Gérer les certificats en bloc entre les clusters CUCM pour la migration de téléphone

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Procédure de gestion de certificats en bloc
  - Exporter les certificats de cluster de destination
  - Exporter les certificats de cluster source
  - Consolidation des fichiers PKCS12 source et de destination
  - Importer des certificats dans les clusters source et de destination
  - Configuration des téléphones du cluster source avec les informations du serveur TFTP du cluster de destination
  - Réinitialiser les téléphones du cluster source pour obtenir le fichier ITL/CTL du cluster de destination afin de terminer le processus de migration
- Vérifier
- Dépannage
- Vidéo de configuration
- Informations connexes

Introduction

Ce document décrit comment gérer la certification groupée entre les clusters Cisco Unified Communications Manager (CUCM) pour la migration de téléphone.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :
· Serveur SFTP (Secure File Transfer Protocol)
· Certificats CUCM

Composants utilisés

Les informations contenues dans ce document sont basées sur CUCM 10.X.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Remarque : Cette procédure est également décrite dans la section Gérer les certificats en bloc du Guide d'administration de CUCM version 12.5(1)

La gestion de certificats en masse permet de partager un ensemble de certificats entre des clusters CUCM. Cette étape est obligatoire pour les fonctions système des clusters individuels qui nécessitent l'établissement d'une relation de confiance entre eux, par exemple pour Extension Mobility Cross Cluster (EMCC), ainsi que pour la migration de téléphones entre les clusters.

Dans le cadre de cette procédure, un fichier de normes de cryptographie à clé publique #12 (PKCS12) contenant des certificats de tous les noeuds d'un cluster est créé. Chaque cluster doit exporter ses certificats vers le même répertoire SFTP sur le même serveur SFTP. Les configurations de gestion de certificats en bloc doivent être effectuées manuellement sur l'éditeur CUCM des clusters source et de destination. Les clusters source et de destination doivent être opérationnels afin que les téléphones à migrer disposent d'une connectivité à ces deux clusters. Les téléphones du cluster source sont migrés vers le cluster de destination.

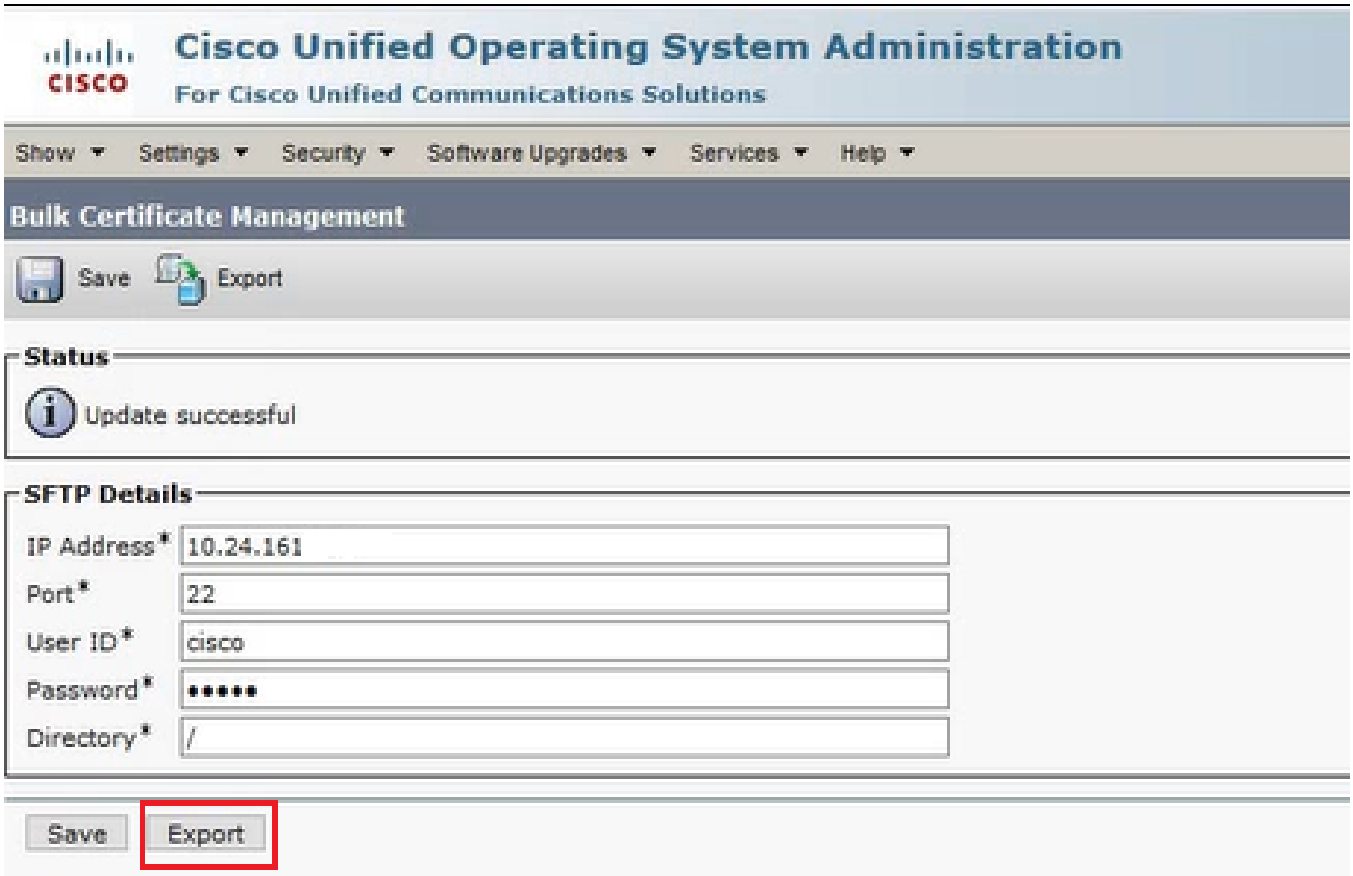
Procédure de gestion de certificats en bloc

