驗證安全雲控制中的域 — CUI更新

目錄

簡介

本檔案將說明思科整合身分(CUI)更新後安全雲端控制(SCC)中新增的網域驗證方式。

背景

在思科安全雲控制(SCC)中宣告和驗證域時，管理員需要發佈DNS TXT記錄來證明域的所有權。

問題

成功驗證所需的DNS記錄位置發生更改。思科文檔中引用的先前說明使用專用的驗證子域：

_cisco-sxso-verification.example.com

但是，當前驗證過程需要將Cisco提供的TXT驗證令牌直接發佈到根域下，而不是發佈專用驗證子域。

發生了什麼變化？

以前的配置（不再適用於當前驗證工作流）：

DNS欄位	價值
記錄型別	TXT
主機/名稱	_cisco-sxso-verification.example.com
價值	思科驗證權杖

新配置（必需）：

DNS欄位	價值
記錄型別	TXT
主機/名稱	@
價值	思科驗證權杖

解決方案

實施步驟

1. 登入您的域DNS提供程式（GoDaddy、Cloudflare、Route 53、Azure DNS等）。
2. 導航到域的DNS管理。
3. 建立新的TXT記錄。
4. 按如下方式配置記錄：
   Type:TXT
   主機/名稱：@
   值：貼上由Cisco SCC生成的驗證令牌。
   TTL:預設值。
5. 儲存DNS記錄並為DNS傳播留出時間。
6. 返回Cisco SCC並點選Verify。

驗證

您可以使用此命令確認正確發佈了TXT記錄：

```
dig TXT example.com
```

響應必須包含思科驗證令牌。

一旦在DNS中看到該記錄，請返回SCC並重試域驗證。

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）。