ユーザIPマッピングを受信するためのUmbrella VAの設定

内容

はじめに

このドキュメントでは、セキュアチャネル経由でユーザIPマッピングを受信するようにCisco Umbrella仮想アプライアンス(VA)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 秘密キーの作成、証明書の作成、証明書の署名および管理は、Umbrellaコンポーネントの範囲外です。これは、これらのコンポーネントの外部で行う必要があります。
- 仮想アプライアンスごとに、一意の共通名を持つ証明書を1つ作成する必要があります。
- また、この共通名を仮想アプライアンスのIPアドレスにポイントするように、内部DNSサーバにAレコードを追加する必要があります。
- 仮想アプライアンスのIPアドレスを変更する必要がある場合は、このAレコードもそれに応じて変更する必要があります。
- 証明書に対応するFQDNは、Umbrellaダッシュボードでローカルドメインとして設定する必

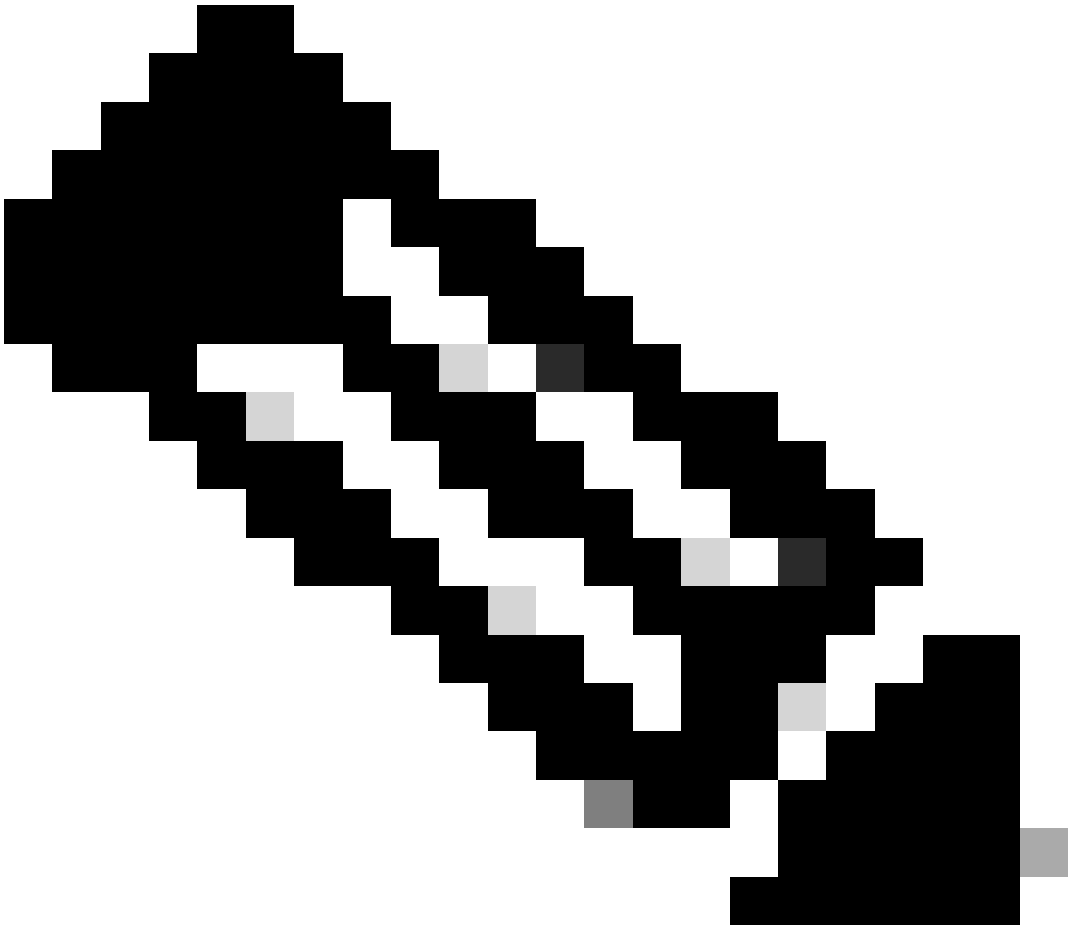
要があります。これにより、VAはこれをローカルドメインとして認識します。

- 秘密鍵と証明書は、それぞれ.key形式と.cer形式で作成する必要があります。
- この目的には、自己署名証明書またはCA署名付き証明書を使用できます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン2.7以降を実行する仮想アプライアンス
- Umbrella ADコネクタは、バージョン1.5以降を実行している必要があります。
- Umbrella Chromebookクライアントは、バージョン1.3.3以降を実行している必要があります。