Exporter les certificats de cluster de destination

Étape 1 : configuration du serveur SFTP pour la gestion de certificats en bloc sur l’éditeur CUCM du cluster de destination

Dans cet exemple, la version du CUCM du cluster de destination est 11.5.1.

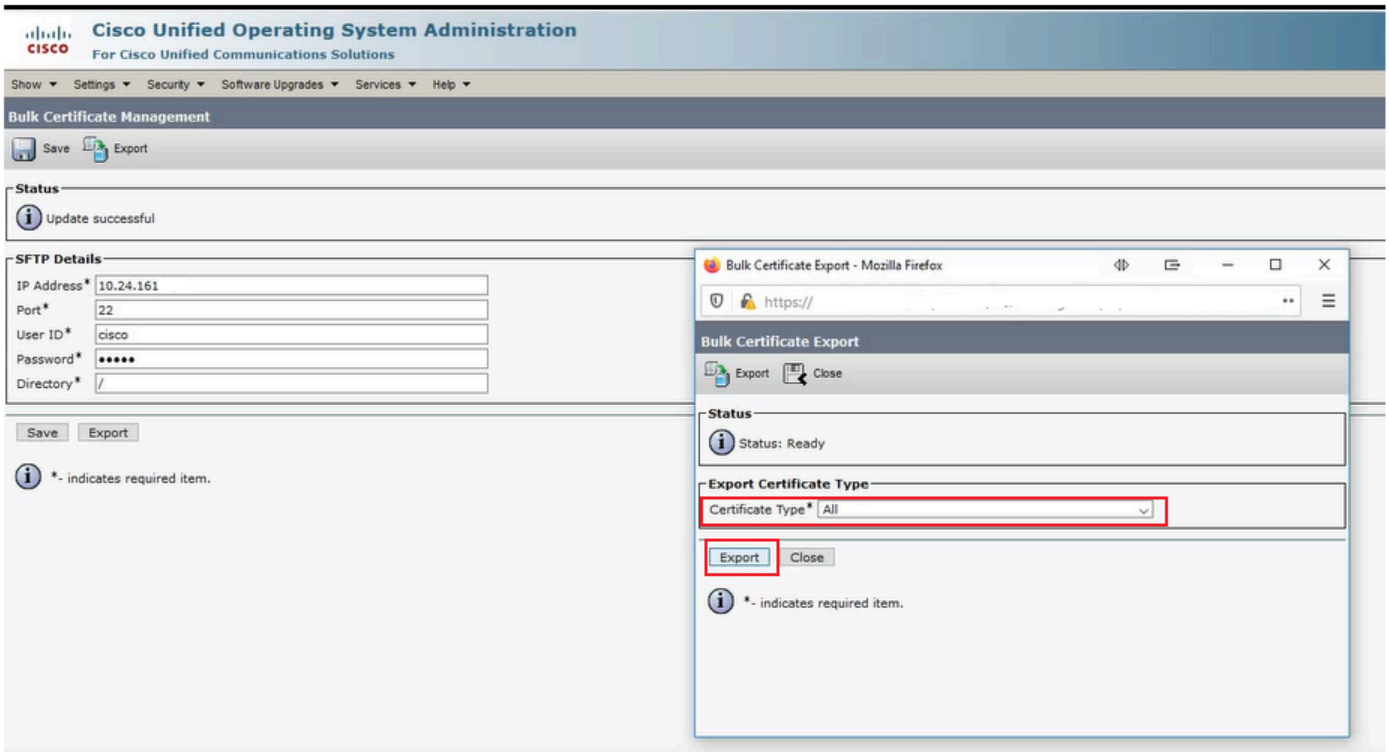
Accédez à Cisco Unified OS Administration > Security > Bulk Certificate Management. Entrez les détails du serveur SFTP et cliquez sur Export (Exporter).



Saisissez les détails du serveur SFTP et cliquez sur Exporter.

