

Expiration et suppression du certificat CER

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Générer un nouveau certificat](#)

[Supprimer les certificats expirés](#)

Introduction

Ce document décrit un problème avec Cisco Emergency Responder (CER) où vous recevez le **CertExpiryEmergency : Expiration du certificat** Message d'alarme **EMERGENCY_ALARM** de la CLI et offre une solution au problème.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les versions 2.x à 9.x de CER.

En outre, cette configuration nécessite que votre système :

- Ne contient aucune configuration DNS (Domain Name Server)
- Un serveur CER est-il installé et des certificats sont sur le point d'expirer ?

Note: L'adresse IP du système n'a pas d'importance si vous entrez les commandes **Generate New** ou **Regenerate** après avoir modifié le nom d'hôte ou l'adresse IP.

Components Used

Les informations contenues dans ce document sont basées sur la version 9.x de l'URCE.

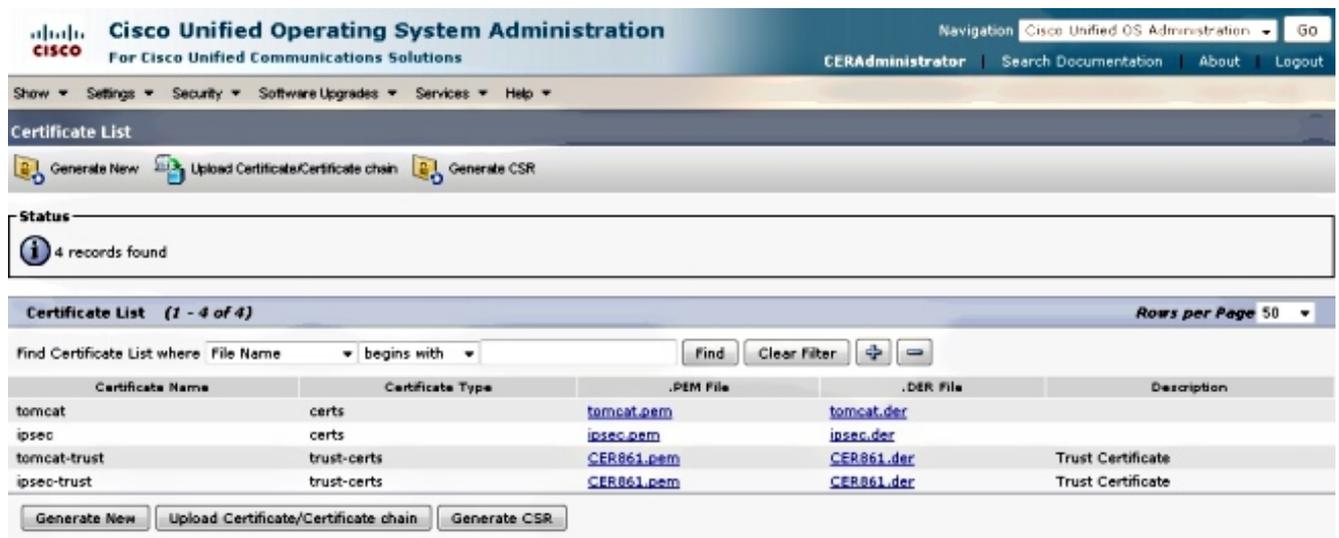
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Générer un nouveau certificat

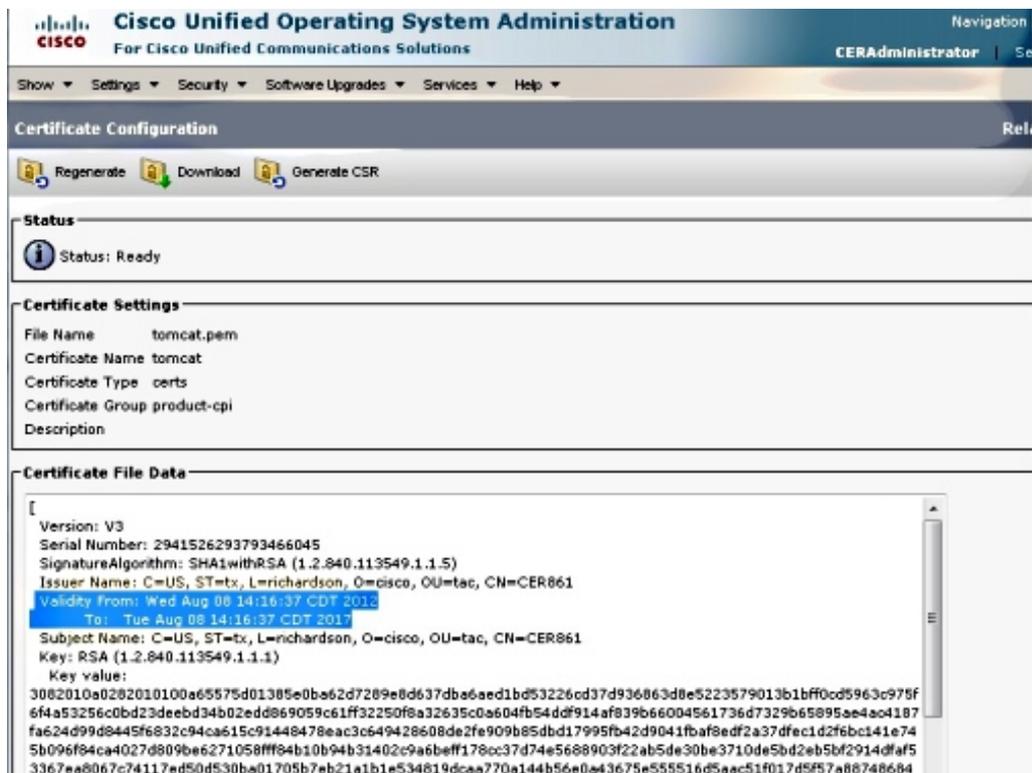
1. Accédez à l'interface utilisateur graphique de la page d'administration du système d'exploitation (OS) et sélectionnez la page **Security > Certificate Management**.



