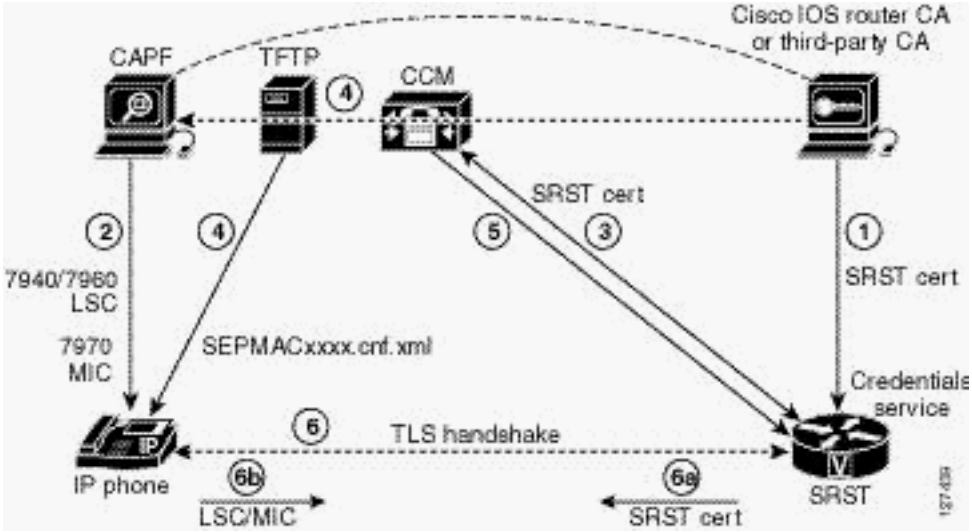
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Le routeur sécurisé SRST et les Téléphones IP de Cisco doivent demander l'authentification mutuelle pendant la prise de contact de TLS. La prise de contact de TLS se produit quand le téléphone s'inscrit au routeur SRST, l'un ou l'autre avant ou après que le lien WAN échoue. L'exemple de configuration n'inclut pas l'utilisation d'une tierce partie CA. Il assume l'utilisation du serveur de certificat de Cisco IOS de générer vos Certificats.

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant. Le diagramme montre le processus de l'authentification sécurisée et du cryptage SRST.



1. Le serveur CA, si c'est un routeur Cisco IOS CA ou une tierce partie CA, fournit un certificat de périphérique à la passerelle SRST, qui active le service de qualifications. Sur option, le

certificat peut auto-être généré par le routeur SRST avec un serveur du Cisco IOS CA.Le routeur CA est le point de confiance final pour la fonction de proxy d'autorité de certification (CAPF). Référez-vous au guide de Sécurité de Cisco CallManager pour plus d'informations sur CAPF.
2. Le CAPF est un processus où les périphériques pris en charge peuvent demander a localement - le certificat significatif (LSC). L'utilitaire CAPF génère une paire de clés et un certificat qui est spécifique pour CAPF, copie ce certificat sur tous les serveurs Cisco CallManagers dans la batterie, et fournit le LSC au téléphone IP de Cisco. Un LSC est exigé pour des Téléphones IP de Cisco qui n'ont pas un certificat installé par fabrication (MIC). Cisco 7970 est équipé d'une MIC et donc n'a pas besoin de passer par le processus CAPF.
3. Le Cisco CallManager demande le certificat SRST du serveur de qualifications, et le serveur de qualifications répond avec le certificat.
4. Pour chaque périphérique, le Cisco CallManager utilise le processus TFTP et insère le certificat dans le fichier de configuration SEPMACxxxx.cnf.xml du téléphone IP de Cisco.
5. Le Cisco CallManager fournit les fichiers de format PEM qui contiennent les informations de certificat de téléphone au routeur SRST. Les fichiers PEM sont fournis au routeur SRST manuellement. Quand le routeur SRST a les fichiers PEM, il peut authentifier le téléphone IP et valider l'émetteur du certificat de téléphone IP pendant la prise de contact de TLS.
6. La prise de contact de TLS se produit, des Certificats sont permutés, et l'authentification mutuelle et l'enregistrement se produit entre le téléphone IP de Cisco et le routeur SRST.Le routeur SRST envoie son certificat, et le téléphone valide le certificat au certificat qu'il a reçu du Cisco CallManager dans l'étape 4.Le téléphone IP de Cisco fournit au routeur SRST le LSC ou la MIC, et le routeur valide le LSC ou la MIC avec les fichiers de format PEM qu'elle a reçus dans l'étape 5.**Remarque:** Le support est chiffré automatiquement une fois que les Certificats de téléphone et de routeur sont permutés et la connexion de TLS est établie avec le routeur SRST.