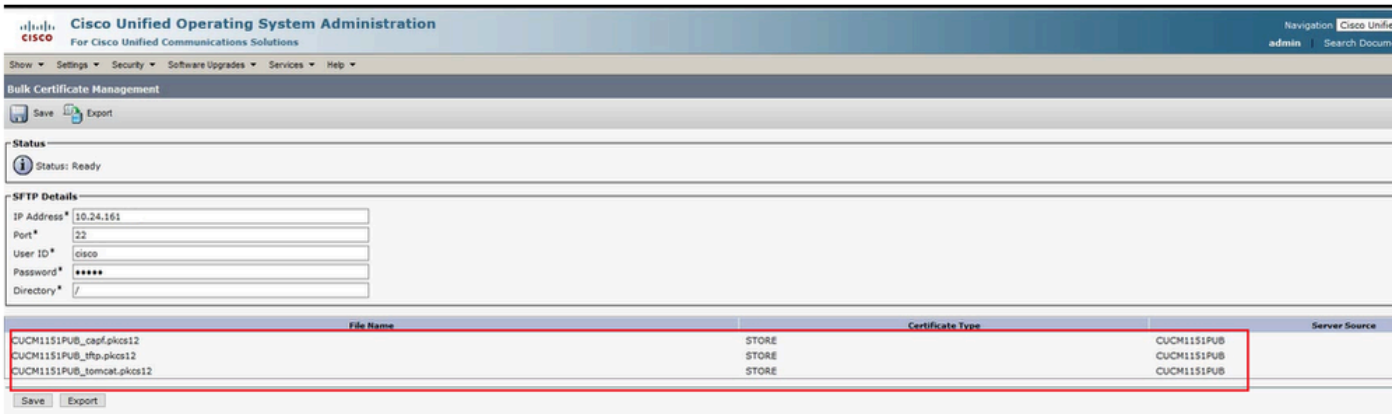
Étape 2. Exportez tous les certificats de tous les noeuds du cluster de destination vers le serveur SFTP.

Dans la fenêtre contextuelle Bulk Certificate Export, sélectionnez All pour Certificate Type, puis cliquez sur Export.



Sélectionnez Tout pour le type de certificat, puis cliquez sur Exporter

Fermez la fenêtre et mettez à jour Bulk Certificate Management avec les fichiers PKCS12 créés pour chacun des noeuds dans le cluster de destination, la page Web s'actualise avec ces informations, comme indiqué dans l'image.



Mises à jour de gestion de certificats en masse avec les fichiers PKCS12

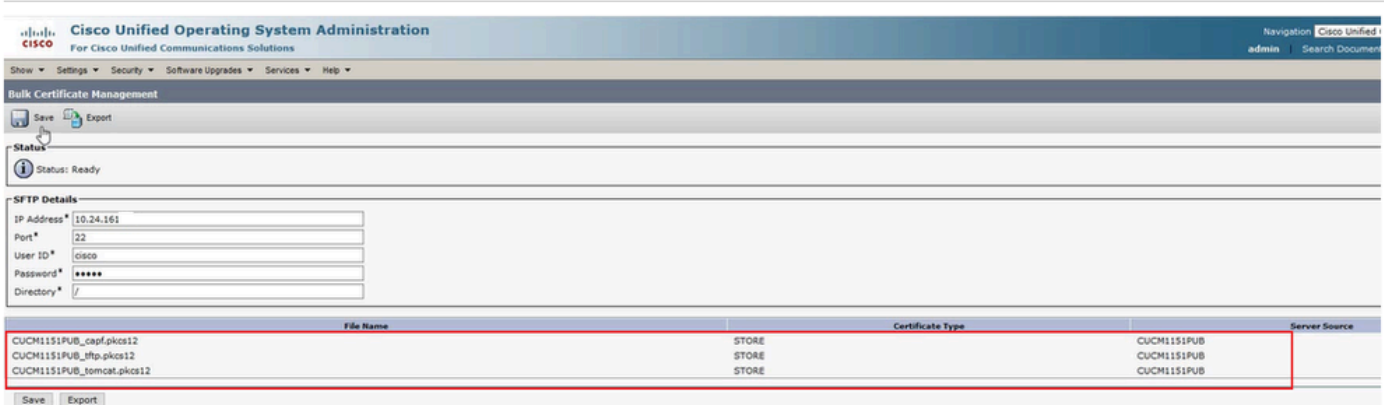
Exporter les certificats de cluster source

Étape 1 : configuration du serveur SFTP pour la gestion de certificats en bloc sur l'éditeur CUCM du cluster source

Dans cet exemple, la version CUCM du cluster source est 10.5.2.

Accédez à Cisco Unified OS Administration > Security > Bulk Certificate Management, entrez les détails du serveur SFTP et cliquez sur Export.

