Supprimer les certificats de répondeur OCSP internes expirés dans ISE

Table des matières

Introduction

Ce document décrit comment supprimer les certificats de répondeur OCSP expirés et/ou sur le point d'expirer dans Cisco Identity Service Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base sur Identity Service Engine (ISE).
- Connaissances de base des certificats.
- Protocole OCSP (Online Certificate Status Protocol)

Composants utilisés

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

- Cisco Identity Service Engine 3.x

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de travaux pratiques spécifique.Tous les périphériques utilisés dans ce document ont démarré avec une configuration désactivée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Un problème courant rencontré par les clients utilisant Cisco Identity Services Engine (ISE) est la réception d'alarmes indiquant qu'un certificat a expiré, en particulier lorsque le certificat du répondeur OCSP a expiré ou est sur le point d'expirer et que le certificat est introuvable. Cette situation conduit souvent les clients à ouvrir des dossiers TAC pour obtenir de l'aide. L'objectif de ce guide est de permettre aux clients de localiser et de supprimer eux-mêmes ces certificats de répondeur OCSP expirés ou sur le point d'expirer, évitant ainsi d'avoir à soulever un dossier TAC.

Le protocole OCSP (Online Certificate Status Protocol) est un protocole utilisé pour vérifier l'état des certificats numériques x.509. Ce protocole est une alternative à la liste de révocation de certificats (CRL) et résout les problèmes qui entraînent la gestion des CRL. Cisco ISE peut communiquer avec les serveurs OCSP via HTTP pour valider l'état des certificats dans les authentifications. La configuration OCSP est configurée dans un objet de configuration réutilisable qui peut être référencé à partir de n'importe quel certificat d'autorité de certification configuré dans Cisco ISE.

Dans chaque déploiement Cisco ISE, les certificats de répondeur OCSP (Online Certificate Status Protocol) sont présents par défaut dans l'infrastructure CA interne (Certificate Authority). Ces certificats sont émis par l'autorité de certification interne Cisco ISE sur le PPAN (noeud d'administration de stratégie principal) et sont automatiquement générés pour chaque noeud du déploiement, y compris le PAN et tous les PSN (noeuds de service de stratégie).

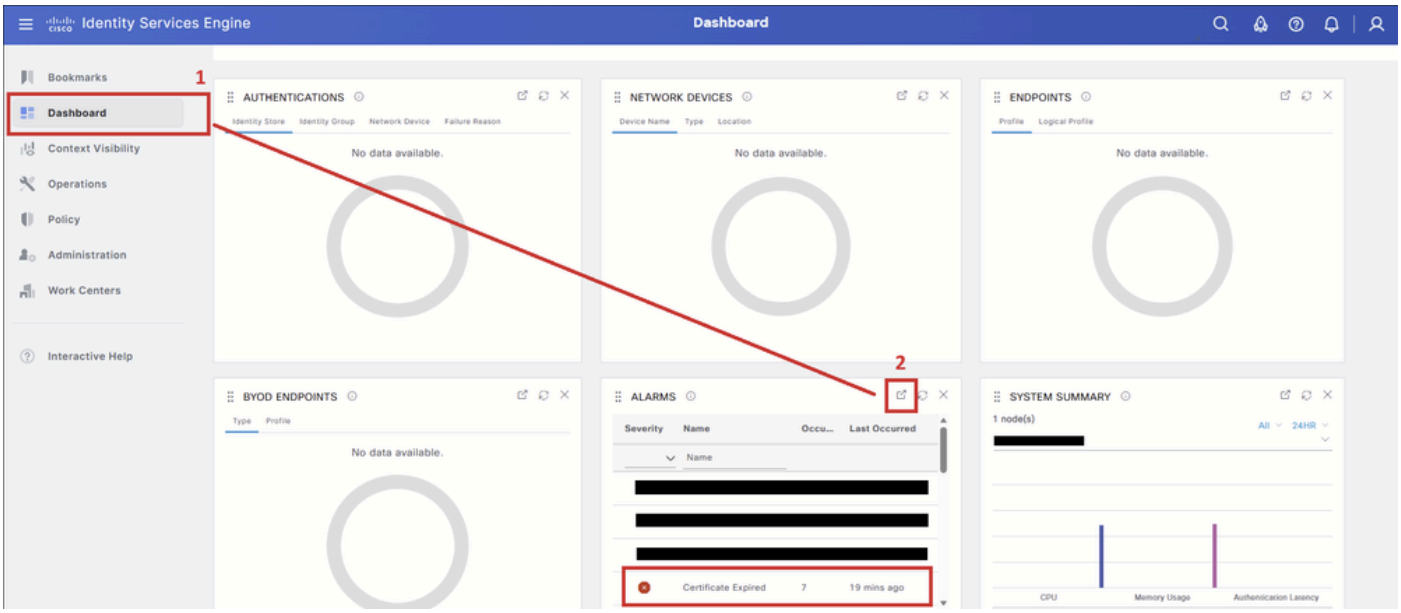
La gestion de ces certificats de répondeur OCSP est importante, car les certificats expirés ou sur le point d'expirer peuvent déclencher des alarmes de certificat expiré dans le tableau de bord

Cisco ISE. Bien que Cisco ISE régénère automatiquement les nouveaux certificats du répondeur OCSP, les entrées expirées restent dans le magasin de certificats de confiance jusqu'à ce qu'elles soient supprimées manuellement.