Avant que vous configuriez

Cisco CallManager

Procédez comme suit :

1. Une fois que le service de qualifications fonctionne sur le routeur SRST, une référence SRST au Cisco CallManager doit être ajoutée, parce que le Cisco CallManager se connecte au routeur SRST pour son certificat de périphérique. Référez-vous à la section de *configuration de Survivable Remote Site Telephony du* guide de Cisco CallManager Administration, libérez 4.1(2) pour des informations complètes sur la façon ajouter SRST au Cisco CallManager.
2. Le retour SRST doit être configuré sur le Cisco CallManager. Afin de faire ceci affectez le Pool d'appareils à SRST. Référez-vous à la section de *configuration de Pool d'appareils du* guide de Cisco CallManager Administration, libérez 4.1(2) pour des informations complètes sur la façon ajouter un Pool d'appareils au Cisco CallManager.
3. La fonction de proxy d'autorité de certification (CAPF) doit être configurée sur le Cisco CallManager. Le processus CAPF permet à des périphériques pris en charge, tels que le Cisco CallManager, pour demander des Certificats LSC des Téléphones IP de Cisco. L'utilitaire CAPF génère une paire de clés et un certificat qui est spécifique pour CAPF, et l'utilitaire copie ce certificat sur tous les serveurs Cisco CallManagers dans la batterie.

Référez-vous à l'authentification et au cryptage de téléphone IP de Cisco pour le Cisco CallManager 4.0(1) pour des instructions complètes sur la façon dont configurer CAPF dans le Cisco CallManager.

Attentions de Sécurité

- La commande de **grant auto** permet des Certificats à émettre et doit être lancée quand vous définissez votre racine CA. Cependant, pour des raisons de sécurité, la commande de **grant auto** ne doit pas demeurer active et doit être désactivée après que des Certificats soient délivrés.
- Une pratique recommandée de Sécurité est de protéger le port de service de qualifications avec la Réglementation du plan de commande. La Réglementation du plan de commande protège la passerelle et met à jour des états de transfert de paquet et de protocole en dépit d'une charge de trafic intense. Référez-vous à la Réglementation du plan de commande pour plus d'informations sur des avions de contrôle. Un exemple de configuration semble également dans la configuration 2 sections de ce document.

Configurations

Ce document utilise les configurations suivantes :

- Le du Â d'âÂ de la configuration 1 configurent votre routeur selon cet exemple de **show running-config**.
- La pratique recommandée de Sécurité du A du Â d'âÂ de la configuration 2 est de protéger le port de service de qualifications avec la Réglementation du plan de commande. Si vous utilisez la Réglementation du plan de commande, configurez votre routeur selon cet exemple partiel de **show running-config**.