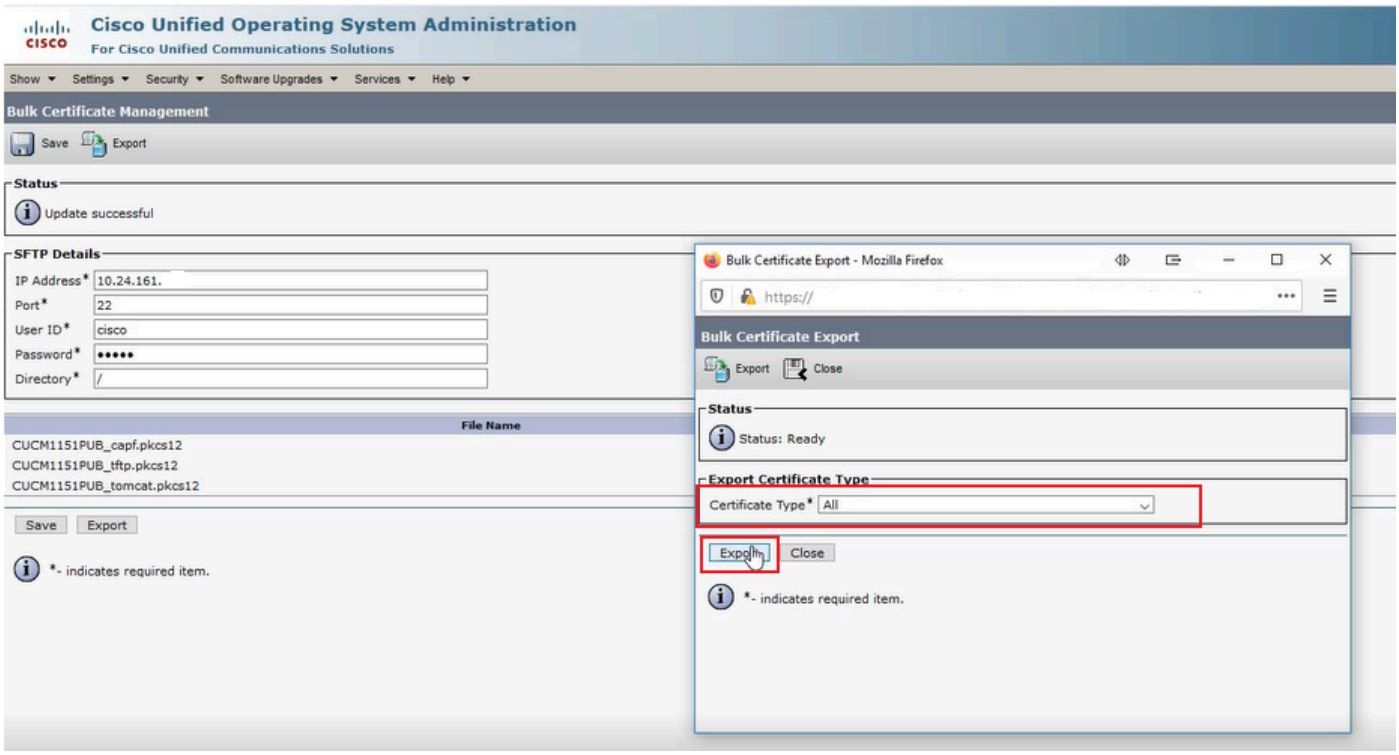
Remarque : Les fichiers PKCS12 exportés du cluster de destination vers le serveur SFTP s'affichent sur la page Web CUCM publisher Bulk Certificate Management du cluster source lorsque vous y accédez.



Saisissez les détails du serveur SFTP et cliquez sur Exporter

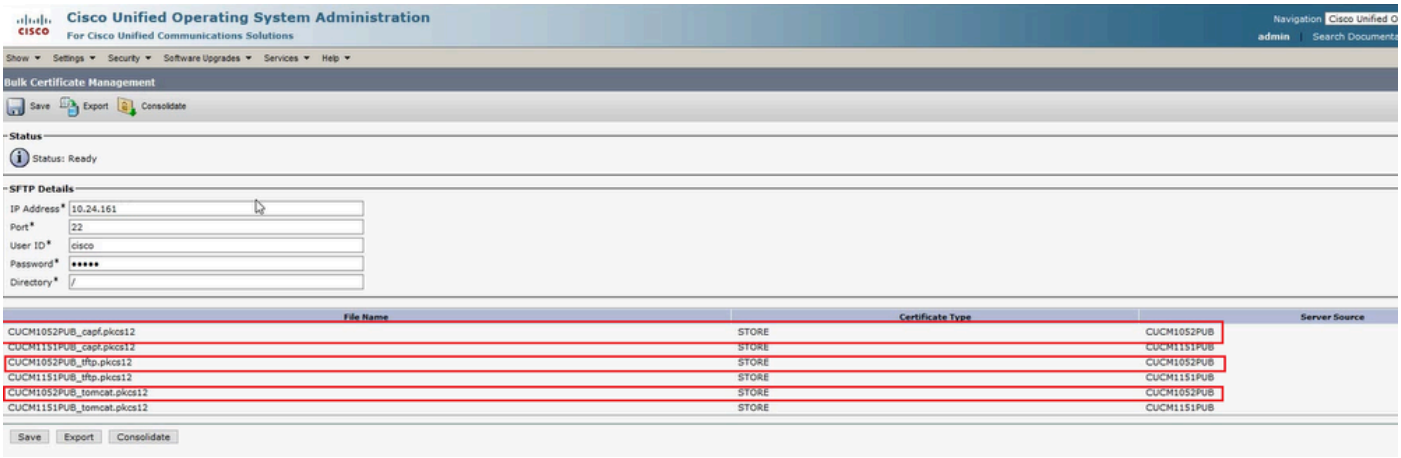
Étape 2. Exportez tous les certificats de tous les noeuds du cluster source vers le serveur SFTP.

Dans la fenêtre contextuelle Bulk Certificate Export, sélectionnez All pour Certificate Type, puis cliquez sur Export :



Exporter tout le type de certificat

Cliquez sur Close pour fermer cette fenêtre. La gestion de certificats en masse est mise à jour avec les fichiers PKCS12 créés pour chacun des noeuds du cluster source. La page Web est actualisée avec ces informations. La page Web de gestion des certificats en masse du cluster source affiche désormais les fichiers PKCS12 source et de destination exportés vers SFTP.



