對Umbrella整合訪問期間的證書過期錯誤進行故障排除

目錄

簡介

本文描述如何在Umbrella整合訪問s-platform.api.opendns.com或fireeye.vendor.api.opendns.com時排除證書過期錯誤。

問題

使用某些第三方客戶端的Umbrella整合可能會失敗，在s-platform.api.opendns.com and fireeye.vendor.api.opendns.com上驗證Umbrella API伺服器的數位證書時出錯。錯誤文本或代碼因整合中使用的客戶端程式而異，但通常表示存在過期的證書。

原因

此問題不是由伺服器的證書引起的，該證書當前有效。相反，此問題是由客戶端使用的過期證書信任儲存導致的。

為s-platform.api.opendns.com和fireeye.vendor.api.opendns.com提供服務的Web伺服器使用由證書頒發機構Let's Encrypt的中間證書R3頒發的數位證書（即數位簽章）。R3使用公鑰進行簽名，該公鑰在 Let Encrypt提供的SRG根X1根證書，以及較舊的SRG根X1交叉簽名版本。因此，存在兩個驗證路徑：一個終止於當前SRG根X1，另一個終止於交叉簽名版本(由證書頒發機構IdenTrust頒發的DST根CA X3證書)的頒發者。

可從Let's Encrypt取得核發圖表。此外，Qualys SSL Labs工具可用於檢視兩個「認證路徑」，其中包含各自的證書和證書詳細資訊，例如到期日期。

根證書儲存在客戶端系統上的一個或多個證書信任儲存中。2021年9月30日，DST根CA X3證書過期。自此日期起，在其信任儲存中具有DST根CA X3證書，但沒有較新的RG根X1根證書的客戶端，由於證書錯誤而無法連線到s-platform.api.opendns.com或fireeye.vendor.api.opendns.com。 錯誤消息或代碼可能表示證書已過期是錯誤的原因。過期的證書是客戶端信任儲存中的DST根CA X3證書，而不是API伺服器(s-platform.api.opendns.com和fireeye.vendor.api.opendns.com)的伺服器證書。

解析

要解決此問題，請更新客戶端的信任儲存以包含新的SRG根X1證書，該證書可從Let's Encrypt網站下載。（此頁面還提供用於測試客戶端的網站。）請參閱您的客戶端或作業系統的文檔，以獲取有關檢視和更新您客戶端的信任儲存的說明。如果官方更新包或自動更新機制可用，則這通常比手動更新信任儲存更可取。

如果使用新的SRG根X1證書手動更新信任儲存，我們還建議刪除過期的DST根CA X3證書，以防客戶機的驗證路徑生成代碼出現問題。從您的客戶端或作業系統的提供商處對信任儲存的正式更新可以新增SRG根X1並刪除DST根CA X3證書。

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）。