注：ご使用のVAまたはADコネクタが以前のバージョンを実行している場合、Umbrellaでサポートチケットを開いて対応するサポートバージョンにアップグレードすることができます。

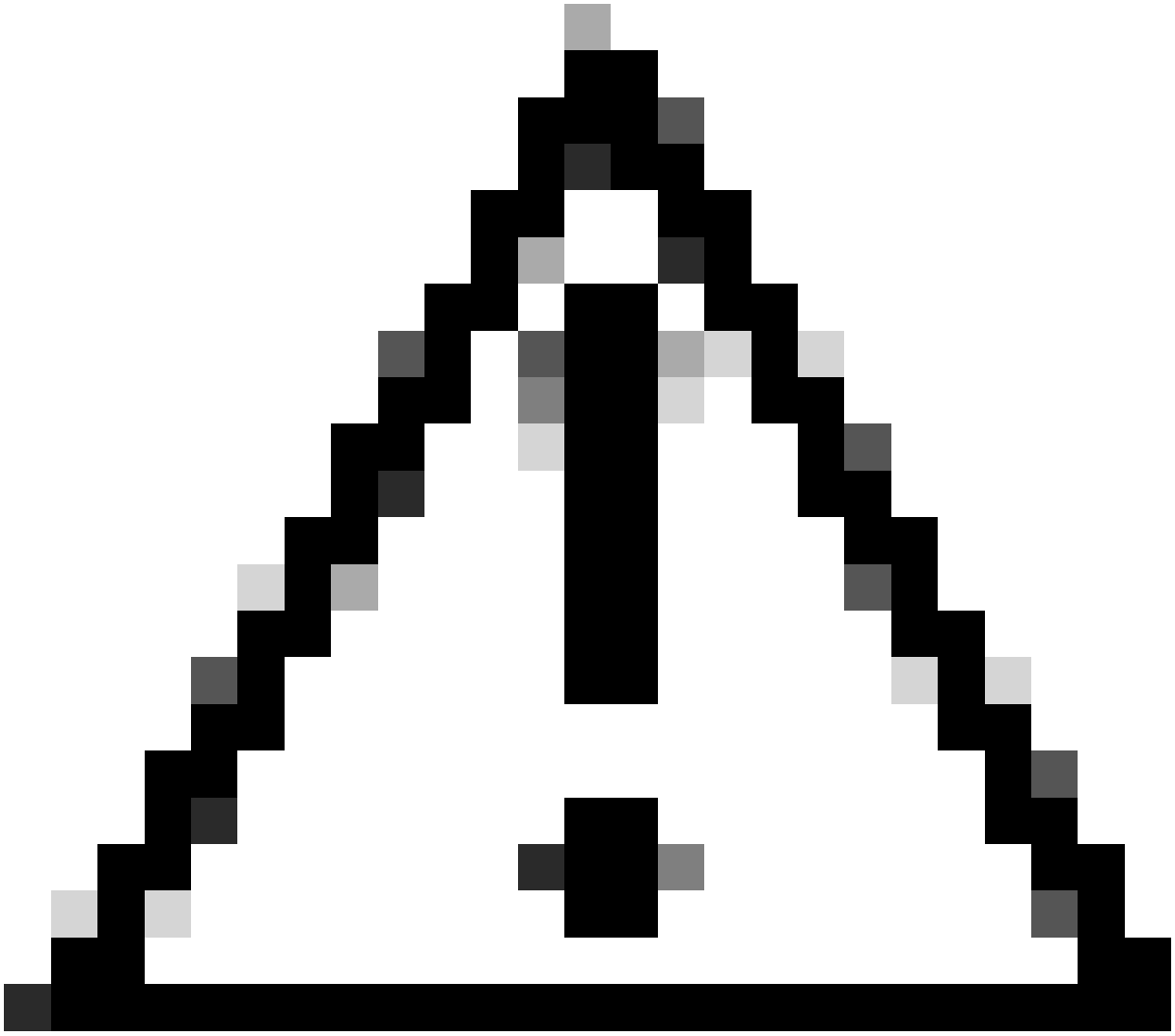
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

