

配置Umbrella VA以接收使用者 — IP對映

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[虛擬裝置](#)

[向VA新增私鑰和證書](#)

[向VA新增證書](#)

[在VA上啟用HTTPS](#)

[驗證HTTPS啟用](#)

[Active Directory](#)

[Umbrella Android使用者端](#)

[Umbrella Chromebook使用者端](#)

[配置順序](#)

簡介

本文檔介紹如何配置Cisco Umbrella虛擬裝置(VA)以通過安全通道接收使用者 — IP對映。

必要條件

需求

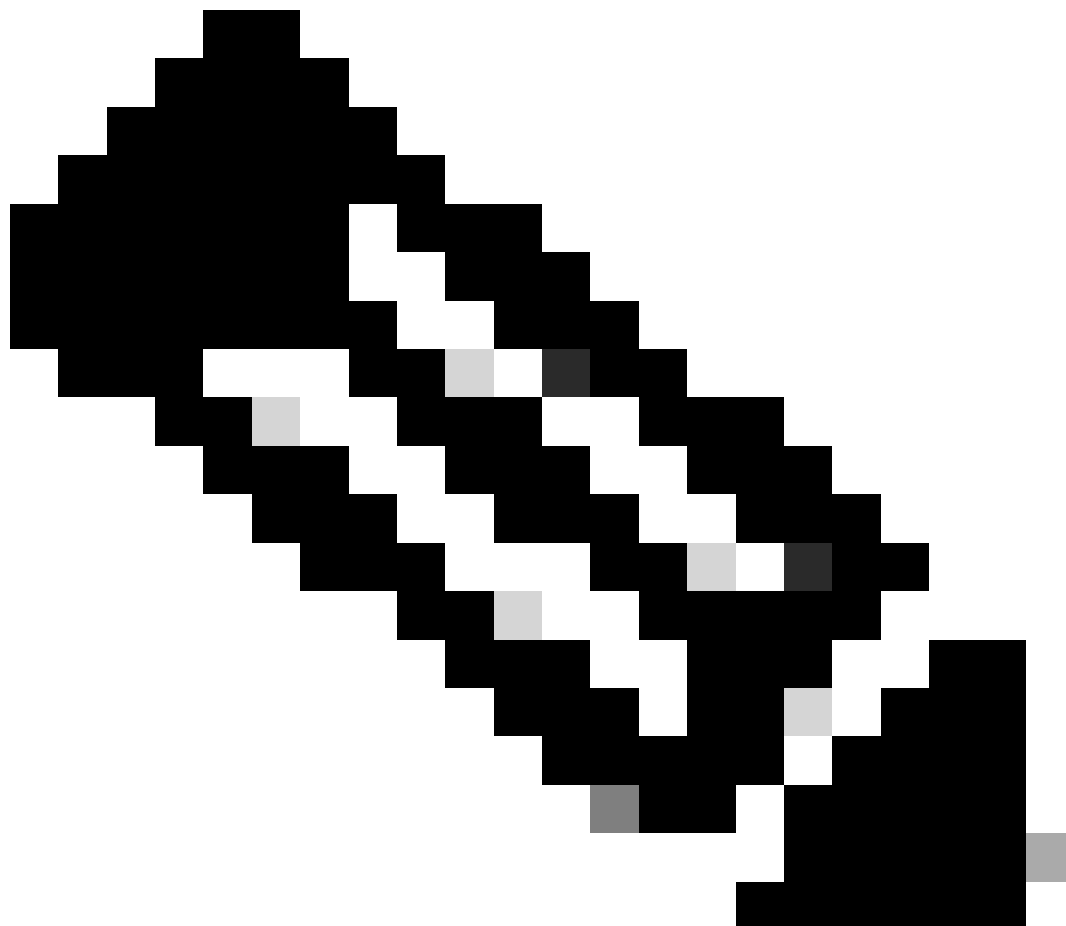
思科建議您瞭解以下主題：

- 私鑰建立、證書建立、證書簽名和管理不在Umbrella元件的範圍內。這必須在這些元件的外部執行。
- 您必須為每個虛擬裝置建立一個具有唯一公用名稱的證書。
- 您還必須在內部DNS伺服器中新增一個A記錄，將此公用名稱指向虛擬裝置的IP地址。
- 如果需要更改虛擬裝置的IP地址，也必須相應地更改此A記錄。
- 與證書對應的FQDN必須配置為Umbrella控制面板上的本地域，以便VA將此域識別為本地域。
 -
- 需要分別以.key和.cer格式建立私鑰和證書。
- 您可以為此使用自簽名證書或CA簽名證書。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行版本2.7或更高版本的虛擬裝置
 - Umbrella AD聯結器必須運行版本1.5或更高版本
 - Umbrella Chromebook客戶端必須運行版本1.3.3或更高版本
-