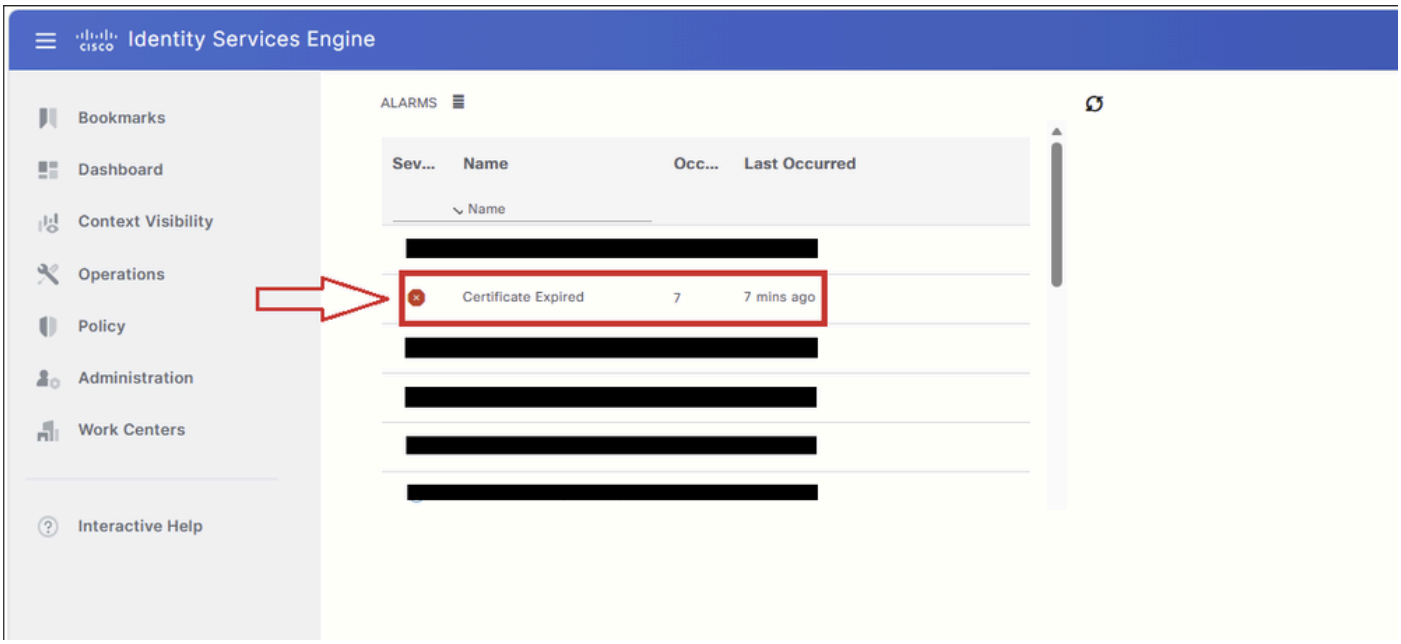
Configuration

Étape 1 : vérification du certificat OCSP expiré

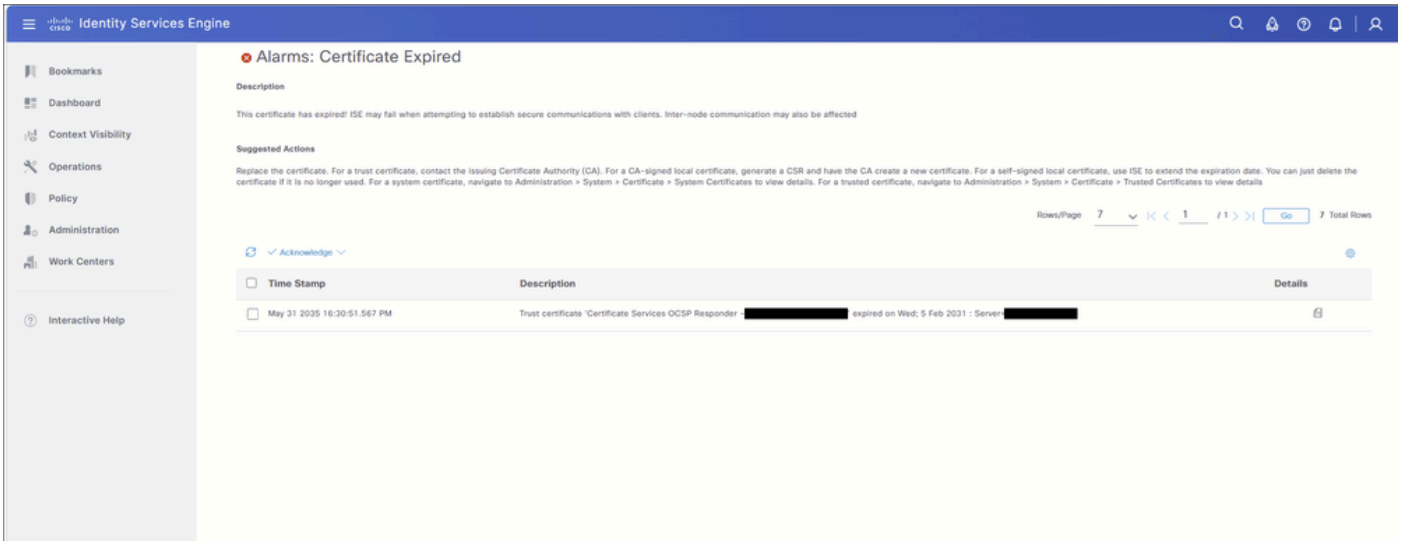
Dans l'interface graphique utilisateur PPAN (Primary Policy Administration Node), accédez à l'onglet Tableau de bord (1). Dans le dashlet Alarmes, cliquez sur le bouton Détacher (2) pour développer la table des alarmes.



Cliquez sur l'alarme Certificate Expired pour développer la table et afficher les entrées de certificat associées à l'alarme.



Tous les certificats qui ont déclenché l'alarme Certificat arrivé à expiration sont affichés dans ce tableau. Ce guide se concentre uniquement sur les certificats des répondeurs OCSP. Si le tableau inclut d'autres types de certificats expirés, tels que EAP, SAML, Admin ou d'autres certificats système, reportez-vous à la documentation Cisco appropriée et au guide de l'administrateur Cisco ISE pour obtenir des conseils sur ces types de certificats.



