自動重新註冊到Cisco IOS CA的證書到期和自動註冊

目錄

簡介

所有數位證書在證書中都有內建的過期時間，該時間由證書頒發機構(CA)伺服器在註冊期間分配。當數位證書用於ISAKMP的VPN IPSec身份驗證時，將自動檢查通訊裝置的證書過期時間和裝置（VPN端點）上的系統時間。 這可確保使用的證書有效且未過期。這也是您必須*在*每個VPN端點（路由器）上設定內部時鐘的原因。 如果在VPN加密路由器上無法實現網路時間協定(NTP)（或簡單網路時間協定[SNTP]），則使用手動**set clock**命令。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於為該平台運行cXXXX-advsecurityk9-mz.123-5.9.T映像的所有路由器。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

數位證書何時被視為已過期或未過期？

- 如果系統時間在證書到期時間之後或證書的頒發時間之前，則證書已過期（無效）。

- 如果系統時間在證書的頒發時間和證書的過期時間之間或兩者之間，則證書未過期（有效）。

自動註冊功能的目的是為CA管理員提供一種機制，允許當前已註冊的路由器在路由器證書的生存期配置的百分比自動向其CA伺服器重新註冊。這是作為控制機制的證書的可管理性/可支援性的一項重要功能。如果您使用特定CA向可能有數千台在一年的生存期（無自動註冊）內使用的分支VPN路由器頒發證書，則在頒發的時間的恰好一年內，所有證書都將過期，並且所有分支都通過IPSec失去連線。或者，如果自動註冊功能設定為「自動註冊70」（如本例所示），則在已頒發證書的生存期（1年）的70%內，每台路由器都會自動向信任點中列出的Cisco IOS® CA伺服器發出新的註冊請求。

註：自動註冊功能的一個例外情況是，如果設定為小*於10*或等於10，則為分鐘。如果大*於10,*則為憑證生存期的百分比。

Cisco IOS CA管理員需要通過自動註冊注意一些警告。管理員需要執行以下操作才能成功重新註冊：

1. 在Cisco IOS CA伺服器上手動授予或拒絕每個重新註冊請求（除非在Cisco IOS CA伺服器上使用「授予自動」）。Cisco IOS CA伺服器仍需要授予或拒絕這些請求中的每一個（假設Cisco IOS CA未啟用「授予自動」）。 但是，註冊路由器上不需要執行任何管理操作即可開始重新註冊過程。
2. 如果適用，將重新註冊的新證書儲存在重新註冊的VPN路由器中。如果路由器中沒有待執行的未儲存配置更改，則新證書將自動儲存到非易失性RAM(NVRAM)。 新憑證將寫入NVRAM中，且先前憑證會移除。如果存在掛起的未儲存的配置更改，則必須在註冊路由器上發出**copy run start**命令，以便將配置更改和新重新註冊的證書儲存到NVRAM中。**copy run start**命令完成後，新證書將寫入NVRAM中，並且先前的證書將被刪除。**注意：**當新的重新註冊成功時，它不會在CA*服*務器上撤銷該已註冊裝置的先前證書。當VPN裝置通訊時，它們會相互傳送證書序列號（唯一編號）。**注意：例**如，如果您處於證書生命期的70%，並且VPN分支要重新註冊到CA，則該CA具有用於該主機名的兩個證書。但是，註冊路由器只有一個（較新的）。如果選擇這樣做，則可以通過管理方式撤銷舊證書，或允許其正常過期。**注意：**自動註冊功能的較新代碼版本有一個選項，可以「重新生成」用於註冊的金鑰對。此選項是「非預設」以重新生成金鑰對。如果選擇此選項，請注意思科錯誤ID CSCea90136。此錯誤修正允許將新金鑰對置於臨時檔案中，同時新證書註冊將在現有IPSec隧道（即使用舊金鑰對）上進行。自動註冊可以在證書續訂時生成新金鑰。目前，這會導致獲取新證書所需的時間內服務中斷。這是因為存在新金鑰，但沒有與其匹配的證書。在新證書可用之前，此功能將保留舊金鑰和證書。還實現了自動金鑰生成以進行手動註冊。系統根據需要，為自動或手動註冊生成金鑰。找到的版本 — 12.3PIH03要修復的版本 — 12.3T版本適用於 — 12.3PI03整合在 — 無如需其他資訊，請聯絡思科技術支援。

相關資訊

- IPSec支援頁面
- 技術支援 - Cisco Systems