附註：如果您的VA或AD聯結器運行的是以前的版本，則可以使用[Umbrella開啟支援票證](#)，以將其升級到相應的支援版本。

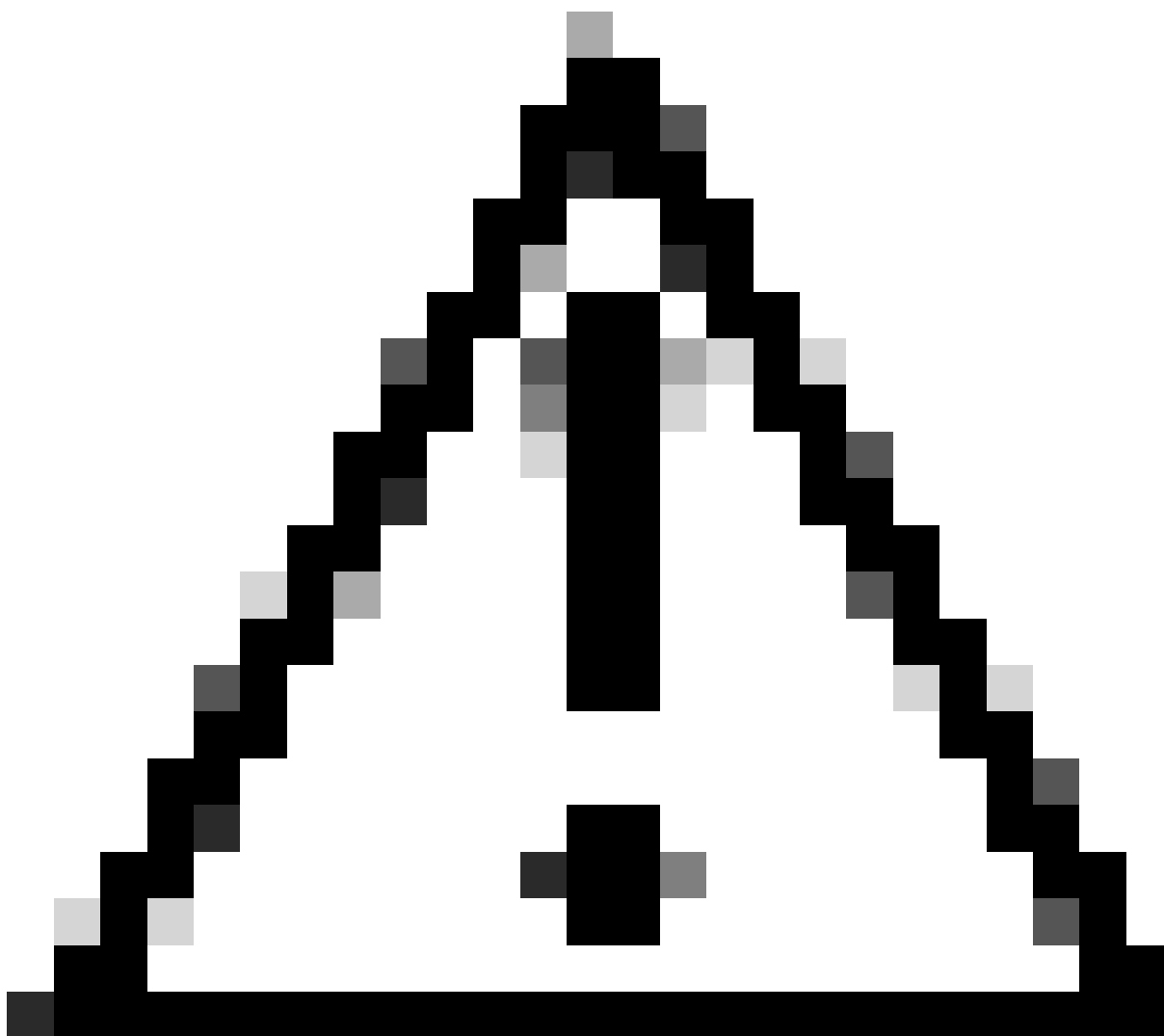
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