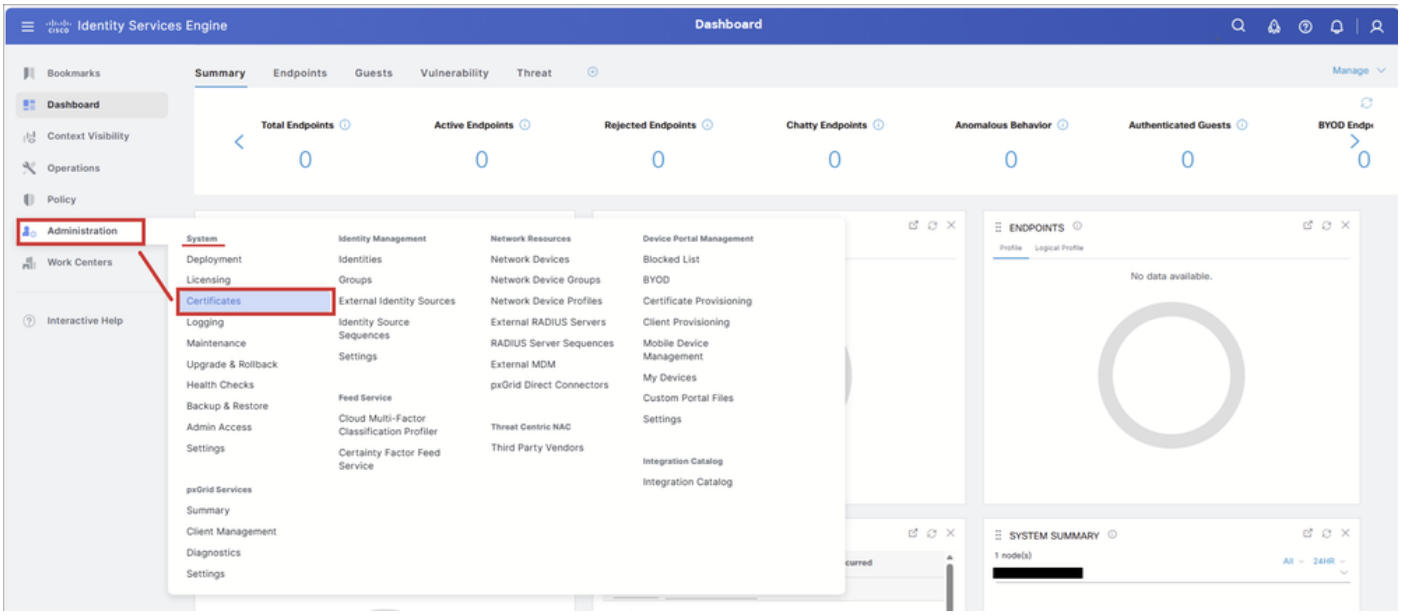
Vérifiez la description de l'alarme pour identifier le certificat qui a expiré ou qui, dans certains cas, va expirer.

Dans cet exemple, le certificat expiré est : Répondeur OCSP des services de certificats - <nom-noeud>#0004.

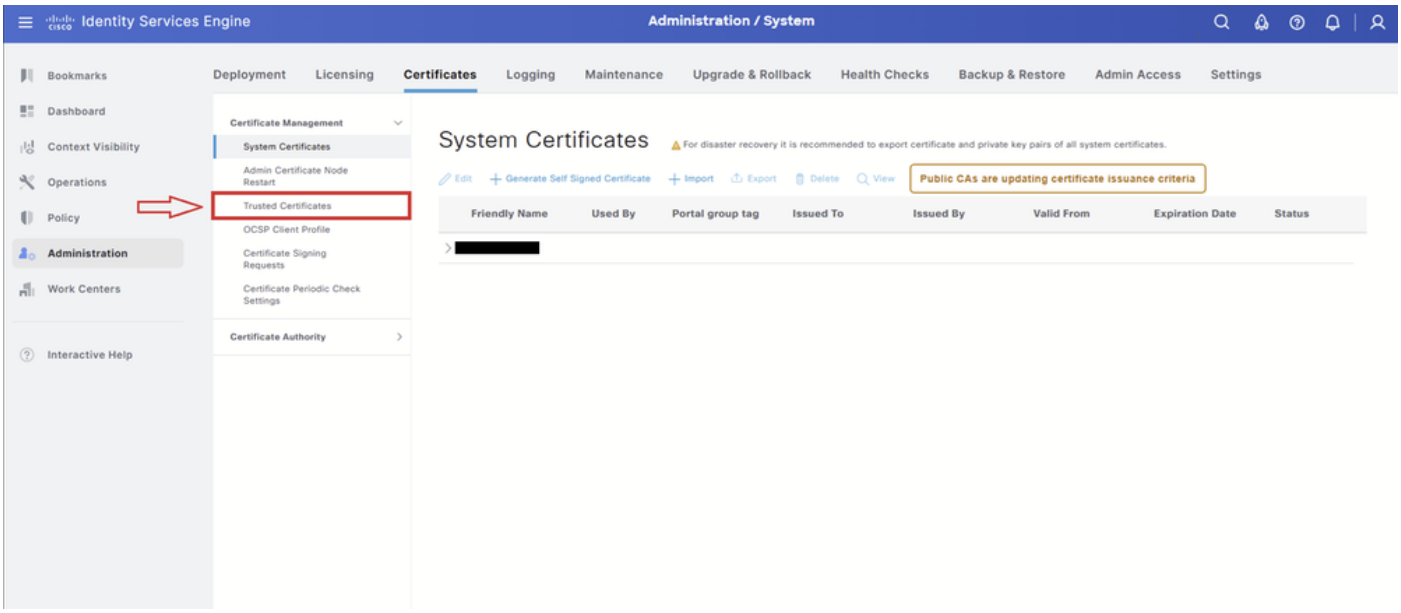
Prenez note du nom du certificat. Ce nom est utilisé dans les étapes suivantes pour localiser et supprimer le certificat du magasin de certificats approuvés.

