Fehlerbehebung bei Warnungen zum Ablauf von Zertifikaten in der benutzerdefinierten Zertifizierungsstellenliste auf der ESA

Inhalt

Einleitung

In diesem Dokument werden benutzerdefinierte Warnmeldungen zum Ablauf von Zertifizierungsstellenzertifikaten auf einem sicheren E-Mail-Gateway (ESA) nach einem Upgrade auf AsyncOS 14.x beschrieben.

Überblick

Bei dem Symptom handelt es sich um Ablaufwarnungen für Zertifikate, die während des Upgrades an die Liste der Zertifizierungsstellen für benutzerdefinierte Zertifikate angefügt wurden. Die Auswirkung ist auf Informationswarnungen beschränkt, da das Ablaufdatum von Zertifikaten in der benutzerdefinierten Liste keine Auswirkungen auf Zertifikate in der Systemliste hat. Die Auflösung besteht darin, die Zertifikatquelle zu überprüfen und entweder das erforderliche benutzerdefinierte Zertifizierungsstellenzertifikat zu ersetzen oder das abgelaufene Zertifikat aus der benutzerdefinierten Liste zu entfernen.

Verwendete Komponenten

Dieses Dokument basiert auf Cisco Secure Email Gateway mit AsyncOS 14.0 oder höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Beim Upgrade auf AsyncOS 14.x werden Kunden aufgefordert, zu bestätigen, ob sie ältere Systemzertifikate an die benutzerdefinierte Zertifizierungsstellenliste anhängen möchten. Dieses Verhalten wird auch in den Versionshinweisen von AsyncOS 14.0 dokumentiert, wie in Abbildung 1 dargestellt. Weitere Informationen finden Sie in den Versionshinweisen von Cisco Secure Email Gateway für AsyncOS 14.0.

Bild 1. Auszug aus den Versionshinweisen, der die Upgrade-Aufforderung zum Anhängen älterer Systemzertifikate an die benutzerdefinierte Zertifizierungsstellenliste anzeigt.

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.

Problem

Nach einem Upgrade auf AsyncOS 14.x können ältere Systemzertifikate, die an die benutzerdefinierte Liste angehängt wurden, im Laufe der Zeit ablaufen und Warnungen wie in diesem Beispiel generieren.

26 Jun 2021 11:27:29 -0400 Ihr Zertifikat CA:Root CA Generalitat Valenciana läuft in 5 Tagen (s) ab.

Diese Warnungen geben an, dass entweder ältere Systemzertifikate ablaufen, die zum Zeitpunkt des Upgrades an die benutzerdefinierte Liste angehängt wurden, oder ein benutzerdefiniertes Zertifikat, das zuvor für den bevorstehenden Ablauf verwendet wurde.

Lösung

Die Warnungen für ältere Systemzertifikate in der benutzerdefinierten Liste sind informativ, und Sie können sie aus der benutzerdefinierten Liste entfernen oder deren Ablauf zulassen.

Diese Bedingung wirkt sich nicht auf den Dienst aus, die Warnung kann jedoch unerwünscht sein.

Wenn Warnungen für ein benutzerdefiniertes Zertifizierungsstellenzertifikat angezeigt werden, das von Ihrer Organisation benötigt wird und derzeit nicht in der Systemliste enthalten ist, wenden Sie sich an die Zertifizierungsstelle, um ein aktualisiertes Zertifikat zu erhalten, und ersetzen Sie es wie im Zertifikatverwaltungsverfahren für das Cisco Secure Email Gateway-Administratorhandbuch beschrieben.

Das Zertifizierungsstellen-Zertifikatspaket des Systems wird nach einem Upgrade automatisch und anschließend in regelmäßigen Abständen aktualisiert. Das Ablaufdatum von Zertifikaten in der benutzerdefinierten Liste hat keine Auswirkungen auf Zertifikate in der Systemliste.

Um zu überprüfen, ob die Systemliste und die benutzerdefinierte Liste aktiviert sind, navigieren Sie zu Netzwerk > Zertifikate > Zertifizierungsstellen > Einstellungen bearbeiten.

Sie können die System- und benutzerdefinierten Listen auch aus demselben Menü exportieren oder die CLI-Befehle certconfig und certauthority verwenden, um die Zertifikate in beiden Listen nach Bedarf zu überprüfen.

Wenn Sie das Zertifikat entfernen möchten, das Warnungen in der benutzerdefinierten Zertifizierungsstellenliste generiert, führen Sie diese Schritte als Administrator über SSH für die

Appliance aus.

1. Führen Sie certconfig aus.
2. Geben Sie certauthority ein, und geben Sie dann custom ein.
3. Geben Sie delete ein, und wählen Sie das Zertifikat aus, das mit der Warnung übereinstimmt.
4. Bestätigen Sie den Löschvorgang, und führen Sie dann commit aus, um die Änderung zu speichern.

Dieses CLI-Beispiel zeigt den Workflow.

 Anmerkung: Überprüfen Sie den Namen und die Position des Zertifikats in der benutzerdefinierten Liste auf Grundlage der Warnung, da es sich von der Beispielausgabe in diesem Beispiel unterscheiden kann.

```
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
```

Stellen Sie sicher, dass Sie commit am Ende ausführen.

Zugehörige Informationen

- Cisco Secure Email Gateway - Versionshinweise
- Benutzerhandbücher zu Cisco Secure Email Gateway

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.