2. Pour afficher la liste des certificats, cliquez sur le bouton **Rechercher**.



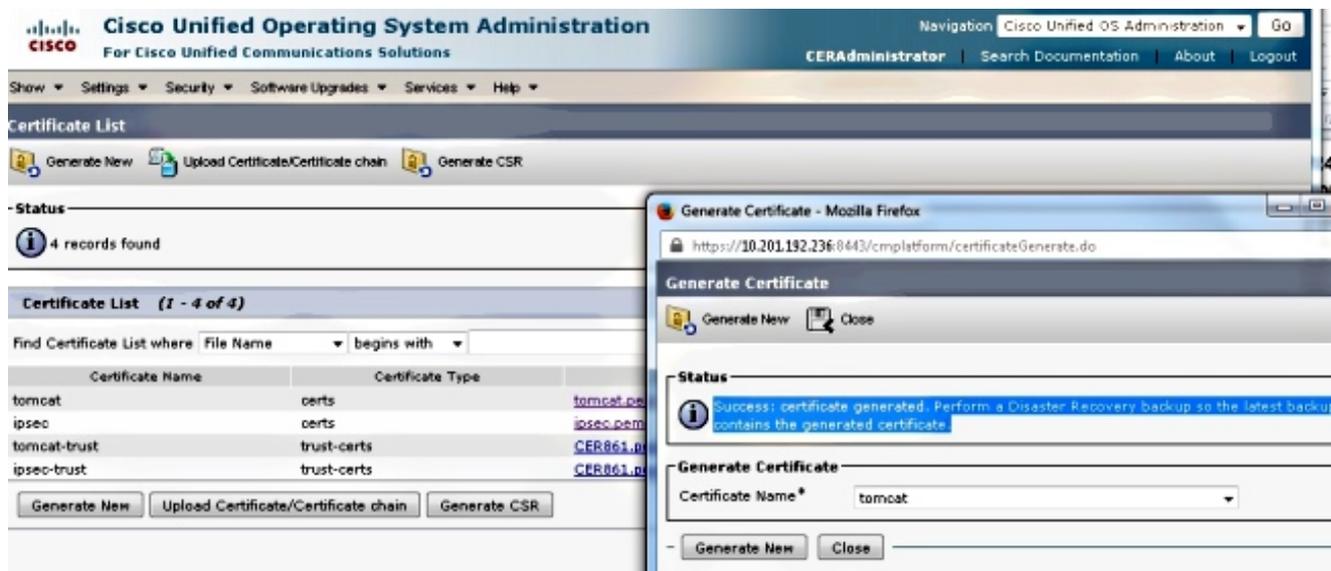
Cette capture d'écran montre le certificat **tomcat.pem** et la date de validité est mise en surbrillance. Si le certificat est sur le point d'expirer, procédez comme suit.



3. Accédez à la page précédente et cliquez sur l'icône **Generate New**. Cet écran s'affiche :



4. Afin de régénérer le certificat, cliquez sur **Generate New** dans la fenêtre contextuelle. Un message de réussite s'affiche afin d'annoncer que le certificat est régénéré.



5. Vous devez redémarrer Tomcat ou le service IPsec (Internet Protocol Security) (si vous avez régénéré des certificats IPsec). Afin de redémarrer Tomcat, ouvrez une CLI sur le noeud et entrez la commande **utils service restart Cisco Tomcat**. La page Web invite à télécharger le nouveau certificat une fois la page de nouveau en ligne.

Supprimer les certificats expirés

Remarques importantes sur la suppression de certificat :

- Assurez-vous que les certificats qui sont définis pour suppression ne sont plus utilisés ou ont en fait expiré.
- Vérifiez toujours toutes les informations du certificat, car il ne peut pas être enregistré après sa suppression.

Vérifiez tous les certificats avec l'extension **.pem** et vérifiez qu'ils se trouvent tous dans une plage de temps valide. Si ce n'est pas le cas, ils peuvent être supprimés.

Si plusieurs serveurs se trouvent dans le cluster, vous devez accéder à l'adresse IP de chacun des serveurs. Ensuite, dans la page Administrateur du système d'exploitation, vous pouvez effectuer les étapes répertoriées dans la section Configurer.