Étape 2 - Recherchez et supprimez le certificat OCSP expiré

Naviguez jusqu'à l'adresse : Administration > Système > Certificats :



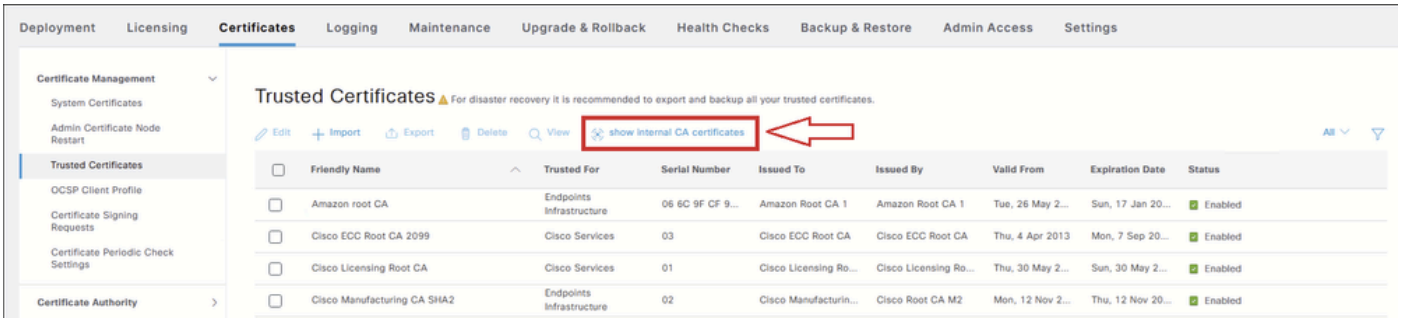
Sélectionnez l'onglet Certificats approuvés.



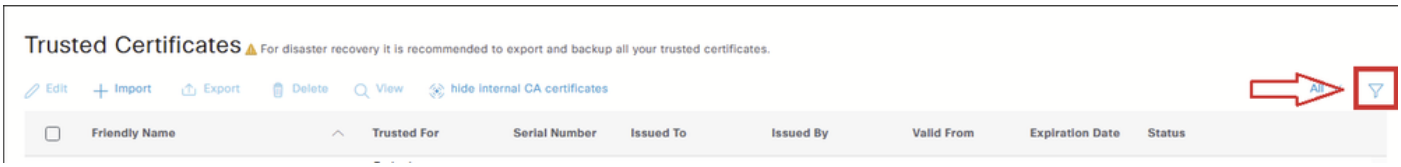
Sur la page Trusted Certificates, sélectionnez show internal CA certificates. Affiche les certificats de l'autorité de certification interne Cisco ISE, y compris les certificats du répondeur OCSP qui sont masqués par défaut.

Une fois sélectionné, le bouton change pour masquer les certificats CA internes.

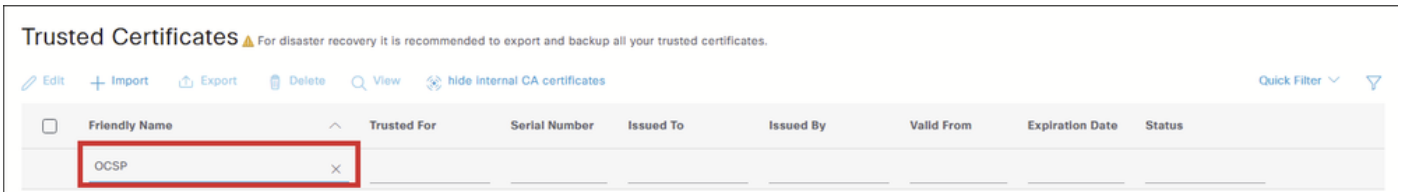
Avertissement : Cette étape est obligatoire. Si l'option show internal CA certificates n'est pas sélectionnée, le certificat du répondeur OCSP n'apparaît pas dans le tableau Trusted Certificate Store.



Dans le tableau Magasin de certificats approuvés, sélectionnez l'icône Filtre pour rechercher le certificat qui doit être supprimé.

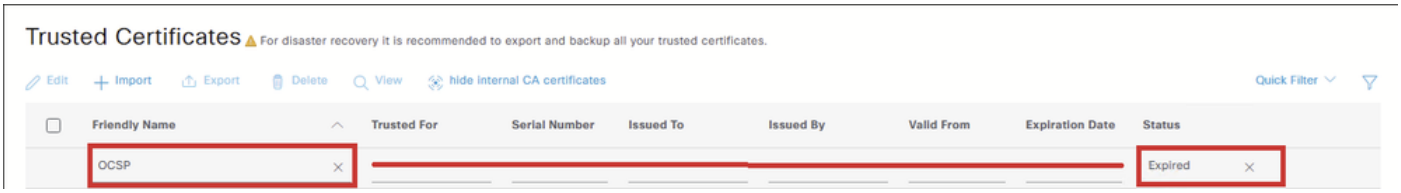


Si le certificat du répondeur OCSP est sur le point d'expirer, filtrez uniquement par OCSP sous Nom convivial. Si le certificat du répondeur OCSP a déjà expiré, passez à l'action suivante.