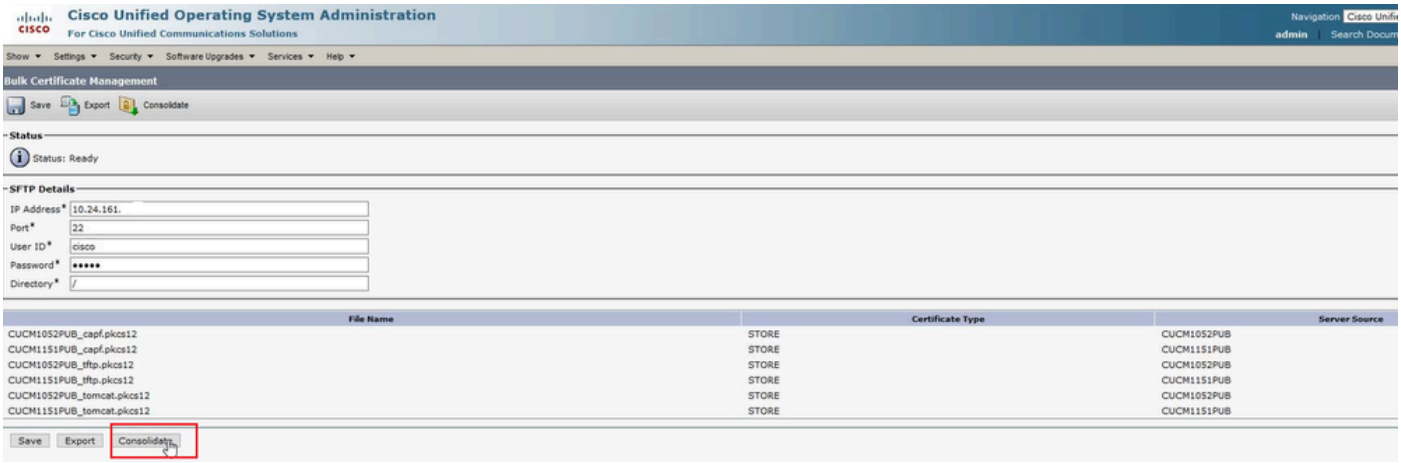
Fichiers PKCS12 exportés vers SFTP.

Consolidation des fichiers PKCS12 source et de destination

Remarque : Alors que l'exportation de gestion de certificats en bloc est effectuée sur les clusters source et de destination, la consolidation est effectuée par l'éditeur CUCM sur un

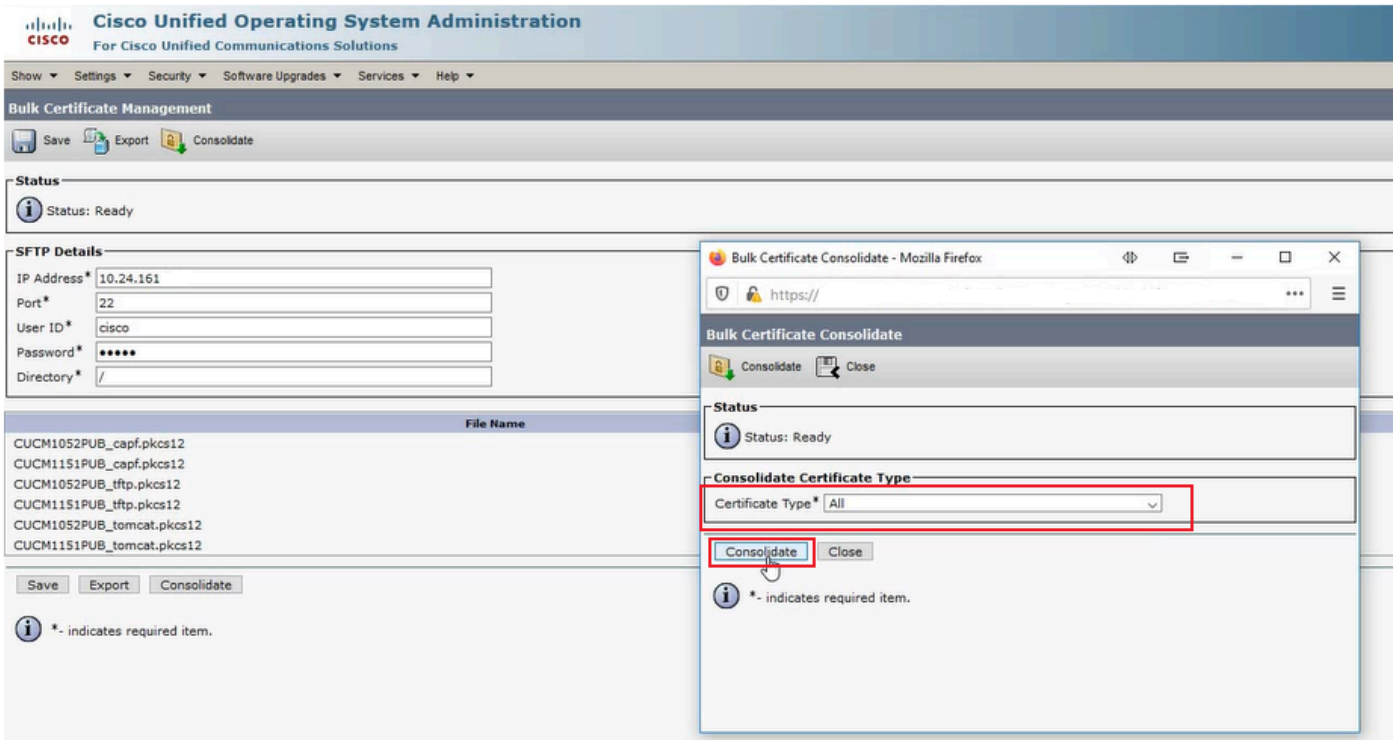
seul des clusters.

