Contenu

Introduction

Ce document décrit un problème avec le Cisco Emergency Responder (CER) où vous recevez le **CertExpiryEmergency : Délivrez un certificat l'échéance** message d'alarme **EMERGENCY_ALARM du** CLI et offrez une solution au problème.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance des versions 2.x à 9.x CER.

Supplémentaire, cette configuration exige que votre système :

- Ne contient aucune configuration de Domain Name Server (DN)
- A un serveur CER installé et les certifcates qui sont sur le point d'expirer

  Remarque: L'adresse IP du système n'importe pas si vous sélectionnez les **nouvelles** ou **régénérées** commandes de **générer** après que vous ayez changé l'adresse Internet ou l'adresse IP.

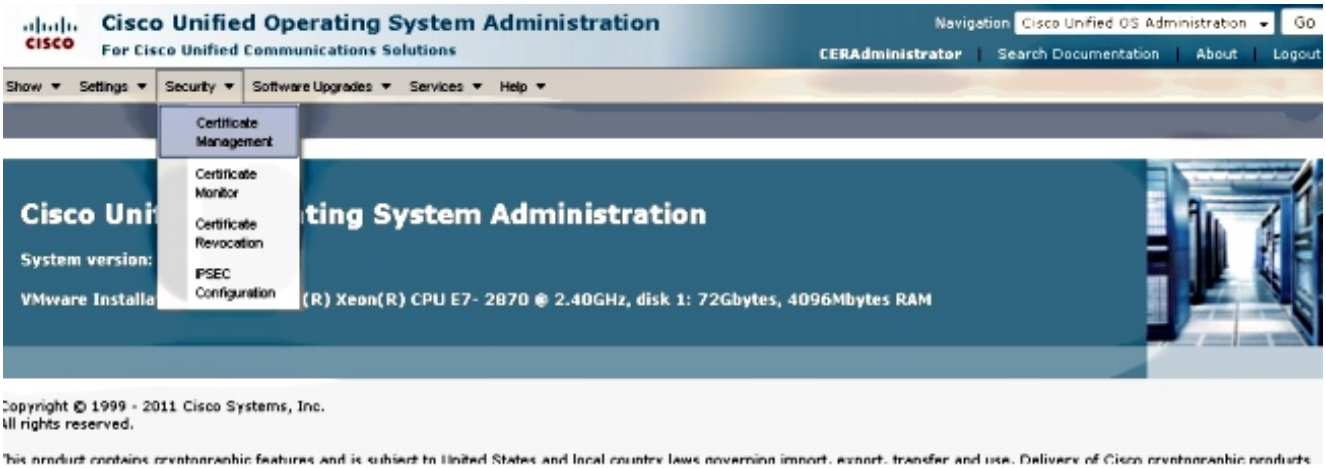
Composants utilisés

Les informations dans ce document sont basées sur la version 9.x CER.

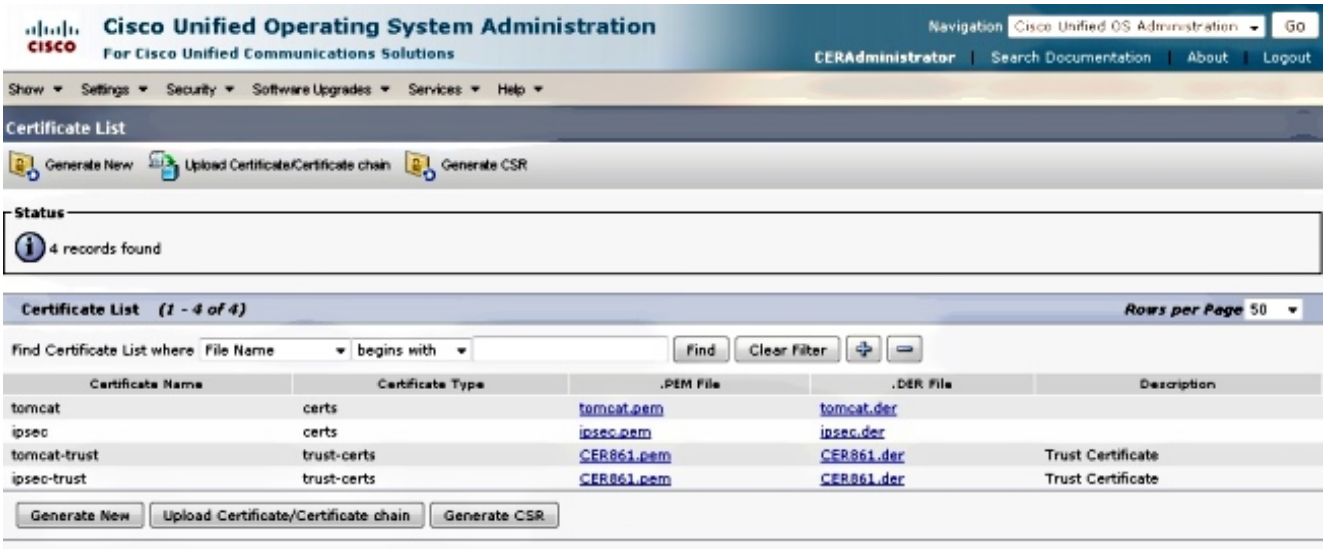
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez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