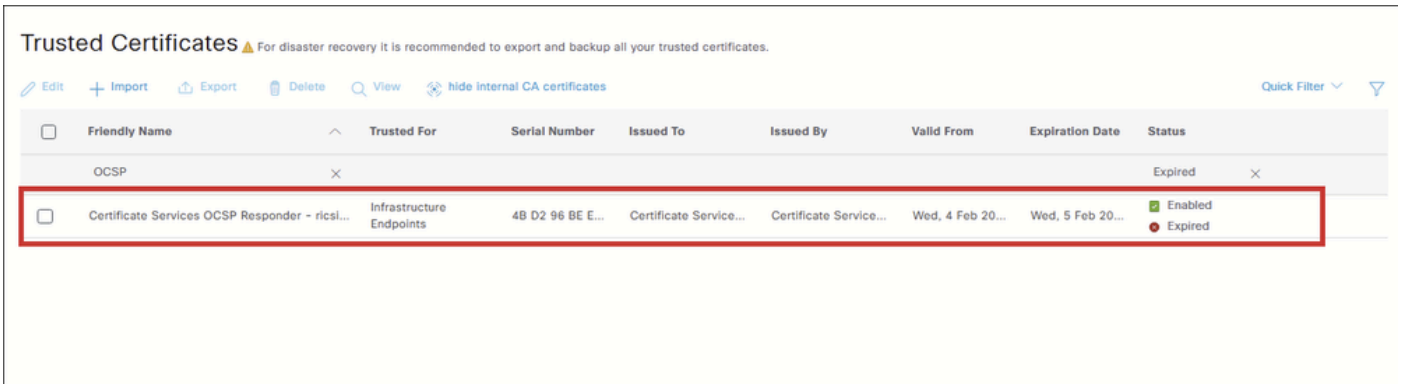
Pour localiser un certificat de répondeur OCSP expiré, entrez ces filtres :

- Nom convivial : OCSP
- État : Expired

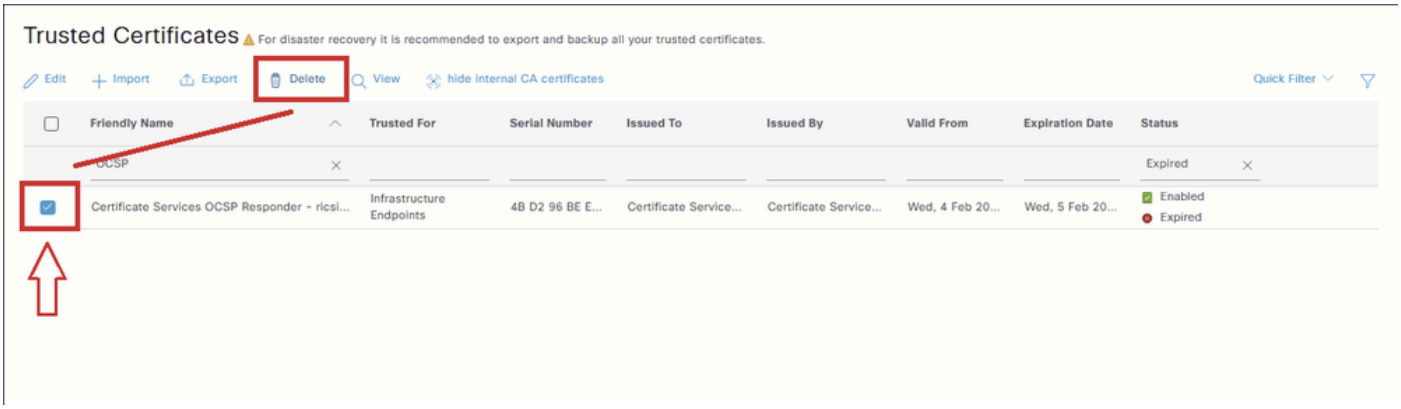


Le tableau affiche les certificats expirés du répondeur OCSP.

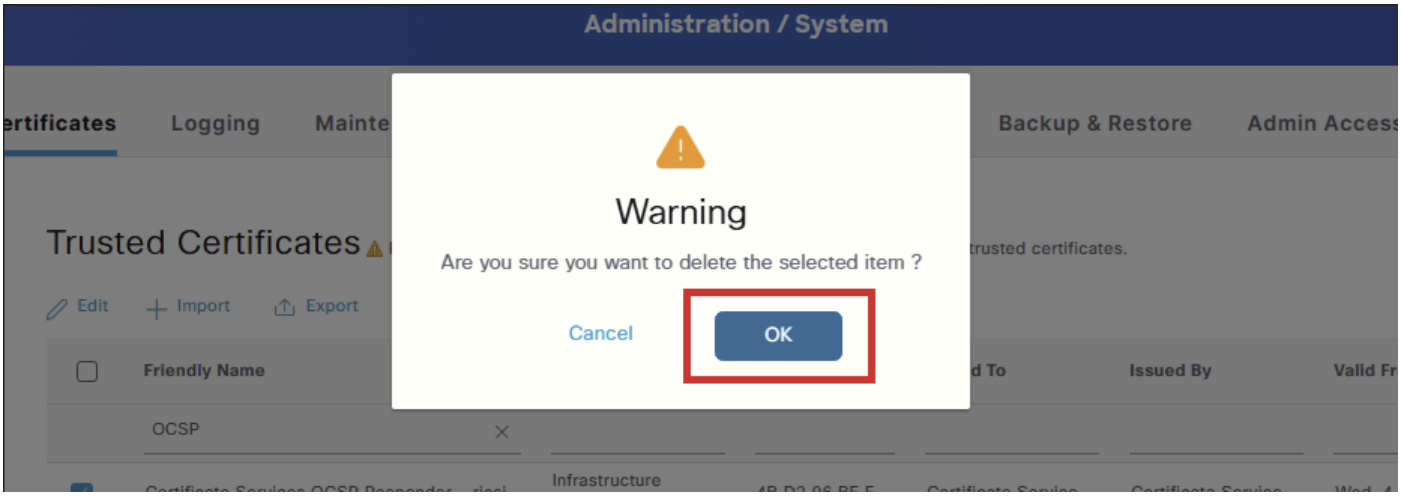
Conseil : Si vous recherchez un certificat de répondeur OCSP qui est sur le point d'expirer, plusieurs certificats peuvent être affichés, en particulier dans les déploiements avec plusieurs noeuds Cisco ISE. Pour identifier le bon certificat, ne filtrez pas uniquement par OCSP. À la place, filtrez par le nom de certificat complet qui a été affiché dans les détails de l'alarme à l'étape 1.