Configuration 1

```
Router#show running-config...!--- Define Cisco
CallManager.ccm-manager fallback-mgcpccm-manager mgcpccm-
manager music-on-holdccm-manager config server 10.1.1.13ccm-
manager config!--- Define root CA. !--- For SRST routers to
provide secure communications, there must be a !--- CA server
that issues the device certificate in the network. !--- The
CA server can be a third-party CA or one generated from a !--
- Cisco IOS certificate server. The Cisco IOS certificate
server !--- provides a certificate generation option to users
who do not !--- have a third-party CA in their network. The
Cisco IOS certificate !--- can run on the SRST router or on a
different Cisco IOS router.crypto pki server srstcaserver
database level complete database url nvram issuer-name
CN=srstcaserver! !--- The secure SRST router needs to define
a trustpoint. That is, !--- it must obtain a device
certificate from the CA server. The procedure !--- is called
certificate enrollment. Once enrolled, the secure SRST router
!--- can be recognized by Cisco CallManager as a secure SRST
router. There !--- are three options to enroll the secure
SRST router to a CA server: !--- autoenrollment, cut and
paste, and TFTP. When the CA server is a !--- Cisco IOS
certificate server, autoenrollment can be used. Otherwise,
manual !--- enrollment is required. Manual enrollment refers
to cut and paste or TFTP. !--- Issue the enrollment URL
command for autoenrollment and the !--- crypto pki
```

```
authenticate command in order to authenticate the SRST
router. !--- Issue the crypto ca enroll command in order to
obtain the SRST router !--- certificate from the CA.crypto
pki trustpoint srstca enrollment url http://10.1.1.22:80
revocation-check none!crypto pki trustpoint srstcaserver
revocation-check none rsakeypair srstcaserver!!--- Define the
CTL/7970/7960 trustpoint to authenticate secure SRST. !---
Repeat the enrollment procedure for each phone or PEM
file.crypto pki trustpoint 7970 enrollment terminal
revocation-check none!crypto pki trustpoint PEM enrollment
terminal revocation-check none!crypto pki trustpoint 7960
enrollment terminal revocation-check none!!--- This is the
SRST router device certificate.crypto pki certificate chain
srstca certificate 02 308201AD 30820116 A0030201 02020102
300D0609 2A864886 F70D0101 04050030 17311530 13060355
0403130C 73727374 63617365 72766572 301E170D 30343034
31323139 35323233 5A170D30 35303431 32313935 3232335A
30343132 300F0603 55040513 08443042 39453739 43301F06
092A8648 86F70D01 09021612 6A61736F 32363931 2E636973
636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2 056E0485
22896D36 6CA70C19 C98F9BAE AE9D1F9B D4BB7A67 F3251174
193BB1A3 12946123 E5C1CCD7 A23E6155 FA2ED743 3FB8B902
03010001 A330302E 300B0603 551D0F04 04030205 A0301F06
03551D23 04183016 8014F829 CE97AD60 18D05467 FC293963
C2470691 F9BD300D 06092A86 4886F70D 01010405 00038181
007EB48E CAE9E1B3 D1E7A185 D7F0D565 CB84B17B 1151BD78
B3E39763 59EC650E 49371F6D 99CBD267 EB8ADF9D 9E43A5F2
FB2B18A0 34AF6564 11239473 41478AFC A86E6DA1 AC518E0B
8657CEBB ED2BDE8E B586FE67 00C358D4 EFDD8D44 3F423141
C2D331D3 1EE43B6E 6CB29EE7 0B8C2752 C3AF4A66 BD007348
D013000A EA3C206D CF quit certificate ca 01 30820207 30820170
A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572
301E170D 30343034 31323139 34353136 5A170D30 37303431
32313934 3531365A 30173115 30130603 55040313 0C737273
