ESA瞭解自定義CA清單證書過期警報

目錄

簡介

本檔案介紹升級到Async OS 14.x後，思科安全電子郵件閘道(ESA)上的自訂憑證授權單位(CA)憑證到期警報以及因應措施解決方案。

採用元件

本文檔中的資訊基於運行Async OS 14.0或更高版本的ESA。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在升級到Async OS 14.x的過程中，客戶需要確認是否要在自定義CA清單中附加舊的系統證書。這也會記錄在14.0版本說明中，如下面的螢幕截圖所示。此處提供完整的版本說明。

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.

問題

升級到14.x後，自定義清單中附加的舊系統證書隨著時間的推移可能會過期，從而產生如下警報。

2021年6月26日11:27:29 -0400您的證書「CA:Root CA Generalitat Valenciana」將在5天後過期。

這些警報表示升級時附加到自定義清單的舊系統證書即將過期，或者表示先前使用的自定義證書即將過期。

解決方案

請注意，自定義清單中的舊系統證書警報只是提供資訊，您可以選擇將其從自定義清單中刪除或使其過期。

雖然對服務沒有影響，但對某些使用者來說，可能收到不需要的警報。

如果您看到貴組織所需的自定義CA證書警報，且當前未包含在系統清單中，您可以聯絡相關CA獲取更新證書，並按照此處的最終使用手冊中的說明進行更換。

系統CA憑證套件組合會在升級後自動更新，且自訂清單中的憑證到期不會影響系統清單中的憑證的使用。

要驗證是否同時啟用系統清單和自定義清單，請導航到Network -> Certificates -> Certificate Authorities:編輯設定

您也可以從同一導航選單匯出系統和自定義清單，或使用CLI certconfig -> certauthority命令根據需要手動檢視兩個清單中的證書。

如果您希望刪除自定義CA清單中的證書生成警報，則下面是管理員使用SSH連線到裝置可以執行的步驟。

> **附註**：請根據警報確認自定義清單中的證書名稱/位置，因為警報可能與下面顯示的示例輸出不同。

```
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.
1. [AAA Certificate Services]
2. [ANCERT Certificados CGN]
3. [ANCERT Certificados Notariales]
4. [ANCERT Corporaciones de Derecho Publico]
5. [Actalis Authentication Root CA]
6. [Admin-Root-CA]
7. [Agence Nationale de Certification Electronique]
8. [Agence Nationale de Certification Electronique]
9. [America Online Root Certification Authority 1]
10. [America Online Root Certification Authority 2]
11. [Autoridad Certificadora Raiz de la Secretaria de Economia]
12. [Autoridad de Certificacion de la Abogacia]
13. [Baltimore CyberTrust Root]
```

```
14. [COMODO Certification Authority]
15. [COMODO RSA Certification Authority]
16. [Certipost E-Trust TOP Root CA]
17. [Certum CA]
18. [Chambers of Commerce Root]
19. [Cisco Root CA 2048]
20. [ComSign Advanced Security CA]
21. [ComSign CA]
22. [ComSign Secured CA]
23. [Cybertrust Global Root]
24. [D-TRUST Root Class 2 CA 2007]
25. [D-TRUST Root Class 3 CA 2007]
26. [DST Root CA X3]
27. [DigiCert Assured ID Root CA]
28. [DigiCert Baltimore CA-2 G2]
29. [DigiCert Global Root CA]
30. [DigiCert Global Root G2]
31. [DigiCert High Assurance EV Root CA]
32. [E-CERT ROOT CA]
33. [Echoworx Root CA2]
34. [Entrust Root Certification Authority - G2]
35. [Entrust Root Certification Authority]
36. [GLOBALTRUST]
37. [GeoTrust Global CA]
38. [GeoTrust Primary Certification Authority - G2]
39. [GeoTrust Primary Certification Authority - G3]
40. [GeoTrust Primary Certification Authority]
41. [GeoTrust RSA CA 2018]
42. [GeoTrust SSL CA - G2]
43. [GeoTrust Universal CA 2]
44. [GeoTrust Universal CA]
45. [Global Chambersign Root]
46. [GlobalSign PersonalSign 2 CA - SHA256 - G3]
47. [GlobalSign Root CA]
48. [GlobalSign]
49. [GlobalSign]
50. [Go Daddy Root Certificate Authority - G2]
51. [Hongkong Post Root CA 1]
52. [HydrantID SSL ICA G2]
53. [InfoNotary CSP Root]
54. [NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado]
55. [Network Solutions Certificate Authority]
56. [OISTE WISeKey Global Root GA CA]
57. [Post. Trust Root CA]
58. [QuoVadis Root CA 2]
59. [Root CA Generalitat Valenciana]
    <<<<<<<<<< Select this one based on sample alert above
60. [S-TRUST Authentication and Encryption Root CA 2005:PN]
61. [SSC Root CA A]
62. [SSC Root CA B]
63. [SSC Root CA C]
64. [Secure Global CA]
65. [SecureTrust CA]
66. [Serasa Certificate Authority III]
67. [Serasa Certificate Authority II]
68. [Serasa Certificate Authority I]
69. [Starfield Services Root Certificate Authority]
70. [SwissSign Gold CA - G2]
71. [SwissSign Platinum CA - G2]
72. [SwissSign Silver CA - G2]
73. [Swisscom Root CA 1]
74. [TC TrustCenter Class 2 CA II]
75. [TC TrustCenter Class 3 CA II]
76. [TC TrustCenter Class 4 CA II]
```

```
77. [TC TrustCenter Universal CA II]
78. [TC TrustCenter Universal CA I]
79. [TDC OCES CA]
80. [Trusted Certificate Services]
81. [UCA Global Root]
82. [UCA Root]
83. [USERTrust RSA Certification Authority]
84. [VAS Latvijas Pasts SSI(RCA)]
85. [VRK Gov. Root CA]
86. [VeriSign Class 3 Public Primary Certification Authority - G5]
87. [VeriSign Universal Root Certification Authority]
88. [Visa Information Delivery Root CA]
89. [Visa eCommerce Root]
90. [WellsSecure Public Root Certificate Authority]
91. [XRamp Global Certification Authority]
92. [thawte Primary Root CA - G3]
93. [thawte Primary Root CA] Select the custom ca certificate you wish 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
```

Please be sure to commit the change at the end.

相關資訊

-
-