Cochez la case en regard du certificat du répondeur OCSP qui doit être supprimé et cliquez sur Supprimer.



Sélectionnez OK sur l'avertissement de confirmation pour continuer la suppression du certificat.



Avant de supprimer le certificat, il est important de comprendre que le certificat du répondeur OCSP fait partie de l'infrastructure d'autorité de certification interne ISE.

L'avertissement qui s'affiche pendant la suppression est générique et s'applique à tous les certificats liés à l'autorité de certification interne. Son objectif est de mettre en garde contre la suppression de certificats au sein de la hiérarchie d'autorité de certification interne, car certains de ces certificats signent des certificats de point d'extrémité utilisés pour des services tels que BYOD, pxGrid ou d'autres fonctions qui reposent sur des certificats émis par l'autorité de certification interne ISE.

Un certificat de répondeur OCSP expiré peut également affecter les certificats émis par l'autorité de certification interne ISE. Lorsqu'un client ou un service interroge l'état d'un certificat émis par cette autorité de certification, le service OCSP renvoie une erreur car le certificat du répondeur OCSP a expiré, ce qui peut entraîner l'échec de la validation de l'état du certificat.

Lorsque vous sélectionnez Supprimer, deux options s'affichent :

- Supprimer le certificat : Cette option supprime le certificat CA interne Cisco ISE du magasin de certificats approuvés. Lorsque le certificat d'autorité de certification interne est supprimé, tous les certificats de point de terminaison signés par cette autorité de certification deviennent invalides et les points de terminaison affectés ne peuvent pas accéder au réseau. Cette action est réversible : vous pouvez restaurer l'accès au réseau en réimportant le même certificat d'autorité de certification interne dans le magasin de certificats approuvés.
- Supprimer et révoquer le certificat : Cette option supprime et révoque le certificat de CA interne Cisco ISE. Comme avec l'option Delete, tous les certificats de point de terminaison signés par l'autorité de certification interne deviennent invalides et les points de terminaison affectés perdent l'accès au réseau. Cependant, cette opération est irréversible. Après la révocation, vous devez remplacer toute la chaîne de certificats racine Cisco ISE pour que le déploiement puisse restaurer la fonctionnalité.

Quelle option sélectionner pour un certificat de répondeur OCSP arrivé à expiration ?

L'impact décrit s'applique aux certificats d'autorité de certification interne qui signent activement des certificats de point de terminaison. Le certificat du répondeur OCSP ne signe pas les certificats de point d'extrémité, il est utilisé pour la communication OCSP. Bien qu'un certificat de répondeur OCSP expiré puisse entraîner l'échec de la validation de l'état du certificat pour les certificats émis par l'autorité de certification interne, le certificat a déjà expiré et ne fournit donc plus de réponses OCSP valides. Sa suppression n'a pas d'impact supplémentaire.

Comme le certificat du répondeur OCSP dans ce scénario a déjà expiré, il n'est plus valide. Dans ce cas, Delete et Delete & Revoke produisent le même résultat, car il ne reste plus rien de valide à révoquer.

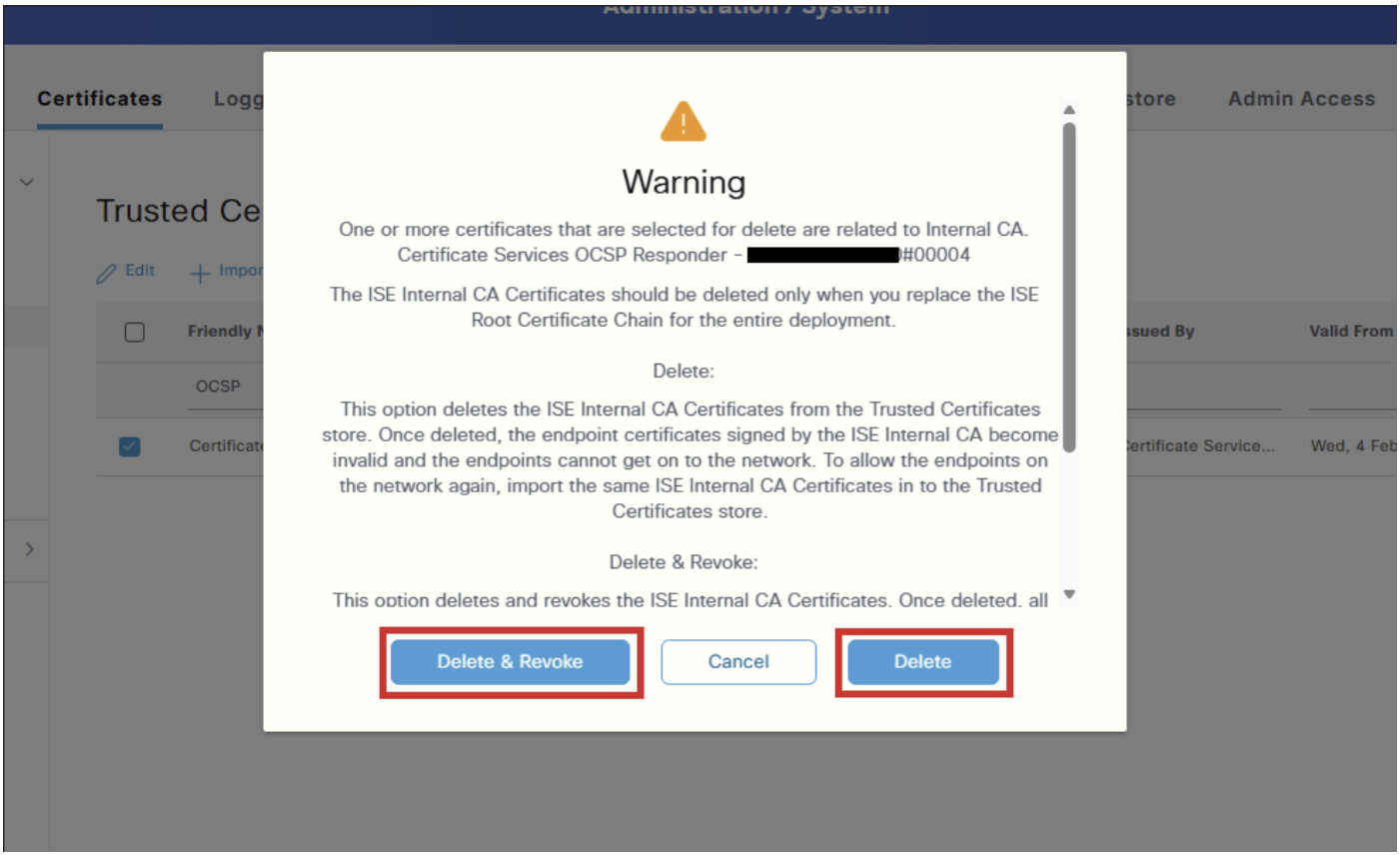
Pour ces raisons, l'option Supprimer est recommandée, car il s'agit de l'action la plus simple qui évite de générer une entrée de révocation inutile.