バージョン2.6以前を実行しているUmbrella仮想アプライアンスは、Umbrella Active Directory(AD)コネクタからユーザIPマッピングを受信し、ポート443で暗号化されていない形式のUmbrella Chromebookクライアントのみをサポートします。その結果、ADコネクタとVA、またはChromebookクライアントとVAは、信頼できるネットワーク上でのみ通信することが導入の必須条件となっています。

バージョン2.7以降、Umbrella仮想アプライアンスは、ADコネクタからHTTPS経由でADユーザIPマッピングを受信できるようになりました。同様に、各Umbrella Chromebookクライアントから HTTPS経由でADユーザIPマッピングを送信できるようになりました。

この記事では、HTTPS通信を有効にするための各コンポーネントの設定手順について詳しく説明します。デフォルトでは、HTTPS通信は無効で、ADコネクタとChromebookクライアントは HTTP経由でのみVAと通信します。



注意：この機能をオンにすると、VAおよびUmbrella ADコネクタのCPUとメモリの使用率が増加し、VAのDNSスループットが低下する可能性があります。したがって、組織のコンプライアンス要件によって義務付けられている場合にのみ、この機能を有効にすることを推奨します。

仮想アプライアンス

VAへの秘密キーと証明書の追加

秘密キーと証明書をVAに追加するには、次の手順を実行します。
1. テキストエディタで秘密キーファイルを開きます。

2. 「すべて」を選択し、コピーして、このコマンドの二重引用符に貼り付けます。

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

VAへの証明書の追加

証明書をVAに追加するには、次の手順を実行します。
1. テキストエディタで証明書ファイルを開きます。

2. 「すべて」を選択し、コピーして、次のコマンドの二重引用符に貼り付けます。

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

VAでHTTPSを有効にする

次のコマンドを使用して、VAでHTTPSを有効にします。

```
config va ssl enable
```

HTTPSの有効化の確認

次のコマンドを使用して、HTTPSが有効になっていることを確認します。

```
config va show
```

このコマンドの出力には、HTTPSステータスやSSL証明書の詳細が含まれます。

出力例：

```
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 = CISCOSUPPORT, CN = server.domain.com
Common Names : vmhost.domain.com
```

VAがHTTPS経由でイベントを受信し始めるまでに、最大で20分かかることがあります。`config va status`コマンドを使用して、約20分後に確認できます。ADコネクタのステータスは、中間期間は黄色（ストール）状態で、VAがHTTPS経由でイベントの受信を開始すると緑色の状態に移行します。