74636173 65727665 7230819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA
2BB9DC8E 5B1BD332 1051C9FE 32A971B3 3C336635 74691954
98E765B1 059E24B6 32154E99 105CA989 9619993F CC72C525
7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499
5AD0849D CAA41417 DD866902 21E5DD03 C37D4B28 0FAB0203
010001A3 63306130 0F060355 1D130101 FF040530 030101FF
300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30
1F060355 1D230418 30168014 F829CE97 AD6018D0 5467FC29
3963C247 0691F9BD 300D0609 2A864886 F70D0101 04050003
8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283
08950414 8633A8B2 C98565A6 C09CA641 88661402 ACC424FD
36F23360 ABFF4C55 BB23C66A C80A3A57 5EE85FF8 C1B1A540
E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
DEDBAAD7 3780136E B112A6 quitcrypto pki certificate chain
srstcaserver certificate ca 01 30820207 30820170 A0030201
02020101 300D0609 2A864886 F70D0101 04050030 17311530
13060355 0403130C 73727374 63617365 72766572 301E170D
30343034 31323139 34353136 5A170D30 37303431 32313934
3531365A 30173115 30130603 55040313 0C737273 74636173
65727665 7230819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E
5B1BD332 1051C9FE 32A971B3 3C336635 74691954 98E765B1
059E24B6 32154E99 105CA989 9619993F CC72C525 7357EBAC
E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963 9D8FC222
```

```
EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D
CAA41417 DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3
63306130 0F060355 1D130101 FF040530 030101FF 300E0603
551D0F01 01FF0404 03020186 301D0603 551D0E04 160414F8
29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355
1D230418 30168014 F829CE97 AD6018D0 5467FC29 3963C247
0691F9BD 300D0609 2A864886 F70D0101 04050003 8181007A
F71B25F9 73D74552 25DFD03A D8D1338F 6792C805 47A81019
795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414
8633A8B2 C98565A6 C09CA641 88661402 ACC424FD 36F23360
ABFF4C55 BB23C66A C80A3A57 5EE85FF8 C1B1A540 E818CE6D
58131726 BB060974 4E1A2F4B E6195522 122457F3 DEDBAAD7
3780136E B112A6 quitcrypto pki certificate chain 7970
certificate ca 353FB24BD70F14A346C1F3A9AC725675 308203A8
30820290 A0030201 02021035 3FB24BD7 0F14A346 C1F3A9AC
72567530 0D06092A 864886F7 0D010105 0500302E 31163014
06035504 0A130D43 6973636F 20537973 74656D73 31143012
06035504 03130B43 41502D52 54502D30 3032301E 170D3033
31303130 32303138 34395A17 0D323331 30313032 30323733
375A302E 31163014 06035504 0A130D43 6973636F 20537973
74656D73 31143012 06035504 03130B43 41502D52 54502D30
30323082 0120300D 06092A86 4886F70D 01010105 00038201
0D003082 01080282 010100C4 266504AD 7DC3FD8D 65556FA6
308FAE95 B570263B 575ABD96 1CC8F394 5965D9D0 D8CE02B9
F808CCD6 B7CD8C46 24801878 57DC4440 A7301DDF E40FB1EF
136212EC C4F3B50F BCAFBB4B CD2E5826 34521B65 01555FE4
D4206776 03368357 83932638 D6FC953F 3A179E44 67255A73
45C69DEE FB4D221B 21D7A3AD 38184171 8FD8C271 42183E65
09461434 736C77CC F380EEBF 632C7B3F A5F92AA6 A8EF3490
8724A84F 4DAF7FD7 0928F585 764D3558 3C0FE9AF 1ED8763F
A299A802 970004AD 1912D265 7DE335B4 BCB6F789 DC68B9FA
C8FDF85E 8A28AD8F 0F4883C0 77112A47 141DBEE0 948FBE53
FE67B308 D40C8029 87BD790E CDAB9FD7 A190C1A2 A462C5F2
4A6E0B02 0103A381 C33081C0 300B0603 551D0F04 04030201
86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D
0E041604 1452922B E288EE2E 098A4E7E 702C56A5 9AB4D49B
96306F06 03551D1F 04683066 3064A062 A060862D 68747470
3A2F2F63 61702D72 74702D30 30322F43 65727445 6E726F6C
6C2F4341 502D5254 502D3030 322E6372 6C862F66 696C653A
