在思科ISE上安裝、續訂和排除SSL數位證書故障

目錄

簡介

本文檔介紹SSL證書安裝、續訂以及針對身份服務引擎上觀察到的最常見問題的解決方案。

必要條件

需求

思科建議您瞭解以下主題：

- 身分識別服務引擎GUI

採用元件

本檔案中的資訊是根據以下軟體版本：

- 思科身分識別服務引擎2.7

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

本檔案提供建議的步驟和常見問題核對表，在您開始進行故障排除和致電思科技術支援之前，需先驗證和解決。

證書是一種電子文檔，用於標識個人、伺服器、公司或其他實體，並將該實體與公鑰相關聯。

自簽名證書由其自己的建立者簽名。證書可以由外部證書頒發機構(CA)自簽名或數位簽章。

CA簽名的數位證書被視為行業標準，並且更安全。

證書用於網路中，以提供安全訪問。

思科ISE使用證書進行節點間通訊，以及與外部伺服器(如系統日誌伺服器、源伺服器和所有終端使用者門戶（訪客、發起人和個人裝置門戶）進行通訊。

證書標識到終端的Cisco ISE節點，並保護該終端與Cisco ISE節點之間的通訊。

證書用於所有HTTPS通訊和可擴展身份驗證協定(EAP)通訊。

本檔案提供建議的步驟和常見問題核對表，在您開始進行故障排除和致電思科技術支援之前，需先驗證和解決。

這些解決方案直接來自思科技術支援已解決的服務請求。 如果您的網路正在作用，請確保您已瞭解為解決這些問題所採取的步驟的潛在影響。

設定

以下指南介紹了如何匯入和更換證書：

匯入系統證書

https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/workflow/html/b_basic_setup_2_7.html#ID547

替換到期的證書

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116977-technote-ise-cert-00.html#anc5