Générez un nouveau certificat

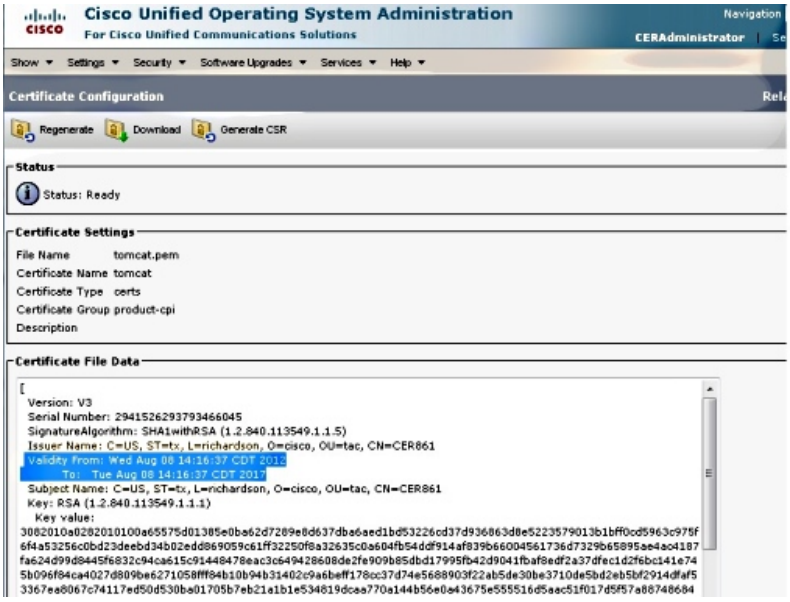
1. Allez au GUI dans la page du système d'exploitation de gestion (de SYSTÈME D'EXPLOITATION) et sélectionnez la page de **Gestion de Sécurité > de certificat**.



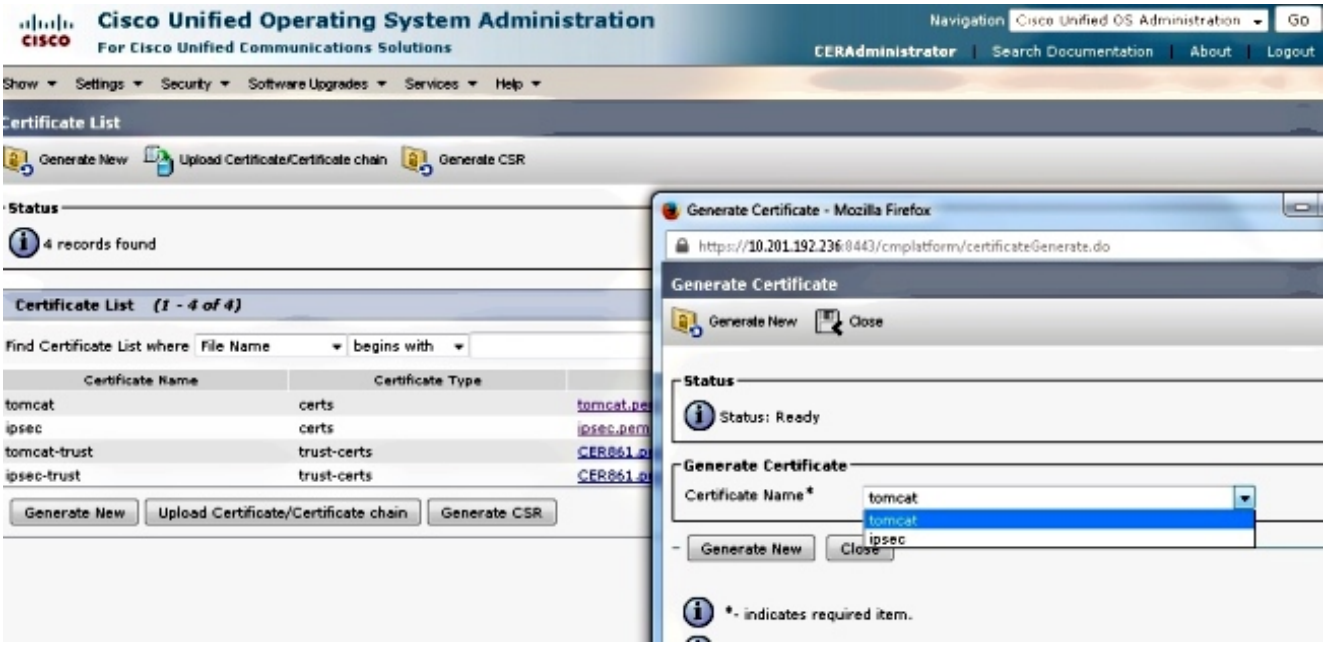
2. Afin d'afficher la liste de Certificats, cliquez sur le bouton de **découverte**.