運行版本2.6或更低版本的Umbrella虛擬裝置支援在埠443上僅以未加密的形式接收來自Umbrella Active Directory(AD)聯結器和使用者的IP對映。因此，部署的一個必備條件是AD聯結器和VA或Chromebook客戶端與VA只能通過受信任的網路進行通訊。

從版本2.7開始，Umbrella虛擬裝置現在可以通過HTTPS從AD聯結器接收AD使用者 — IP對映，也可以通過HTTPS從每個Umbrella Chromebook客戶端接收類似的GSuite使用者 — IP對映。

本文詳細介紹每個元件上啟用HTTPS通訊的配置步驟。預設情況下，HTTPS通訊被禁用，並且AD聯結器和Chromebook客戶端僅通過HTTP與VA通訊。



注意：啟用此功能會增加VA和Umbrella AD聯結器上的CPU和記憶體利用率，並會導致VA的DNS吞吐量降低。因此，建議僅在您的組織符合性要求時啟用此功能。

虛擬裝置

向VA新增私鑰和證書

將私鑰和證書新增到VA的步驟：

- 1.通過文本編輯器開啟私鑰檔案。
- 2.選擇「全部」、「複製」，然後貼上此命令的雙引號：

```
config va ssl key "paste the contents of the .key file here"
```

向VA新增證書

將證書新增到VA的步驟：

- 1.通過文本編輯器開啟證書檔案。
- 2.選擇「全部」、「複製」，然後貼上下面命令的雙引號：

```
config va ssl cert "paste the contents of the .crt file here"
```

在VA上啟用HTTPS

使用以下命令在VA上啟用HTTPS:

```
config va ssl enable
```

驗證HTTPS啟用

使用以下命令驗證是否已啟用HTTPS:

```
config va show
```

此命令的輸出可包括HTTPS狀態以及SSL證書詳細資訊。

輸出示例：

```
HTTPS status : enabled
SSL Certificate Start Time : 2024-04-16 16:11:08
SSL Certificate Expiry Time : 2025-04-16 16:11:08
Issuer : C = US, ST = MASSACHUSETTS, L = BOSTON, O = CISCO SUPPORT, CN = server.domain.com
Common Names : vmhost.domain.com
```

VA可能需要20分鐘才能開始通過HTTPS接收事件。大約過20分鐘後，可以使用`config va status`命令檢查。AD聯結器的狀態在中間時段處於黃色（停止）狀態，並且在VA開始通過HTTPS接收事件後變為綠色狀態。

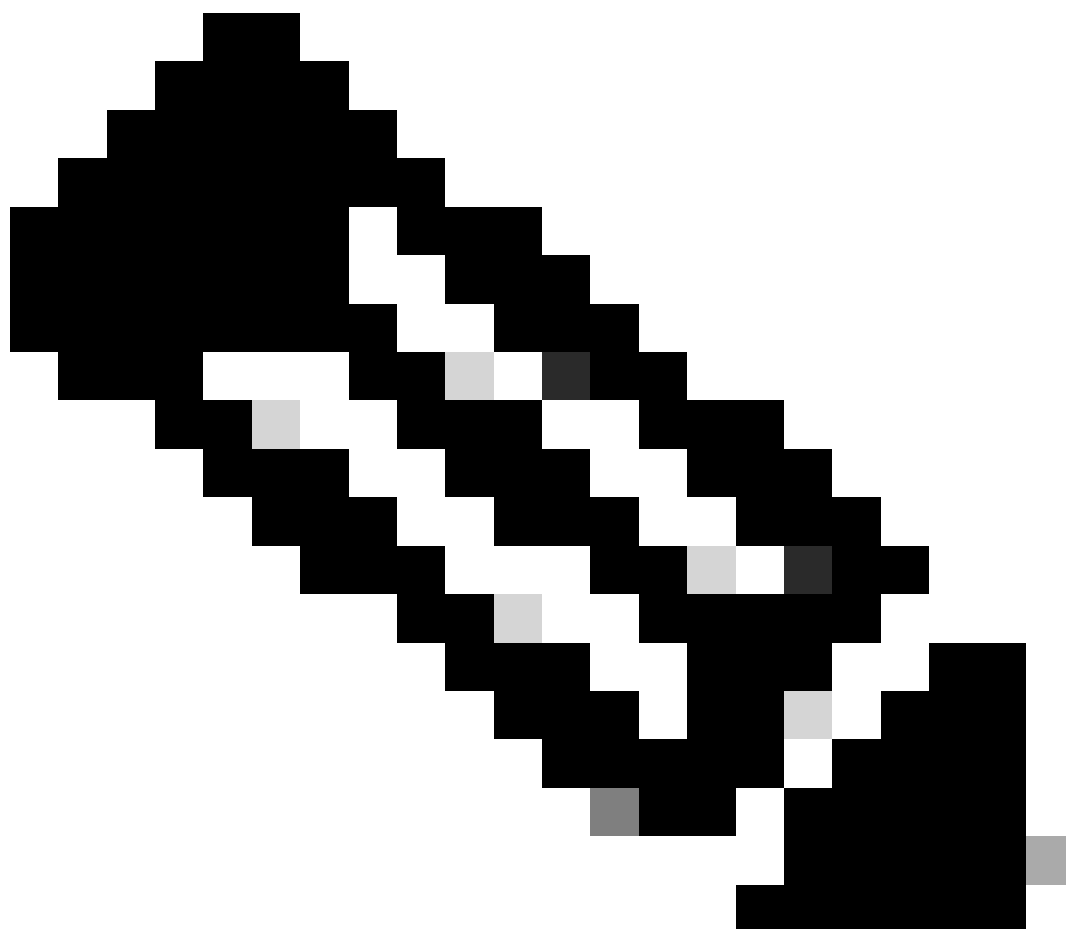
如果要停用HTTPS並恢復為HTTP，請使用命令`config va ssl disable`。