Remarque : Les certificats du répondeur OCSP ne sont pas régénérés en fonctionnement normal. Elles sont régénérées uniquement lorsqu'un correctif est installé :
- Dans un déploiement à plusieurs noeuds, les certificats sont régénérés lorsque le correctif est installé via l'interface utilisateur graphique.
- Dans un déploiement autonome, les certificats sont régénérés lorsque le correctif est installé via l'interface utilisateur graphique ou l'interface de ligne de commande.

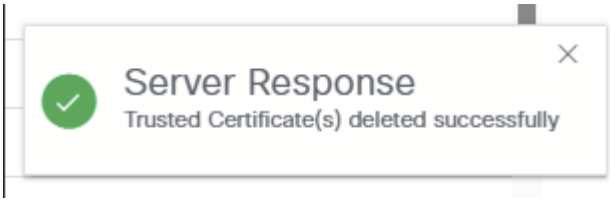
Un nouveau certificat de répondeur OCSP est généré uniquement lors de la prochaine installation du correctif.

Mise en garde : Assurez-vous que le noeud affecté dispose d'un certificat de répondeur OCSP actif et valide dans le magasin de certificats de confiance. Si aucun certificat valide n'est présent et que le protocole OCSP est utilisé pour valider les certificats signés par l'autorité de certification interne ISE, cette validation échoue jusqu'à ce qu'un nouveau certificat de répondeur OCSP soit généré.

Si aucun certificat de répondeur OCSP valide n'est présent, renouvelez les certificats de répondeur OCSP à partir du PPAN (noeud d'administration de stratégie principale) comme décrit ici :
1. Accédez à l'interface utilisateur graphique ISE PPAN.
2. Accédez à Administration > Système > Certificats.
3. Sélectionnez Certificate Signing Requests sur la gauche.
4. Cliquez sur Générer CSR. Pour Utilisation, sélectionnez Renouveler le répondeur ISE OCSP.
5. Cliquez sur Renew ISE OCSP Responder Certificates pour terminer le processus.



Une fois le certificat supprimé, une notification de réponse du serveur apparaît, indiquant que le certificat approuvé a été supprimé :



Vérifier

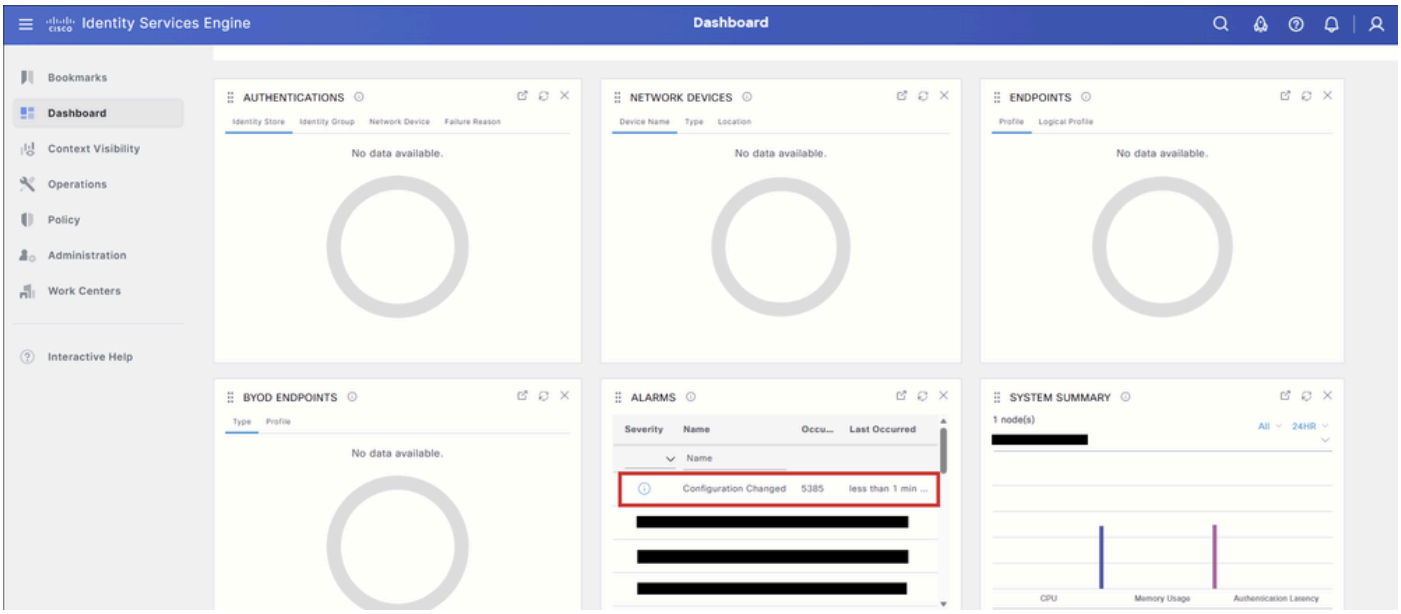
Une fois le certificat supprimé, vous pouvez utiliser l'une de ces méthodes ou les deux pour vérifier que l'opération a réussi.