Étape 1. Retournez à la page Bulk Certificate Management de l'éditeur CUCM de la grappe source et cliquez sur Consolidate :



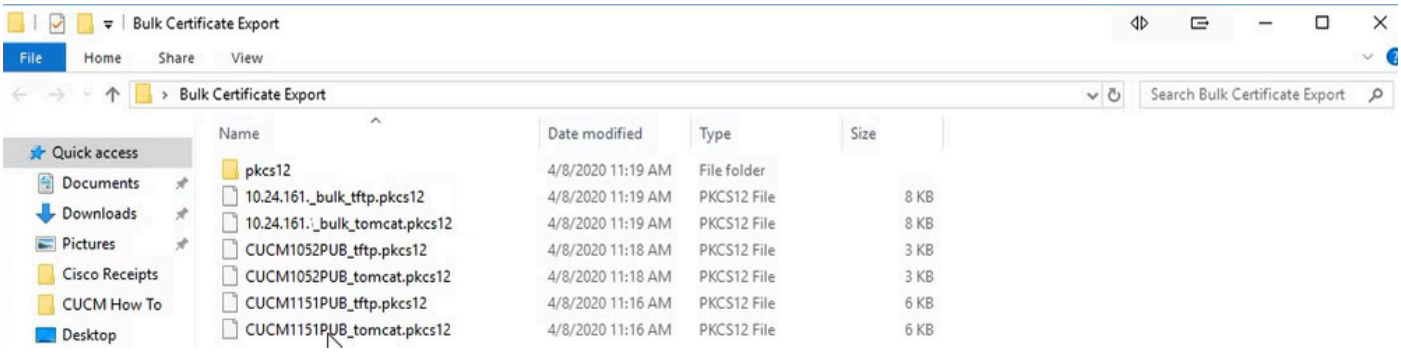
Cliquez sur Consolider

Dans la fenêtre contextuelle Consolidation de certificats en bloc, sélectionnez Tous pour Type de certificat, puis cliquez sur Consolider. Cliquez sur Fermer pour fermer cette fenêtre.

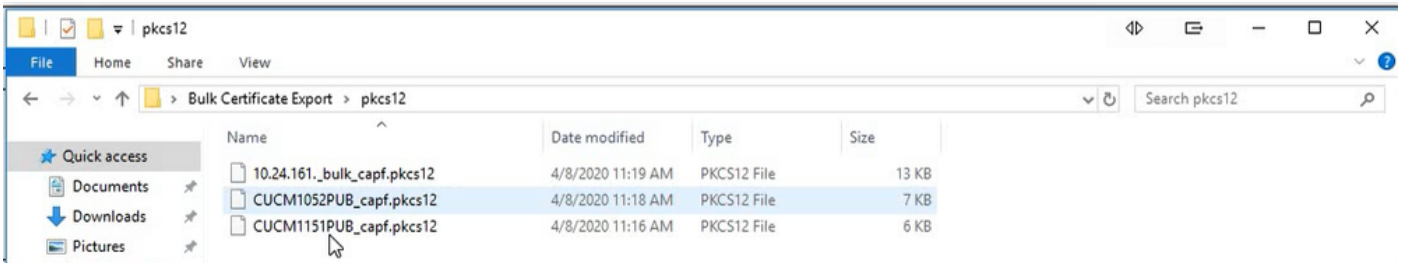


Consolider tous les types de certificats

À tout moment, vous pouvez vérifier dans le répertoire SFTP les fichiers PKCS 12 contenus dans les clusters source et de destination. Le contenu du répertoire SFTP après l'exportation de tous les certificats, à partir des clusters source et de destination, est terminé. Ceci est montré dans les images suivantes.