2F2F5C5C 6361702D 7274702D 3030325C 43657274 456E726F
6C6C5C43 41502D52 54502D30 30322E63 726C3010 06092B06
01040182 37150104 03020100 300D0609 2A864886 F70D0101
05050003 82010100 56838CEF C4DA3AD1 EA8FBB15 2FFE6EE5
50A1972B D4D7AF1F D298892C D5A2A76B C3462866 13E0E55D
DC0C4B92 5AA94B6E 69277F9B FC73C697 11266E19 451C0FAB
A55E6A28 901A48C5 B9911EE6 348A8920 0AEDE1E0 B6EA781C
FFD97CA4 B03C0E34 0E5B0649 8B0A34C9 B73A654E 09050C1F
4DA53E44 BF78443D B08C3A41 2EEEB873 78CB8089 34F9D16E
91512F0D 3A8674AD 0991ED1A 92841E76 36D7740E CB787F11
685B9E9D 0C67E85D AF6D05BA 3488E86D 7E2F7F65 6918DE0F
BD3C7F67 D8A33F70 9C4A596E D9F62B3B 1EDEE854 D5882AD4
3D71F72B 8FAB7F3C 0B5F0759 D9828F83 954D7BB1 57A638EC
7D72BFF1 8933C16F 760BCA94 4C5B1931 67947A4F 89A1BDB5
quitcrypto pki certificate chain PEM certificate ca
7612F960153D6F9F4E42202032B72356 308203A8 30820290 A0030201
02021076 12F96015 3D6F9F4E 42202032 B7235630 0D06092A
864886F7 0D010105 0500302E 31163014 06035504 0A130D43
6973636F 20537973 74656D73 31143012 06035504 03130B43
41502D52 54502D30 3031301E 170D3033 30323036 32333237
31335A17 0D323330 32303632 33333633 345A302E 31163014
06035504 0A130D43 6973636F 20537973 74656D73 31143012
06035504 03130B43 41502D52 54502D30 30313082 0120300D
06092A86 4886F70D 01010105 00038201 0D003082 01080282
010100AC 55BBED18 DE9B8709 FFBC8F2D 509AB83A 21C1967F
```

```
DEA7F4B0 969694B7 80CC196A 463DA516 54A28F47 5D903B5F
104A3D54 A981389B 2FC7AC49 956262B8 1C143038 5345BB2E
273FA7A6 46860573 CE5C998D 55DE78AA 5A5CFE14 037D695B
AC816409 C6211F0B 3BBF09CF B0BBB2D4 AC362F67 0FD145F1
620852B3 1F07E2F1 AA74F150 367632ED A289E374 AF0C5B78
CE7DFB9F C8EBBE54 6ECF4C77 99D6DC04 47476C0F 36E58A3B
6BCB24D7 6B6C84C2 7F61D326 BE7CB4A6 60CD6579 9E1E3A84
8153B750 5527E865 423BE2B5 CB575453 5AA96093 58B6A2E4
AA3EF081 C7068EC1 DD1EBDDA 53E6F0D6 E2E0486B 109F1316
78C696A3 CFBA84CC 7094034F C1EB9F81 931ACB02 0103A381
C33081C0 300B0603 551D0F04 04030201 86300F06 03551D13
0101FF04 05300301 01FF301D 0603551D 0E041604 14E917B1
82C71FCF ACA91B6E F4A9269C 70AE05A0 9A306F06 03551D1F
04683066 3064A062 A060862D 68747470 3A2F2F63 61702D72
74702D30 30312F43 65727445 6E726F6C 6C2F4341 502D5254
502D3030 312E6372 6C862F66 696C653A 2F2F5C5C 6361702D
7274702D 3030315C 43657274 456E726F 6C6C5C43 41502D52
54502D30 30312E63 726C3010 06092B06 01040182 37150104
03020100 300D0609 2A864886 F70D0101 05050003 82010100
AB64FDEB F60C32DC 360F0E10 5FE175FA 0D574AB5 02ACDCA3
C7BBED15 A4431F20 7E9286F0 770929A2 17E4CDF4 F2629244
2F3575AF E90C468C AE67BA08 AAA71C12 BA0C0E79 E6780A5C
F814466C 326A4B56 73938380 73A11AED F9B9DE74 1195C48F
99454B8C 30732980 CD6E7123 8B3A6D68 80B97E00 7F4BD4BA
0B5AB462 94D9167E 6D8D48F2 597CDE61 25CFADCC 5BD141FB
210275A2 0A4E3400 1428BA0F 69953BB5 50D21F78 43E3E563
98BCB2B1 A2D4864B 0616BACD A61CD9AE C5558A52 B5EEAA6A
08F96528 B1804B87 D26E4AEE AB7AFFE9 2FD2A574 BAFE0028
96304A8B 13FB656D 8FC60094 D5A53D71 444B3CEF 79343385
3778C193 74A2A6CE DC56275C A20A303D quitcrypto pki
certificate chain 7960 certificate ca F301 308201F7 30820160
A0030201 020202F3 01300D06 092A8648 86F70D01 01050500
3041310B 30090603 55040613 02555331 1A301806 0355040A
13114369 73636F20 53797374 656D7320 496E6331 16301406
03550403 130D4341 50462D33 35453038 33333230 1E170D30
34303430 39323035 3530325A 170D3139 30343036 32303535
30315A30 41310B30 09060355 04061302 5553311A 30180603
55040A13 11436973 636F2053 79737465 6D732049 6E633116
30140603 55040313 0D434150 462D3335 45303833 33323081
