Dépannage des alertes d'expiration de certificat de liste de CA personnalisée sur ESA

Table des matières

Introduction

Aperçu

Composants utilisés

Informations générales

Problème

Solution

Informations connexes

Introduction

Ce document décrit les alertes d'expiration de certificat CA personnalisées sur une passerelle de messagerie sécurisée (ESA) après une mise à niveau vers AsyncOS 14.x.

Aperçu

Le symptôme est l'apparition d'alertes d'expiration pour les certificats ajoutés à la liste Autorité de certification personnalisée pendant la mise à niveau. L'impact est limité aux alertes d'information car l'expiration des certificats dans la liste personnalisée n'affecte pas les certificats dans la liste système. La résolution consiste à vérifier la source du certificat et à remplacer le certificat CA personnalisé requis ou à supprimer le certificat expiré de la liste personnalisée.

Composants utilisés

Ce document est basé sur la passerelle de messagerie sécurisée Cisco exécutant AsyncOS 14.0 ou version ultérieure.

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

Au cours du processus de mise à niveau vers AsyncOS 14.x, les clients sont invités à confirmer s'ils souhaitent ajouter d'anciens certificats système à la liste d'autorités de certification personnalisée. Ce comportement est également décrit dans les notes de version d'AsyncOS 14.0, comme illustré dans l'image 1. Reportez-vous aux Notes de version de Cisco Secure Email Gateway pour AsyncOS 14.0.

Image 1. Extrait des notes de version qui montre l'invite de mise à niveau pour ajouter d'anciens certificats système à la liste d'autorités de certification personnalisée.

Certificate Authority Configuration Changes	The Certificate Authority (CA) configuration changes are applicable in any one of the following scenarios: • Upgrade from a lower AsyncOS version to AsyncOS 14.0 version and later. • Install AsyncOS 14.0 for Cisco Secure Email Gateway for the first time. The following changes are made to the Certificate Authorities list: • You can view the count and details of custom and system CA certificates in your email gateway. Use the **Managed Trusted Root Certificates** option in Network > Certificates > page to view the custom or system CA certificate details. • You can upload, delete, or append the custom CA certificate in your email gateway. • You will not be able to upload duplicate custom CA certificates to your email gateway. • [**Applicable for new AsyncOS install only**]: You can update the existing system CA certificate bundle to the latest available version. Use the **Update Now** option in Network > Certificates page in the web interface or the `updatenow` CLI command to update the existing system CA certificate bundle. • [**Applicable for AsyncOS upgrade only**]: – During upgrade, you can choose to append the valid CA certificates from the system CA bundle (of the current AsyncOS build) to the custom CA bundle of the upgraded AsyncOS build. **Note** The backup of the current system CA bundle is stored in the following location - `/data/pub/systemca.old/trustedca.old.pem` – After upgrade, the system CA certificate bundle of the current AsyncOS build is updated to the latest version automatically.

Problème

Après une mise à niveau vers AsyncOS 14.x, les certificats système plus anciens ajoutés à la liste personnalisée peuvent expirer au fil du temps et générer des alertes comme dans cet exemple.

26 juin 2021 11:27:29 -0400 Votre certificat CA : Root CA Generalitat Valenciana expire dans 5 jours (s).

Ces alertes indiquent l'expiration d'anciens certificats système ajoutés à la liste personnalisée au moment de la mise à niveau ou l'expiration prochaine d'un certificat personnalisé précédemment utilisé.

Solution

Les alertes pour les certificats système plus anciens de la liste personnalisée sont fournies à titre d'information et vous pouvez choisir de les supprimer de la liste personnalisée ou de les laisser expirer.

Cette condition n'affecte pas le service, mais l'alerte peut être indésirable.

Si vous voyez des alertes pour un certificat d'autorité de certification personnalisé qui est requis par votre organisation et ne fait pas actuellement partie de la liste système, contactez l'autorité de certification pour un certificat mis à jour et remplacez-le comme décrit dans la procédure de gestion de certificat du Guide d'administration de Cisco Secure Email Gateway.

L'ensemble de certificats CA système est mis à jour automatiquement après une mise à niveau et périodiquement par la suite. L'expiration des certificats de la liste personnalisée n'affecte pas les certificats de la liste système.

Pour vérifier que la liste système et la liste personnalisée sont toutes deux activées, accédez à Réseau > Certificats > Autorités de certification > Modifier les paramètres.

Vous pouvez également exporter les listes système et personnalisées à partir du même menu, ou utiliser les commandes CLI certconfig et certauthority pour vérifier les certificats dans les deux listes si nécessaire.

Si vous souhaitez supprimer le certificat qui génère des alertes dans la liste d'autorités de certification personnalisée, effectuez ces étapes en tant qu'administrateur sur SSH vers l'appliance.

1. Exécutez certconfig.
2. Saisissez certauthority, puis custom.

3. Entrez delete et sélectionnez le certificat qui correspond à l'alerte.
4. Confirmez la suppression, puis exécutez commit pour enregistrer la modification.

Cet exemple de CLI illustre le workflow.

Remarque : Vérifiez le nom et la position du certificat dans la liste personnalisée en fonction de l'alerte, car il peut être différent de l'exemple de sortie présenté dans cet exemple.

```
example.com> certconfig

Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]> certauthority

Certificate Authority Summary
Custom List: Enabled
System List: Enabled

Choose the operation you want to perform:
- CUSTOM - Manage Custom Certificate Authorities
- SYSTEM - Manage System Certificate Authorities
[]> custom

Choose the operation you want to perform:
- DISABLE - Disable the custom certificate authorities list
- IMPORT - Import the list of custom certificate authorties
- EXPORT - Export the list of custom certificate authorties
- DELETE - Remove a certificate from the custom certificate authorty list
- PRINT - Print the list of custom certificate authorties
- CHECK_CA_FLAG - Check CA flag in uploaded custom CA certs
[]> delete

You must enter a value from 1 to 104.
...
59. [Root CA Generalitat Valenciana] <<< Select this certificate based on the sample alert in this exam
...
93. [thawte Primary Root CA]

Select the custom CA certificate you want to delete
[]> 59

Are you sure you want to delete "Root CA Generalitat Valenciana"? [N]> Y
Custom CA certificate "Root CA Generalitat Valenciana" removed

Choose the operation you want to perform:
- DISABLE - Disable the custom certificate authorities list
- IMPORT - Import the list of custom certificate authorties
- EXPORT - Export the list of custom certificate authorties
- DELETE - Remove a certificate from the custom certificate authorty list
- PRINT - Print the list of custom certificate authorties
- CHECK_CA_FLAG - Check CA flag in uploaded custom CA certs
[]> [ENTER]

Certificate Authority Summary
```

```
Custom List: Enabled
System List: Enabled
Choose the operation you want to perform:
- CUSTOM - Manage Custom Certificate Authorities
- SYSTEM - Manage System Certificate Authorities
[]> [ENTER]

Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]> [ENTER]

example.com> commit
```

Assurez-vous d'exécuter commit à la fin.

Informations connexes

- Notes de version de Cisco Secure Email Gateway
- Guides d'utilisation de Cisco Secure Email Gateway

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.