Contenu du répertoire SFTP après l'exportation de tous les certificats

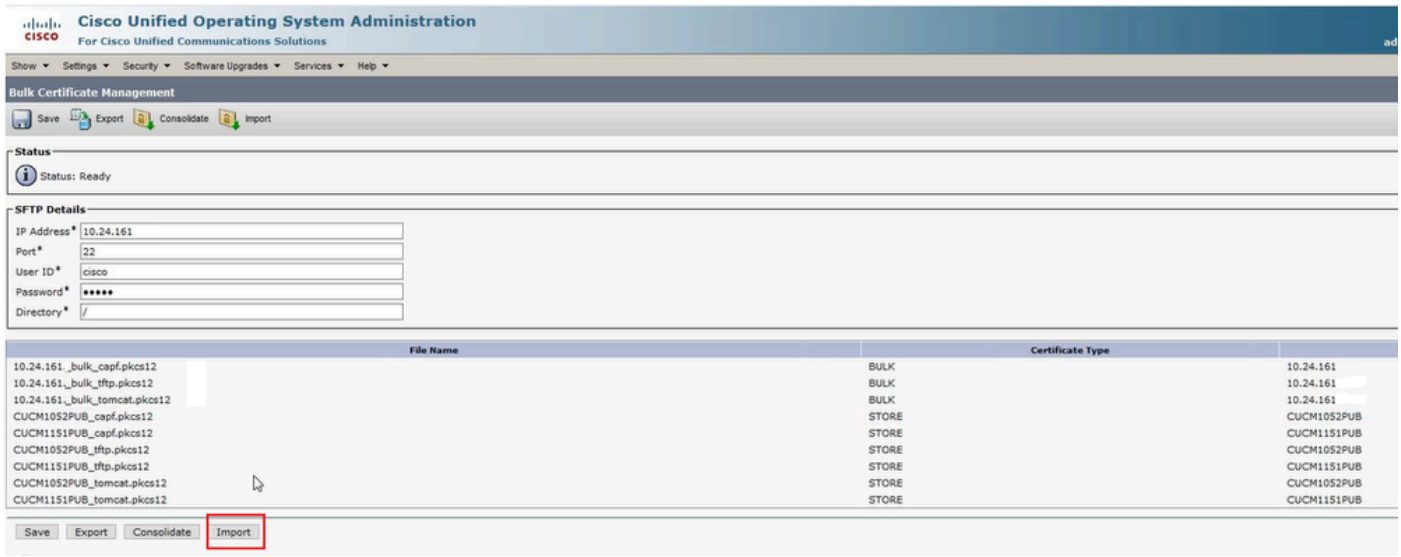


Contenu du répertoire SFTP

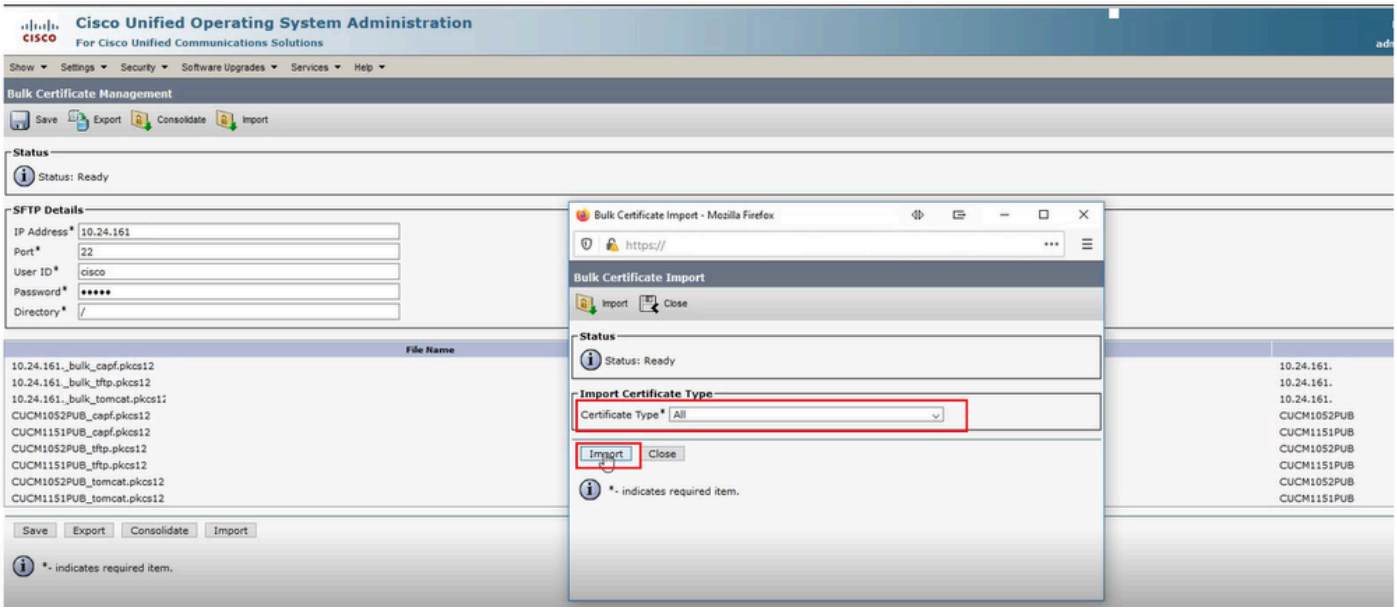
Importer des certificats dans les clusters source et de destination

Étape 1. Importer des certificats vers le cluster de destination.

Sur l'éditeur CUCM du cluster de destination, accédez à Cisco Unified OS Administration > Security > Bulk Certificate Management et laissez la page s'actualiser, puis cliquez sur Import :



Dans la fenêtre contextuelle Importation de certificat en masse, sélectionnez Tout pour le type de certificat, puis cliquez sur Importer. Cliquez sur Close pour fermer cette fenêtre.



Sélectionnez Tout, puis Importer

Étape 2. Répétez l'étape 1 pour le cluster source.

Remarque : Lorsque l'importation de certificats en bloc est effectuée, les certificats sont téléchargés vers le cluster distant de la manière suivante :
- Le certificat CAPF (Certificate Authority Proxy Function) est téléchargé en tant que CallManager-trust.
- Le certificat Tomcat est téléchargé en tant que tomcat-trust.
- Le certificat CallManager est téléchargé en tant que Phone-SAST-trust et CallManager-trust.
- Le certificat de récupération de la liste de confiance d'identité (ITLRecovery) est téléchargé en tant que Phone-SAST-trust et CallManager-trust.