9F300D06 092A8648 86F70D01 01010500 03818D00 30818902
818100C8 BD9B6035 366B44E8 0F693A47 250FF865 D76C35F7
89B1C4FD 1D122CE0 F5E5CDFF A4A87EFF 41AD936F E5C93163
3E55D11A AF82A5F6 D563E21C EB89EBFA F5271423 C3E875DC
E0E07967 6E1AAB4F D3823E12 53547480 23BA1A09 295179B6
85A0E83A 77DD0633 B9710A88 0890CD4D DB55ADD0 964369BA
489043BB B667E60F 93954B02 03010001 300D0609 2A864886
F70D0101 05050003 81810056 60FD3AB3 6F98D2AD 40C309E2
C05B841C 5189271F 01D864E8 98BCE665 2AFBCC8C 54007A84
8F772C67 E3047A6C C62F6508 B36A6174 B68C1D78 C2228FEA
A89ECEFB CC8BA9FC 0F30E151 431670F9 918514D9 868D1235
18137F1E 50DFD32E 1DC29CB7 95EF4096 421AF22F 5C1D5804
B83F8E8E 95B04F45 86563BFE DF976C5B FB490A quit!!no crypto
isakmp enable!!--- Enable IPsec.crypto isakmp policy 1
authentication pre-share lifetime 28800crypto isakmp key
cisco123 address 10.1.1.13!--- The crypto key must match the
key configured on Cisco CallManager. ! !--- The crypto IPSec
configuration must match your Cisco CallManager !---
configuration.crypto ipsec transform-set rtpset esp-des esp-
md5-hmac!!crypto map rtp 1 ipsec-isakmp set peer 10.1.1.13
set transform-set rtpset match address 116!!interface
FastEthernet0/0 ip address 10.1.1.22 255.255.255.0 duplex
auto speed auto crypto map rtp!interface FastEthernet0/1 no
ip address shutdown duplex auto speed auto!ip classless!ip
http serverno ip http secure-server!!!--- Define the traffic
```

```
to be encrypted by IPsec.access-list 116 permit ip host
10.1.1.22 host 10.1.1.13!!control-plane!!call application
alternate DEFAULT!!voice-port 1/0/0!voice-port 1/0/1!voice-
port 1/0/2!voice-port 1/0/3!voice-port 1/1/0 timing
hookflash-out 50!voice-port 1/1/1!voice-port 1/1/2!voice-port
1/1/3!!--- Enable the MGCP voice protocol.mgcpmgcp call-agent
10.1.1.13 2427 service-type mgcp version 0.1mgcp dtmf-relay
voip codec all mode out-of-bandmgcp rtp unreachable timeout
1000 action notifymgcp package-capability rtp-packagemgcp
package-capability sst-packageno mgcp package-capability fxr-
packageno mgcp timer receive-rtcpmgcp sdp simplemgcp fax t38
inhibitmgcp rtp payload-type g726r16 static!mgcp profile
default!!dial-peer voice 81235 pots application mgcpapp
destination-pattern 81235 port 1/1/0 forward-digits all!dial-
peer voice 81234 pots application mgcpapp destination-pattern
81234 port 1/0/0!dial-peer voice 999100 pots application
mgcpapp port 1/0/0!dial-peer voice 999110 pots application
mgcpapp port 1/1/0!!!--- Enable the credentials service on
the gateway. !--- Cisco CallManager takes the certificate
retrieved from the secure SRST !--- device certificate and
places it in the configuration file of the !--- Cisco IP
phone. Activate credentials service on all SRST routers. !---
Enable the SRST router to receive messages from Cisco
CallManager. The !--- IP address is the preexisting router IP
address, typically one of the !--- addresses of the Ethernet
port of the router. The default port number is
2445.credentials ip source-address 10.1.1.22 port 2445!---
Specify the name of the trustpoint that is to be associated
with the SRST !--- router certificate. The trustpoint name
must be the same as the one already !--- declared. trustpoint
srstca!!!--- Enable SRST mode on the SRST router to support
Cisco IP phone functions.call-manager-fallback secondary-
dialtone 9 transfer-system full-consult ip source-address
10.1.1.22 port 2000 max-ephones 15 max-dn 30 transfer-pattern
........
```