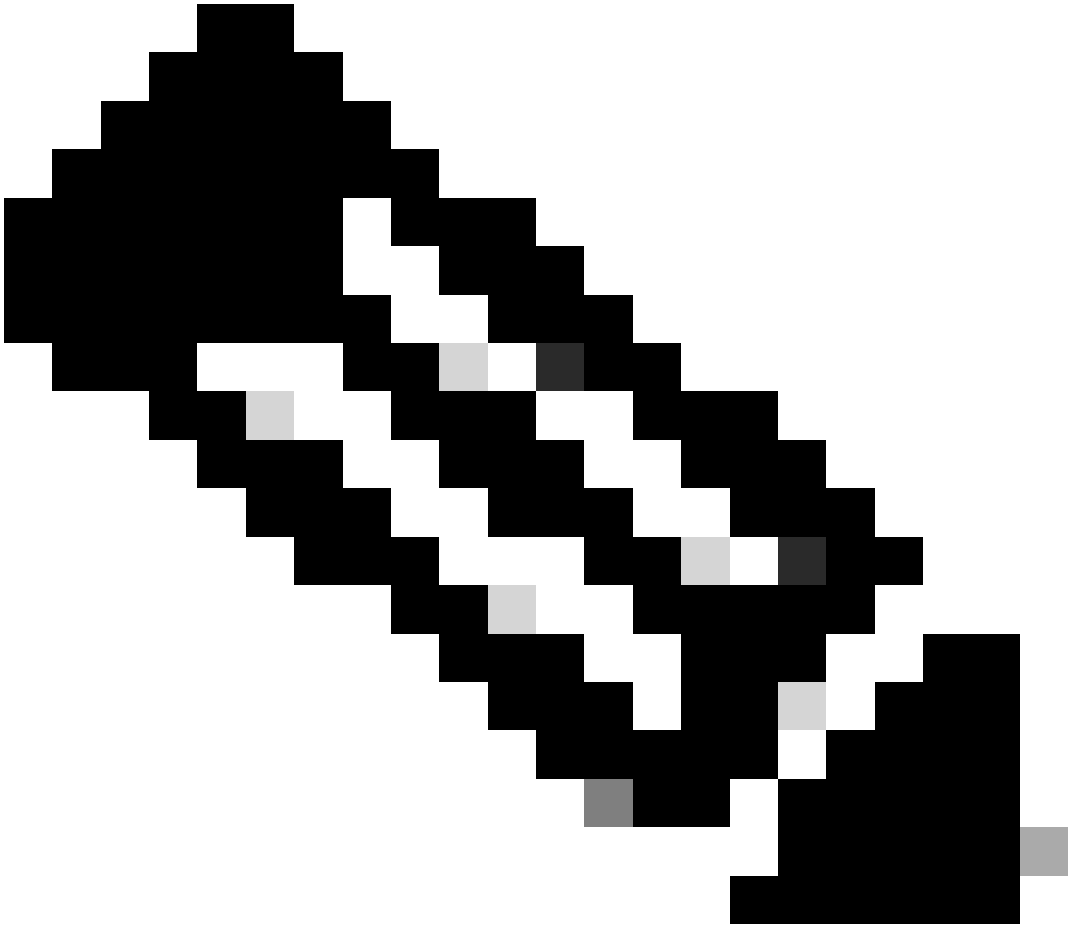
HTTPSを無効にしてHTTPに戻すには、`config va ssl disable`コマンドを使用します。

HTTPSを再度有効にする場合は、秘密キーと証明書を再度追加してから、`config va enable`コマンドを使用する必要があります。

Active Directory

各VAに対してCA署名付き証明書を使用している場合は、ルート証明書と各VA証明書の発行側CA証明書が、VAと同じサイト内のAD Connectorを実行している各システムにインストールされていることを確認します。

各VAに自己署名証明書を使用している場合は、各VA証明書が、VAと同じUmbrellaサイト内のADコネクタを実行している各システムにインストールされていることを確認します。



> 注:ADコネクタにインストールする必要があるのは、ADコネクタと同じUmbrellaサイトにあるVAの証明書だけです。

VAがHTTPSステータスをUmbrellaに同期し、AD Connectorに同期されるまでに最大で20分かかることがあります。その結果、コネクタがHTTPS経由でVAにデータを送信し始めるまでに最大

20分かかる場合があります。この間に送信されたユーザIPマッピングは、VAによって破棄されます。したがって、VAの設定の変更は、ユーザログインが予期されないダウンタイム時にのみ行うことをお勧めします。

Umbrella Androidクライアント

VA用のCA署名付き証明書を使用している場合は、各VA証明書のルート証明書と発行側CA証明書が各Androidデバイスにプッシュされてインストールされていることを確認します。

VAの自己署名証明書を使用している場合は、各VA証明書がにプッシュされ、各Androidデバイスにインストールされていることを確認します。

証明書が使用可能になると、Umbrella Androidクライアントはこの証明書を使用してVAとのHTTPSチャネルの設定を開始できます。

Umbrella Chromebookクライアント

VA用にCA署名付き証明書を使用している場合は、各VA証明書のルート証明書と発行側CA証明書が各Chromebookにプッシュされ、インストールされていることを確認します。

VAに自己署名証明書を使用している場合は、各VA証明書が各Chromebookにプッシュされ、インストールされていることを確認します。

証明書が使用可能になると、Umbrella Chromebook Clientはこの証明書を使用してVAとのHTTPSチャネルの設定を開始できます。

詳細については、『Umbrella Chromebookクライアント：Umbrella仮想アプライアンスへのセキュアチャネル経由でのユーザIPマッピングの送信』を参照してください。