常見問題

場景1：無法替換ISE節點上即將到期的門戶證書

錯誤

將新門戶證書與CSR繫結時，證書繫結進程失敗，錯誤如下所示：

內部錯誤。要求您的ISE管理員檢查日誌以瞭解詳細資訊

此錯誤的最常見原因如下：

— 新證書的使用者名稱與現有證書相同

— 匯入使用現有證書的同一私鑰的續訂證書

解決方案

1. 將門戶使用臨時分配給同一節點上的另一個證書
2. 刪除即將到期的門戶證書
3. 安裝新的門戶證書，然後分配門戶使用情況

例如，如果您要將門戶使用臨時分配給使用EAP身份驗證的現有證書，請執行以下步驟：

步驟 1.選擇並編輯使用EAP身份驗證的證書，在Usage和Save下新增門戶角色

步驟 2.刪除即將到期的門戶證書

步驟 3.上傳新的門戶證書，而不選擇任何角色（在「使用」下）並提交

步驟 4.選擇並編輯新的門戶證書，在Usage and Save下分配門戶角色

場景2：無法生成具有多用途使用率的同一ISE節點的兩個CSR

錯誤

為具有多用途用途的同一節點建立新CSR失敗，錯誤為：
已存在另一個具有相同友好名稱的證書。友好名稱必須是唯一的。

解決方案

每個ISE節點的CSR友好名稱均採用硬式編碼，因此不允許為具有多用途用途的同一節點建立2個

CSR。使用案例位於特定節點上，有一個用於管理員和EAP身份驗證使用的CA簽名證書和另一個用於SAML和門戶使用的CA簽名證書，兩個證書都將過期。

在此情況中：

步驟 1.生成具有多用途使用率的第一個CSR

步驟 2.將CA簽名的證書與第一個CSR繫結，並分配Admin和EAP身份驗證角色

步驟 3.生成具有多用途使用的第二個CSR

步驟 4.將CA簽名的證書與第二個CSR繫結並分配SAML和門戶角色

方案3：無法繫結用於門戶的CA簽名證書，或者無法將門戶標籤分配給證書並出現錯誤

錯誤

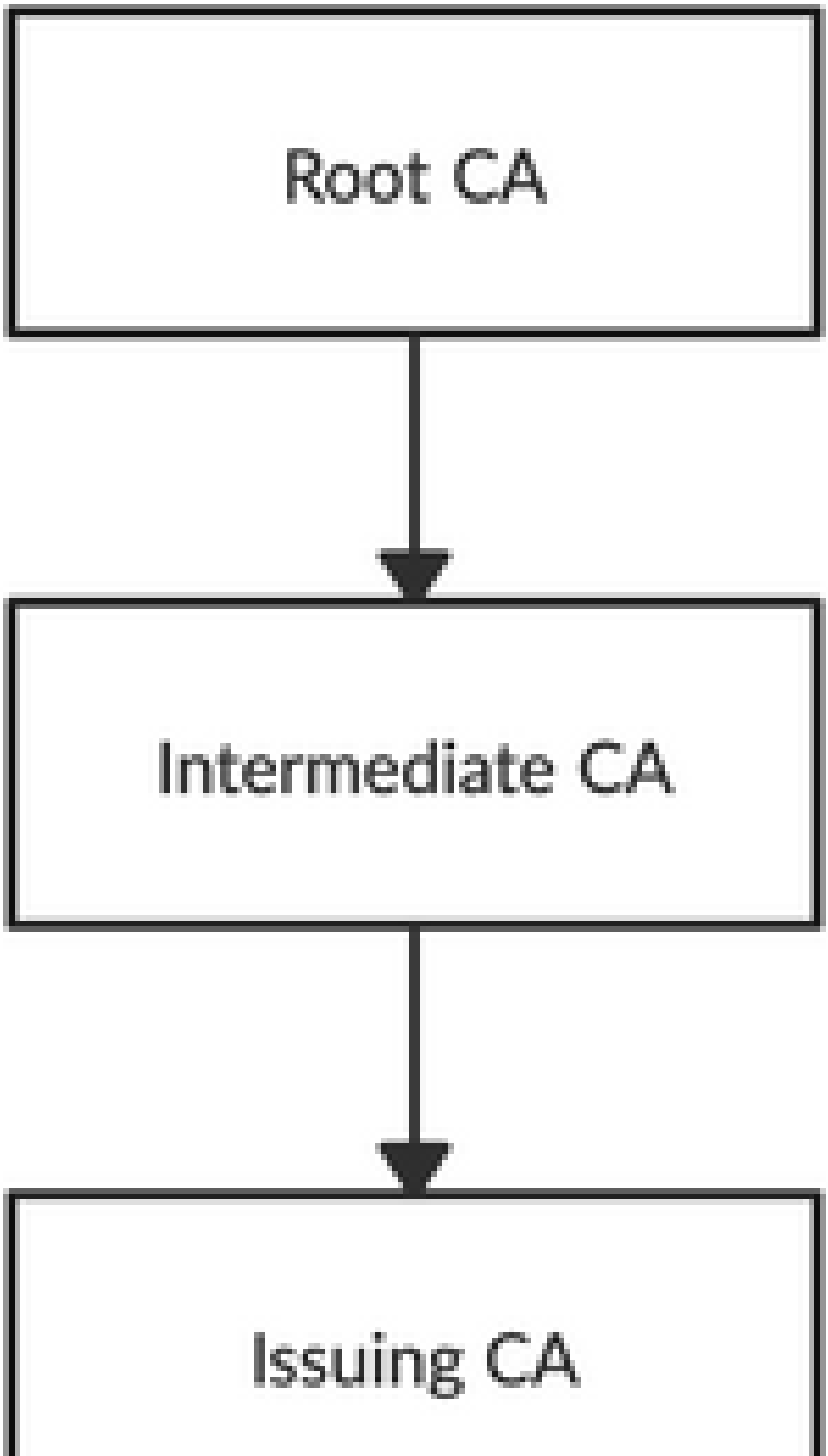
為門戶使用繫結CA簽名的證書引發錯誤：

存在一個或多個受信任證書，這些證書屬於門戶系統證書鏈或選擇具有基於證書的管理身份驗證角色，其主題名稱相同，但序列號不同。匯入/更新已中止。若要成功匯入/更新，您需要從重複的受信任證書中禁用基於購物車的管理員身份驗證角色，或者從鏈中含有重複的受信任證書的系統證書中更改門戶角色。

解決方案

步驟 1.檢查CA簽名證書的證書鏈（用於門戶使用）並在受信任的證書儲存中，驗證證書鏈中是否有重複的證書。
步驟 2.刪除重複證書，或從重複證書中取消選中Trust for certificate-based admin authentication覈取方塊。

例如，CA簽名的門戶證書具有以下證書鏈：


Root CA
Intermediate CA
Issuing CA

不允許禁用或刪除或信任證書，因為正在遠端日誌記錄目標下的系統證書和/或安全系統日誌目標中引用該證書。

解決方案

1. 驗證已過期的預設自簽名證書是否未與任何現有遠端日誌記錄目標關聯。可以在Administration > System > Logging > Remote Logging Targets > Select and Edit SecureSyslogCollector(s)下驗證這一點
2. 驗證已過期的預設自簽名證書是否未與任何特定角色（用法）相關聯。可以在管理>系統>證書>系統證書下驗證這一點。

如果問題仍然存在，請聯絡TAC。

場景5：無法將CA簽名的pxGrid證書與ISE節點上的CSR繫結

錯誤

將新的pxGrid證書與CSR繫結時，證書繫結進程失敗，出現錯誤：

pxGrid的證書必須在擴展金鑰使用(EKU)擴展中包含客戶端和伺服器身份驗證。

解決方案

確保CA簽名的pxGrid證書必須具有TLS Web伺服器身份驗證(1.3.6.1.5.5.7.3.1)和TLS Web客戶端身份驗證(1.3.6.1.5.5.7.3.2)擴展金鑰用法，因為它用於客戶端和伺服器身份驗證（以保護pxGrid客戶端和伺服器之間的通訊）

參考連結：https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_011010.html

方案6：由於現有LDAP或SCEP RA配置檔案配置，無法從受信任的證書儲存中刪除已過期的預設自簽名證書

錯誤

從受信任的證書儲存中刪除已過期的預設自簽名證書將導致以下錯誤：

無法刪除信任證書，因為正在其他位置引用該證書，可能是從SCEP RA配置檔案或LDAP身份源

*預設自簽名伺服器證書

要刪除證書，請刪除SCEP RA配置檔案或編輯LDAP身份源以不使用此證書。

解決方案

1. 導航到管理>身份管理>外部身份源> LDAP >伺服器名稱>連線
2. 確保LDAP伺服器根CA未使用「預設自簽名伺服器證書」
3. 如果LDAP伺服器未使用安全連線所需的證書，請導航到Administration > System > Certificates > Certificate Authority > External CA Settings > SCEP RA Profiles
4. 確保任何SCEP RA配置檔案未使用預設自簽名證書

其他資源

如何安裝萬用字元憑證
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

管理ISE證書
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

在ISE上安裝第三方CA證書
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/200295-Install-a-3rd-party-CA-certificate-in-IS.html

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。