使用AD證書服務建立Umbrella自定義根證書

目錄

簡介

本文檔介紹使用Microsoft Windows Active Directory(AD)證書服務建立自定義根證書的說明。

必要條件

需求

思科建議您瞭解以下主題：

- Microsoft當前支援的Microsoft Windows Server版本
- Windows伺服器上安裝的Active Directory證書服務
- 具有Active Directory證書服務和Web服務/Web註冊服務角色的帳戶
- 配置為使用UTF-8編碼(「UTF8STRING」)頒發證書的證書服務

採用元件

本檔案中的資訊是根據Cisco Umbrella。

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。

概觀

本文包含使用Microsoft Windows Active Directory證書服務建立自定義根證書(用於代替標準Cisco Umbrella根CA證書)，然後使用該根證書從Umbrella的客戶CA簽名的CA證書功能簽署證書簽名請求(CSR)的說明。

證書字串編碼

如果您的憑證服務設定為使用預設編碼(「PRINTABLESTRING」)，則產生的憑證鏈不能由某些Web使用者端（最明顯的是Firefox）信任。

Cisco Umbrella安全Web閘道代理使用使用UTF8STRING編碼字串的憑證鏈結。如果您的簽署憑證（例如根憑證）簽署CSR以建立Cisco Umbrella客戶CA中間憑證時使用PRINTABLESTRING編碼，則Cisco Umbrella客戶CA憑證的Subject欄位的編碼為PRINTABLESTRING。此編碼無法與Cisco Umbrella R1 CA中間證書中Issuer欄位的UTF8STRING編碼匹配，該欄位位於證書鏈的下一個。

RFC 5280第4.1.2.6節要求憑證鏈結在已發行憑證的Issuer欄位與發行憑證的Subject欄位之間維持相同的字串編碼：

"如果證書的主題是CA，則主題欄位的編碼方式必須與主題CA頒發的所有證書中頒發者欄位（第4.1.2.4節）的編碼方式相同。"

許多瀏覽器不執行此要求，但有些瀏覽器（最明顯的是Firefox）會執行此要求。因此，將安全Web閘道(SWG)與客戶CA簽名的CA憑證功能配合使用時，Firefox等Web使用者端可能會產生不受信任的站點錯誤，且不會載入網站。

要解決此問題，請使用不執行RFC 5280要求的瀏覽器（例如Chrome）。

步驟 1:準備AD證書服務模板

1.導航到開始>運行> MMC，開啟Active Directory證書頒發機構MMC。

2.選擇檔案>新增/刪除管理單元，然後新增證書模板和證書頒發機構管理單元。選擇OK。

3.展開證書模板，然後按一下右鍵下屬證書頒發機構。按一下複製模板。

現在，您可以建立一個自定義證書模板，以符合Umbrella文檔中列出的要求。

以下是本文建立時詳細介紹的要求：

- 「常規」頁籤
  - 請為模板指定一個對您有意義的名稱。
  - 將「有效期」設置為35個月（3年減一個月）。
  - 將續訂期間設置為20天。
- 擴展選項卡
  - 按兩下「Basic Constraints(基本約束)」。
    - 確保選中Make this extension critical。
  - 在金鑰用法下：
    - 確保選中Certificate Signing&CRL Signing。
    - 取消選擇數位簽章。
    - 確保在此處也勾選此擴展為關鍵。
- 選擇Apply和OK

步驟 2:發佈模板

1.返回到在上一個進程的步驟2中設定的MMC中，展開Certificate Authority部分。

2.在新展開的部分中，按一下右鍵Certificate Templates資料夾，然後選擇New > Certificate Template to Issue。

3.在新視窗中，選擇在上一節中建立的證書模板的名稱，然後選擇確定。

CA現在已準備好協助該請求。

步驟 3:下載並簽名CSR

1.登入您的Umbrella Dashboard(https://dashboard.umbrella.com)。

2.導航到部署>配置>根證書。

3.選擇角中的Add(+)圖示，並在新視窗中命名您的CA。

4.下載憑證簽署請求(CSR)。

5.在新瀏覽器頁籤中，導航到Active Directory證書服務的Web服務。(如果您使用的是本地電腦，則應為127.0.0.1/certsrv/或類似設定。)

6.在新頁面中，選擇請求證書。

7.選擇Advanced Certificate Request。

8.在已儲存的請求下，複製並貼上您在步驟4中下載的CSR的內容（您必須使用文字編輯器將其開啟）。

9.在「Certificate Template」下，選擇在「Preparing AD Certificate Services Template」部分中建立的證書模板的名稱，然後選擇Submit。

10.請務必選擇Base64 Encoded，然後選擇Download Certificate，並記下.cer檔案的位置。

步驟 4:上傳簽名的CSR（和公共根證書）

1.在Umbrella Dashboard上，導航到Deployment > Configuration > Root Certificate。

2.選擇您在上一節的步驟3中建立的根證書。

3.選擇行右下角的Upload CA*。

4.選擇頂端瀏覽按鈕(證書頒發機構（簽名的CSR）)。

5.瀏覽到在上一節中建立的.cer檔案的位置，然後選擇Save。

6.選擇下一步，然後選擇要將證書用於其中的電腦/使用者組（而不是思科根證書），然後選擇儲存。

*您也可以選擇上傳CA憑證。可以從證書頒發機構伺服器的Web介面(http://127.0.0.1/certsrv/)中檢

索該證書，然後選擇下載CA證書、證書鏈或CRL。完成螢幕提示在Base 64中「下載CA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）。