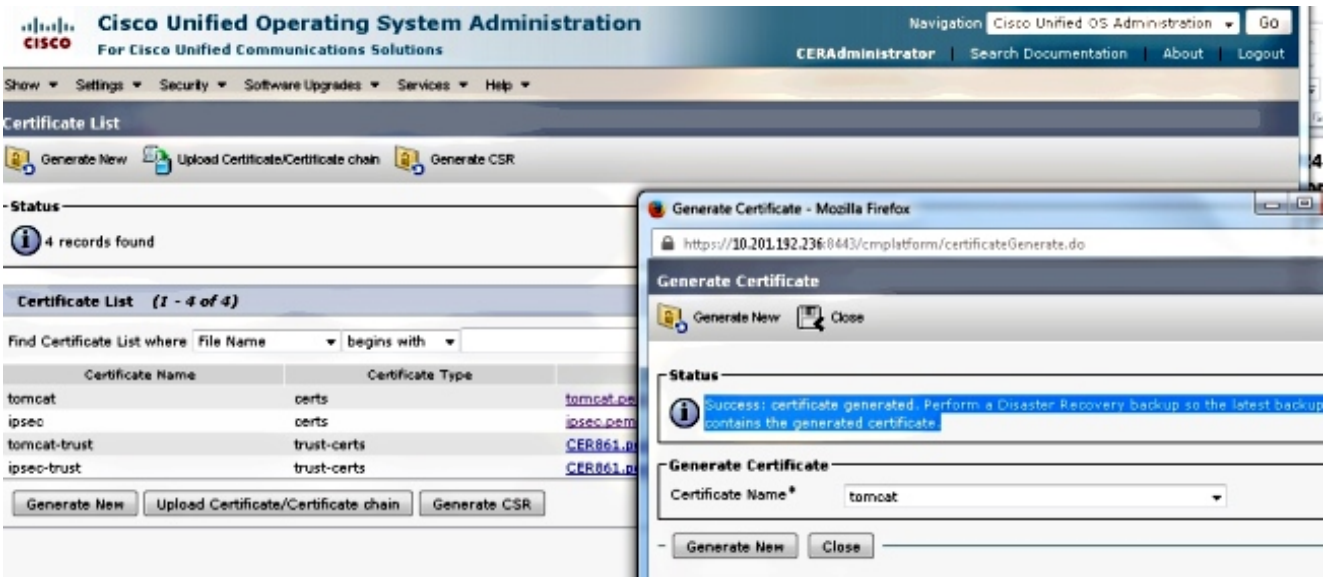
Cette capture d'écran affiche le **certificat tomcat.pem**, et le Validitydate est mis en valeur. Si le certificat est sur le point d'expirer, terminez-vous les étapes à venir.



3. Naviguez vers la page précédente et cliquez sur la **nouvelle** icône de **générer**. Cet écran s'affiche :



4. Afin de régénérer le certificat, le clic **génèrent nouveau** dans la fenêtre contextuelle. Affichages de message de succès afin d'annoncer que le certificat est régénéré.



5. Vous devez redémarrer Tomcat ou le service d'IPSec (IPSec) (si vous régénériez des Certificats d'IPSec). Afin de redémarrer Tomcat, ouvrir un CLI au noeud et sélectionner la commande de **Cisco Tomcat de reprise de service d'utils**. La page Web incite pour un téléchargement du nouveau certificat une fois que la page est de retour en ligne.

L'effacement a expiré des Certificats

Les informations importantes au sujet de la suppression de certificat :

- Assurez-vous que les Certificats qui sont placés pour la suppression ne sont plus en service

ou sont expirés réellement.
- Vérifiez toujours toutes les informations dans le certificat, parce qu'il ne peut pas être enregistré après qu'il soit supprimé.

Examinez tous les Certificats avec l'extension **.pem** et les vérifiez qu'ils sont tous dans une plage de temps valide. S'ils ne sont pas, alors ils peuvent être supprimés.

Si les plusieurs serveurs sont dans la batterie, vous devez aller à l'adresse IP de chacun des serveurs. Puis, dans la page d'admin de SYSTÈME D'EXPLOITATION, vous pouvez se terminer les étapes répertoriées dans la section de configurer.