如果要重新啟用HTTPS，必須再次新增私鑰和證書，然後使用`config va enable`命令。

Active Directory

如果對每個VA使用CA簽名的證書，請確保在運行AD聯結器的每個系統上安裝根證書和每個VA證書的頒發CA證書，該系統與VA位於同一站點。

如果對每個VA使用自簽名證書，請確保每個VA證書安裝在運行AD聯結器的每個系統上，該系統與VA位於同一Umbrella站點。



附註：僅需要在AD聯結器上安裝與AD聯結器位於同一Umbrella站點中的VA的證書。

VA最多可能需要20分鐘才能將HTTPS狀態同步到Umbrella，然後將其同步到AD聯結器。因此，聯結器開始通過HTTPS向VA傳送資料可能需要長達20分鐘。VA會丟棄在此期間傳送的任何使用者 — IP對映。因此，建議僅在不需要使用者登入的停機時間內對VA進行配置更改。

Umbrella Android使用者端

如果您使用的是針對VA的CA簽名證書，請確保將根證書和針對每個VA證書的頒發CA證書推送到每個Android裝置並安裝在每台裝置上。

如果您為VA使用自簽名證書，請確保將每個VA證書推送到每個Android裝置並安裝在每個VA裝置上。

證書可用後，Umbrella Android客戶端可以開始使用此證書設定VA的HTTPS通道。

Umbrella Chromebook使用者端

如果您將由CA簽名的證書用於VA，請確保將根證書和每個VA證書的頒發CA證書推送到每個Chromebook並安裝在每個Chromebook上。

如果您將自簽名證書用於VA，請確保將每個VA證書推送到每個Chromebook並安裝在每個Chromebook上。

證書可用後，Umbrella Chromebook客戶端可以開始使用此證書設定VA的HTTPS通道。

有關詳細資訊，請參閱Umbrella Chromebook Client: 一文通過安全通道將使用者 — IP對映傳送到Umbrella虛擬裝置。

配置順序

在VA上啟用HTTPS後，VA不接受通過HTTP以明文傳送的使用者 — IP對映。因此，通過HTTP傳送的任何使用者登入都會被丟棄，並且這些使用者的DNS請求的使用者屬性不可用。因此，建議按以下順序配置這些元件：

- 1.根據CA簽名或自簽名證書為每個VA建立證書和私鑰。
- 2.將證書和私鑰分別新增到每個VA。
- 3.確保每個VA證書（或VA自簽名證書）的根證書和中間父證書安裝在與VA在同一站點中運行AD聯結器的每個系統上，以及安裝在每個Chromebook上。
- 4.在停機時間內，在虛擬助理上啟用HTTPS。



附註：VA上的證書必須在過期之前被替換，並且中間父級和根證書必須安裝在AD聯結器和Umbrella Chromebook客戶端上。如果未執行此操作，則AD聯結器和Umbrella Chromebook客戶端無法與VA通訊。

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）。