Configuration de l'appliance virtuelle Umbrella pour recevoir les mappages utilisateur-IP

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Aperçu
- Appareil virtuel
  - Ajouter une clé privée et un certificat à l'appliance virtuelle
  - Ajouter un certificat à la VA
  - Activer HTTPS sur l'appliance virtuelle
  - Vérification de l'activation HTTPS
- Active Directory
- Client Android Umbrella
- Umbrella Chromebook Client
  - Séquence de configuration

Introduction

Ce document décrit comment configurer l'appliance virtuelle Cisco Umbrella pour recevoir des mappages utilisateur-IP sur un canal sécurisé.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La création de clés privées, la création de certificats, la signature et la gestion de certificats sont hors de portée des composants Umbrella. Cette opération doit être effectuée en dehors de ces composants.
- Vous devez créer un certificat avec un nom commun unique par appliance virtuelle.
- Vous devez également ajouter un enregistrement A dans votre serveur DNS interne, en pointant ce nom commun vers l'adresse IP de l'appliance virtuelle.
- Si l'adresse IP d'une appliance virtuelle doit être modifiée, cet enregistrement A doit également être modifié en conséquence.

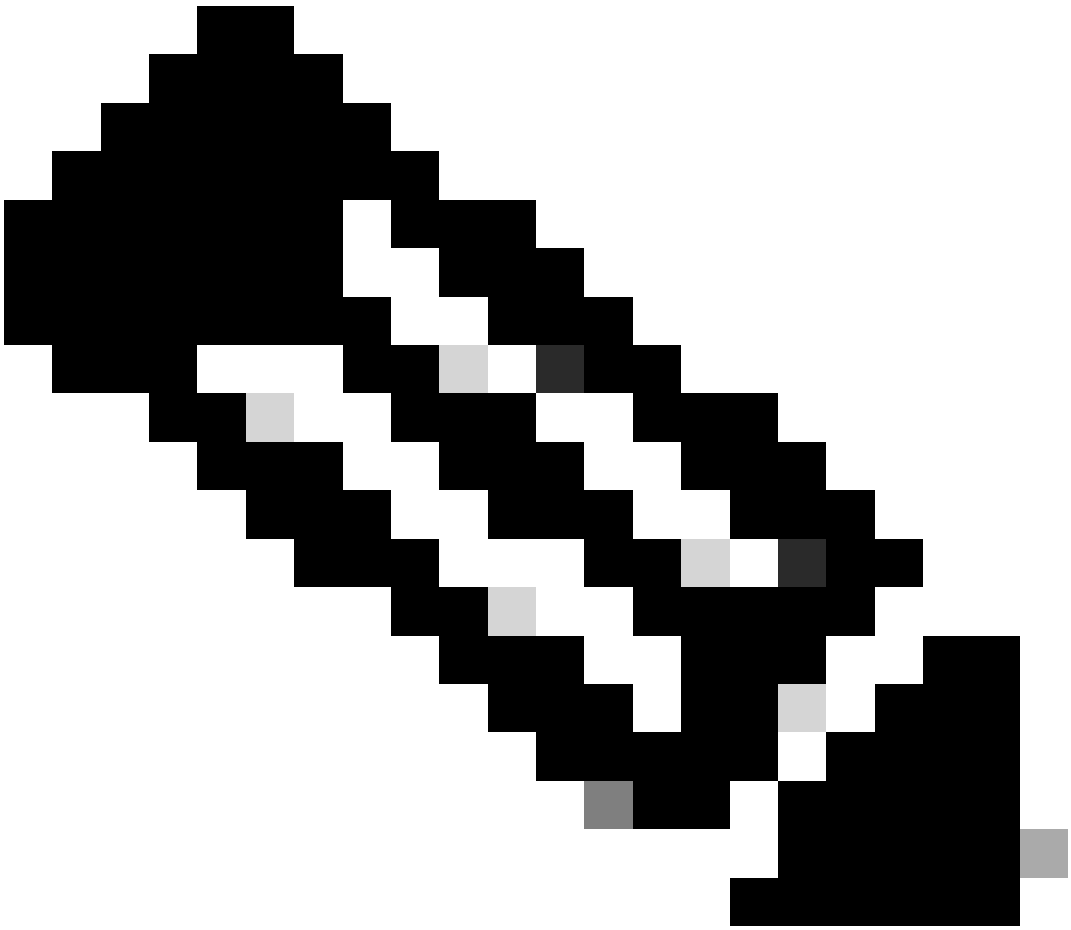
- Le nom de domaine complet correspondant au certificat doit être configuré en tant que domaine local sur le tableau de bord Umbrella afin que l'appliance virtuelle le reconnaisse comme domaine local.
- La clé privée et les certificats doivent être créés respectivement au format .key et .cer.
- Vous pouvez utiliser des certificats auto-signés ou des certificats signés par une autorité de certification à cette fin.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appareil virtuel exécutant la version 2.7 ou ultérieure
- Le connecteur AD Umbrella doit exécuter la version 1.5 ou ultérieure
- Les clients Umbrella Chromebook doivent exécuter la version 1.3.3 ou ultérieure

---



Remarque : Si votre connecteur VA ou AD exécute des versions précédentes, vous pouvez ouvrir un ticket d'assistance avec Umbrella pour les mettre à niveau vers les versions prises en charge respectives.