Configuration 2

```
!--- Allow trusted host traffic.access-list 140 deny tcp host
10.1.1.11 any eq 2445!--- Rate-limit all other
traffic.access-list 140 permit tcp any any eq 2445access-list
140 deny ip any any!--- Define class-map sccp-class.class-map
match-all sccp-class match access-group 140policy-map
control-plane-policy class sccp-class police 8000 1500 1500
conform-action drop exceed-action drop!--- Define aggregate
control plane service for the active Route Processor.control-
plane service-policy input control-plane-policy
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Vérifiez les configurations de créance

Afin de vérifier les configurations de créance sur le routeur SRST qui sont fournies au Cisco CallManager pour l'usage pendant le retour sécurisé SRST, émettez la commande de **qualifications d'exposition**.

```
Router#show credentialsCredentials IP: 10.1.1.22Credentials PORT: 2445Trustpoint: srstca
```

Vérifiez l'inscription de certificat

Si vous utilisiez le Cisco IOS délivre un certificat le serveur en tant que votre CA, émet la **commande show running-config** afin de vérifier l'inscription de certificat ou la commande de **show crypto pki server** afin de vérifier l'état du serveur CA.

1. Émettez la **commande show running-config** afin de vérifier la création Certificats du serveur (01) et du périphérique CA des 02) (. Cet exemple affiche les Certificats inscrits.
```
! SRST router device certificate.crypto pki certificate chain srstca certificate 02  308201AD 30820116 A0030201
02020102 300D0609 2A864886 F70D0101 04050030  17311530 13060355 0403130C 73727374 63617365 72766572
301E170D 30343034  31323139 35323233 5A170D30 35303431 32313935 3232335A 30343132 300F0603
55040513 08443042 39453739 43301F06 092A8648 86F70D01 09021612 6A61736F  32363931 2E636973 636F2E63
6F6D305C 300D0609 2A864886 F70D0101 01050003  4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2 056E0485
22896D36 6CA70C19  C98F9BAE AE9D1F9B D4BB7A67 F3251174 193BB1A3 12946123 E5C1CCD7 A23E6155
FA2ED743 3FB8B902 03010001 A330302E 300B0603 551D0F04 04030205 A0301F06  03551D23 04183016 8014F829
CE97AD60 18D05467 FC293963 C2470691 F9BD300D  06092A86 4886F70D 01010405 00038181 007EB48E CAE9E1B3
D1E7A185 D7F0D565  CB84B17B 1151BD78 B3E39763 59EC650E 49371F6D 99CBD267 EB8ADF9D 9E43A5F2
FB2B18A0 34AF6564 11239473 41478AFC A86E6DA1 AC518E0B 8657CEBB ED2BDE8E  B586FE67 00C358D4 EFDD8D44
3F423141 C2D331D3 1EE43B6E 6CB29EE7 0B8C2752  C3AF4A66 BD007348 D013000A EA3C206D CF  quit
certificate ca 01  30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034  31323139 34353136 5A170D30
37303431 32313934 3531365A 30173115 30130603  55040313 0C737273 74636173 65727665 7230819F 300D0609
2A864886 F70D0101  01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989  9619993F CC72C525 7357EBAC
E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963  9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499
5AD0849D CAA41417  DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04  160414F8 29CE97AD 6018D054
67FC2939 63C24706 91F9BD30 1F060355 1D230418  30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD
300D0609 2A864886  F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2  C98565A6 C09CA641 88661402
ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57  5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B
E6195522 122457F3  DEDBAAD7 3780136E B112A6  quit
```
2. Émettez la commande de **show crypto pki server** afin de vérifier l'état du serveur CA après une procédure de démarrage.
```
Router#show crypto pki serverCertificate Server srstcaserver:Status: enabledServer's configuration is locked (enter "shut" to unlock it)Issuer name: CN=srstcaserverCA cert fingerprint: AC9919F5 CAFE0560 92B3478A CFF5EC00Granting mode is: autoLast certificate issued serial number: 0x2CA certificate expiration timer: 13:46:57 PST Dec 1 2007CRL NextUpdate timer: 14:54:57 PST Jan 19 2005Current storage dir: nvramDatabase Level: Complete - all issued certs written as <serialnum>.cer
```

Vérifiez l'état du téléphone et les enregistrements

Afin de vérifier ou dépanner l'état et l'enregistrement de téléphone IP, terminez-vous ces étapes dans le mode d'exécution privilégié.

1. Émettez la commande d'**ephone d'exposition** afin d'afficher des Téléphones IP d'enregistré Cisco et leurs capacités. Cette commande affiche également l'état d'authentification et de cryptage une fois utilisée pour SRST sécurisé. Dans cet exemple, l'état d'authentification et de cryptage est en activité avec une connexion de TLS.
```
Router#show ephoneephone-1 Mac:1000.1111.0002 TCP socket:[5] activeLine:0 REGISTERED in SCCP ver 5 + Authentication + Encryption with TLS connection mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 IP:10.1.1.40 32626 7970 keepalive 390 max_line 8 button 1: dn 14 number 2002 CM Fallback CH1 IDLEephone-2 Mac:1000.1111.000B TCP socket:[12] activeLine:0 REGISTERED in SCCP ver 5 + Authentication + Encryption with TLS connection mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 IP:10.1.1.40 32718 7970 keepalive 390 max_line 8 button 1: dn 21 number 2011 CM Fallback CH1 IDLEephone-3 Mac:1000.1111.000A TCP socket:[16] activeLine:0 REGISTERED
```