設定シーケンス

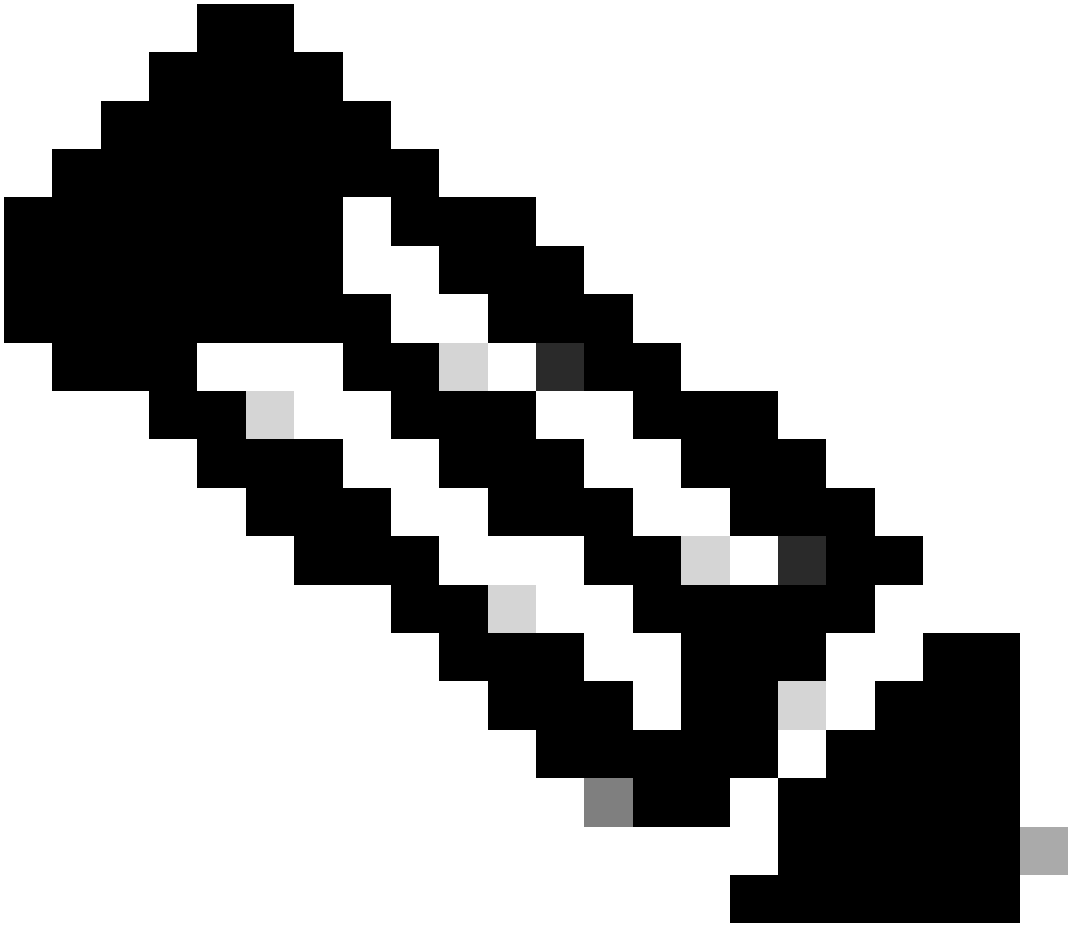
VAでHTTPSが有効になると、VAはHTTP経由でプレーンテキストに送信されたユーザIPマッピングを受け入れません。その結果、HTTP経由で送信されたユーザログインはすべて破棄され、これらのユーザからのDNS要求に対するユーザ属性は使用できなくなります。したがって、次のコンポーネントをこの順序で設定することを推奨します。

1. CA署名付き証明書または自己署名証明書に基づいて、各VAの証明書および秘密キーを作成します。

2. 証明書と秘密キーを各VAにそれぞれ追加します。

3. 各VA証明書（またはVA自己署名証明書）のルート証明書と中間親証明書が、VAと同じサイト内のADコネクタを実行している各システムと各Chromebookにインストールされていることを確認します。

4. ダウンタイム時には、VAでHTTPSを有効にします。



注：有効期限が切れる前にVAの証明書を交換し、ADコネクタとUmbrella Chromebook Clientに中間の親およびルート証明書をインストールする必要があります。これを行わないと、ADコネクタとUmbrella Chromebook ClientがVAと通信できません。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。