Option 1 : vérification à partir des alarmes du tableau de bord

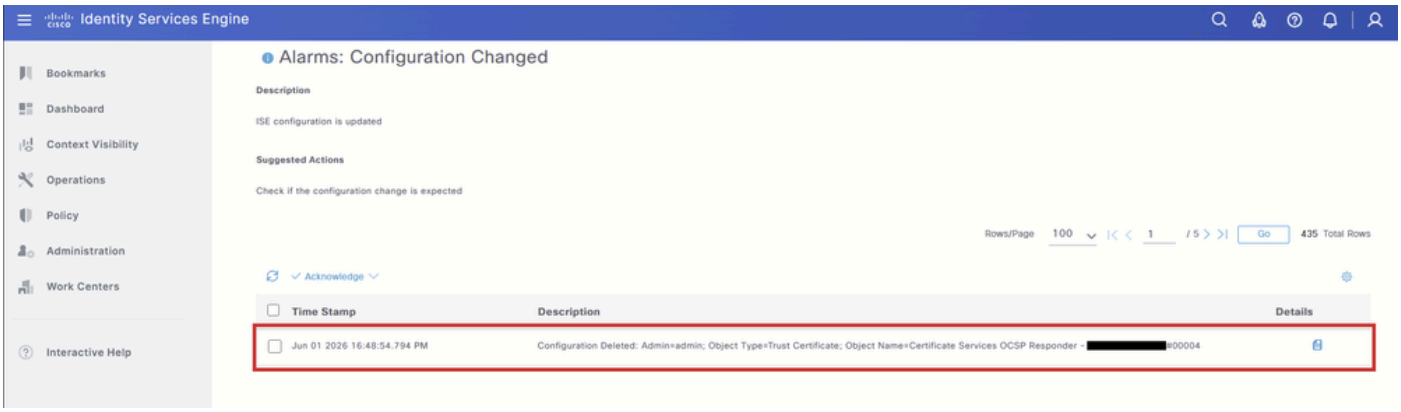
Accédez à la page Tableau de bord.

Dans le dashlet Alarmes, localisez l'alarme Configuration modifiée. Sélectionnez l'alarme pour

afficher les détails.



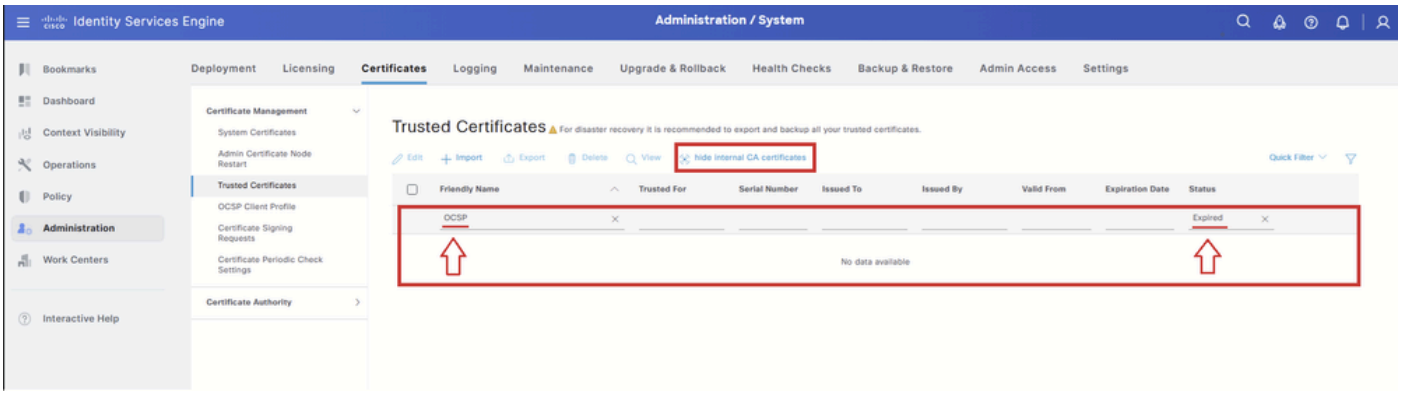
Une entrée doit apparaître pour indiquer qu'un objet de configuration a été supprimé. Le nom de l'objet doit correspondre au certificat du répondeur OCSP qui a été supprimé.



Option 2 - Vérification à partir du magasin de certificats de confiance

Comme étape supplémentaire, revenez à la table Trusted Certificate Store et filtrez le certificat du répondeur OCSP. Le certificat ayant été supprimé, la table doit afficher Aucune donnée disponible.

Remarque : N'oubliez pas de sélectionner show internal CA certificates.


Identity Services Engine
Administration / System
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade & Rollback
Health Checks
Backup & Restore
Admin Access
Settings
Certificate Management
System Certificates
Admin Certificate Node Restart
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Settings
Certificate Authority
Trusted Certificates
For disaster recovery it is recommended to export and backup all your trusted certificates.
Edit
Import
Export
Delete
View
Hide Internal CA certificates
Quick Filter
Friendly Name
Trusted For
Serial Number
Issued To
Issued By
Valid From
Expiration Date
Status
OCSP
Expired
No data available

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.