Configuration des téléphones du cluster source avec les informations du serveur TFTP du cluster de destination

Configurez l'étendue DHCP pour les téléphones de cluster source avec l'option 150 TFTP (Trivial File Transfer Protocol) pour pointer vers les serveurs TFTP CUCM du cluster de destination.

Réinitialiser les téléphones du cluster source pour obtenir le fichier ITL/CTL du cluster de destination afin de terminer le processus de migration

Dans le cadre du processus de migration, les téléphones du cluster source tentent de configurer une connexion sécurisée au service de vérification de la confiance Cisco (TVS) du cluster source pour vérifier le certificat CallManager ou ITLRecovery du cluster de destination.

Remarque : Le certificat CallManager des clusters source d'un serveur CUCM qui exécute le service TFTP (également appelé certificat TFTP) ou son certificat ITLRecovery signe un fichier CTL (Certificate Trust List) et/ou ITL (Identity Trust List) de noeud CUCM source. De

même, le certificat CallManager du cluster de destination provenant d'un serveur CUCM qui exécute le service TFTP ou son certificat ITLRecovery signe un fichier CTL et/ou ITL de noeud CUCM du cluster de destination. Les fichiers CTL et ITL sont créés sur les noeuds CUCM qui exécutent le service TFTP. Si un fichier CTL et/ou ITL de cluster de destination n'est pas validé par le TVS de cluster source, la migration du téléphone vers le cluster de destination échoue.

Remarque : Avant de lancer le processus de migration des téléphones du cluster source, vérifiez que ces téléphones disposent d'un fichier CTL et/ou ITL valide. Assurez-vous également que la fonctionnalité d'entreprise Préparer le cluster pour la restauration vers la version antérieure à 8.0 est définie sur False pour le cluster source. Vérifiez également que les noeuds CUCM du cluster de destination qui exécutent le service TFTP disposent de fichiers CTL et/ou ITL valides.

Il s'agit du processus sans cluster sécurisé pour les téléphones sources afin d'obtenir le fichier ITL du cluster de destination pour terminer la migration des téléphones :

Étape 1. Ni CallManager ni le certificat ITLRecovery contenu dans le fichier ITL du cluster de destination, qui est présenté au téléphone du cluster source lors de la réinitialisation, ne peuvent être utilisés pour valider le fichier ITL actuellement installé. Le téléphone du cluster source établit alors une connexion au TVS du cluster source pour valider le fichier ITL du cluster de destination.
Étape 2. Le téléphone établit une connexion au TVS du cluster source sur le port TCP 2445.
Étape 3. Le TVS du cluster source présente son certificat au téléphone. Le téléphone valide la connexion et demande au TVS du cluster source de valider le certificat CallManager ou ITLRecovery du cluster de destination pour permettre au téléphone de télécharger le fichier ITL du cluster de destination.
Étape 4. Après la validation et l’installation du fichier ITL du cluster de destination, le téléphone du cluster source peut désormais valider et télécharger les fichiers de configuration signés à partir du cluster de destination.

Il s'agit du processus avec cluster sécurisé pour les téléphones sources afin d'obtenir le fichier CTL du cluster de destination pour terminer la migration des téléphones :

Étape 1. Le téléphone démarre et tente de télécharger le fichier CTL à partir du cluster de destination.
Étape 2. Le fichier CTL est signé par le certificat CallManager ou ITLRecovery du cluster de destination qui ne se trouve pas dans le fichier CTL ou ITL actuel du téléphone.
Étape 3. Par conséquent, le téléphone contacte TVS sur le cluster source pour vérifier le certificat CallManager ou ITLRecovery.

Remarque : À ce stade, le téléphone a toujours son ancienne configuration qui contient l'adresse IP du service TVS du cluster source. Les serveurs TVS spécifiés dans la configuration des téléphones sont identiques au groupe CallManager des téléphones.

Étape 4. Le téléphone configure une connexion TLS (Transport Layer Security) au TVS sur le

cluster source.
Étape 5. Lorsque le TVS du cluster source présente son certificat au téléphone, celui-ci le compare au certificat figurant dans son fichier ITL actuel.
Étape 6. S'ils sont identiques, la connexion s'effectue correctement.
Étape 7. Le téléphone source demande à la TVS du cluster source de vérifier le certificat CallManager ou ITLRecovery à partir du fichier CTL du cluster de destination.
Étape 8. Le service TVS source trouve CallManager ou ITLRecovery du cluster de destination dans son magasin de certificats, le valide et le téléphone du cluster source procède à la mise à jour avec le fichier CTL du cluster de destination.
Étape 9. Le téléphone source télécharge le fichier CTL du cluster de destination qui est validé par rapport au fichier CTL du cluster de destination qu'il contient maintenant. Puisque le fichier CTL du téléphone source contient maintenant le certificat CallManager ou ITLRecovery du cluster de destination, le téléphone source peut maintenant vérifier le certificat CallManager ou ITLRecovery sans devoir contacter le TVS du cluster source.

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Vidéo de configuration

Ce lien permet d'accéder à une vidéo qui parcourt la gestion de certificats en bloc entre les clusters CUCM :

Gestion de certificats en masse entre les clusters CUCM

Informations connexes

- Section Gestion des certificats en bloc du Guide d'administration de CUCM version 12.5(1)
- Gestion de certificats en masse entre les clusters CUCM
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.