```
in SCCP ver 5 + Authentication + Encryption with TLS connection mediaActive:0 offhook:0 ringing:0
reset:0 reset_sent:0 paging 0 debug:0 IP:10.1.1.40 32862 7970 keepalive 390 max_line 8 button 1: dn
2 number 2010 CM Fallback CH1 IDLE
```

2. Émettez la commande d'**offhook d'ephone d'exposition** afin d'afficher l'état et la qualité de téléphone IP de Cisco pour tous les téléphones qui sont outre de crochet. Dans cet exemple, l'état d'authentification et de cryptage est en activité avec une connexion de TLS, et il y a un appel sécurisé actif.`Router#`**`show ephone offhook`**`ephone-1 Mac:1000.1111.0002 TCP socket:[5] activeLine:1 REGISTERED in SCCP ver 5 + Authentication + Encryption with TLS connection mediaActive:1 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 :0 IP:10.1.1.40 32626 7970 keepalive 391 max_line 8 button 1: dn 14 number 2002 CM Fallback CH1 CONNECTED Active Secure Call on DN 14 chan 1 :2002 10.1.1.40 29632 to 10.1.1.40 25616via 10.1.1.40 G711Ulaw64k 160 bytes no vad Tx Pkts 295 bytes 49468 Rx Pkts 277 bytes 46531 Lost 0 Jitter 0 Latency 0 callingDn 22 calledDn -1ephone-2 Mac:1000.1111.000B TCP socket:[12] activeLine:1 REGISTERED in SCCP ver 5 + Authentication + Encryption with TLS connection mediaActive:1 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 IP:10.1.1.40 32718 7970 keepalive 391 max_line 8 button 1: dn 21 number 2011 CM Fallback CH1 CONNECTED Active Secure Call on DN 21 chan 1 :2011 10.1.1.40 16382 to 10.1.1.40 16382 via 10.1.1.40 G711Ulaw64k 160 bytes no vad Tx Pkts 295 bytes 49468 Rx Pkts 277 bytes 46531 Lost 0 Jitter 0 Latency 0 callingDn -1 calledDn 11`
3. Émettez la commande d'**état de show voice call** afin d'afficher l'état d'appel pour tous les ports vocaux sur le routeur de Cisco SRST. Cette commande s'applique pas applicable pour des appels entre deux homologues de numérotation POTS.`Router#`**`show voice call status`**` CallID CID ccVdb Port DSP/Ch Called # Codec Dial-peers 0x1164 2BFE 0x8619A460 50/0/35.0 2014 g711ulaw 20035/20027 0x1165 2BFE 0x86144B78 50/0/27.0 *2014 g711ulaw 20027/20035 0x1166 2C01 0x861043D8 50/0/21.0 2012 g711ulaw 20021/20011 0x1168 2C01 0x860984C4 50/0/11.0 *2012 g711ulaw 20011/20021 0x1167 2C04 0x8610EC7C 50/0/22.0 2002 g711ulaw 20022/20014 0x1169 2C04 0x860B8894 50/0/14.0 *2002 g711ulaw 20014/20022 0x116A 2C07 0x860A374C 50/0/12.0 2010 g711ulaw 20012/20002 0x116B 2C07 0x86039700 50/0/2.0 *2010 g711ulaw 20002/20012 0x116C 2C0A 0x86119520 50/0/23.0 2034 g711ulaw 20023/20020 0x116D 2C0A 0x860F9150 50/0/20.0 *2034 g711ulaw 20020/20023 0x116E 2C0D 0x8608DC20 50/0/10.0 2022 g711ulaw 20010/20008 0x116F 2C0D 0x86078AD8 50/0/8.0 *2022 g711ulaw 20008/20010 0x1170 2C10 0x861398F0 50/0/26.0 2016 g711ulaw 20026/20028 0x1171 2C10 0x8614F41C 50/0/28.0 *2016 g711ulaw 20028/20026 0x1172 2C13 0x86159CC0 50/0/29.0 2018 g711ulaw 20029/20004 0x1173 2C13 0x8604E848 50/0/4.0 *2018 g711ulaw 20004/20029 0x1174 2C16 0x8612F04C 50/0/25.0 2026 g711ulaw 20025/20030 0x1175 2C16 0x86164F48 50/0/30.0 *2026 g711ulaw 20030/20025 0x1176 2C19 0x860D8C64 50/0/17.0 2032 g711ulaw 20017/20018 0x1177 2C19 0x860E4008 50/0/18.0 *2032 g711ulaw 20018/20017 0x1178 2C1C 0x860CE3C0 50/0/16.0 2004 g711ulaw 20016/20019 0x1179 2C1C 0x860EE8AC 50/0/19.0 *2004 g711ulaw 20019/20016 0x117A 2C1F 0x86043FA4 50/0/3.0 2008 g711ulaw 20003/20024 0x117B 2C1F 0x861247A8 50/0/24.0 *2008 g711ulaw 20024/20003 0x117C 2C22 0x8608337C 50/0/9.0 2020 g711ulaw 20009/20031 0x117D 2C22 0x8616F7EC 50/0/31.0 *2020 g711ulaw 20031/20009 0x117E 2C25 0x86063990 50/0/6.0 2006 g711ulaw 20006/20001 0x117F 2C25 0x85C6BE6C 50/0/1.0 *2006 g711ulaw 20001/20006 0x1180 2C28 0x860ADFF0 50/0/13.0 2029 g711ulaw 20013/20034 0x1181 2C28 0x8618FBBC 50/0/34.0 *2029 g711ulaw 20034/20013 0x1182 2C2B 0x860C3B1C 50/0/15.0 2036 g711ulaw 20015/20005 0x1183 2C2B 0x860590EC 50/0/5.0 *2036 g711ulaw 20005/20015 0x1184 2C2E 0x8617A090 50/0/32.0 2024 g711ulaw 20032/20007 0x1185 2C2E 0x8606E234 50/0/7.0 *2024 g711ulaw 20007/20032 0x1186 2C31 0x861A56E8 50/0/36.0 2030 g711ulaw 20036/20033 0x1187 2C31 0x86185318 50/0/33.0 *2030 g711ulaw 20033/20036 18 active calls found`

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Pour des informations supplémentaires sur la façon dépanner, voyez les informations relatives