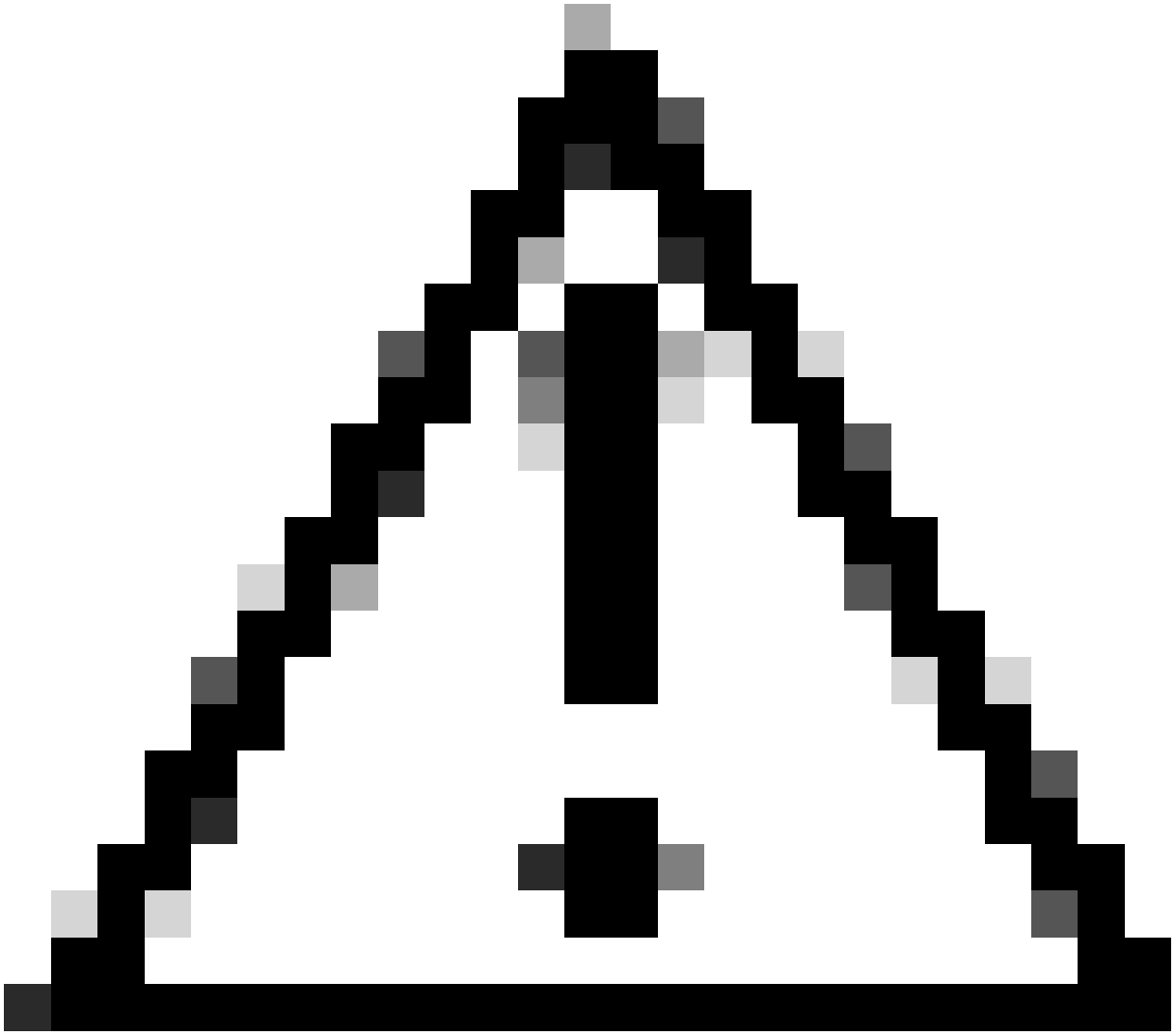
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

Les appareils virtuels Umbrella, exécutant la version 2.6 ou antérieure, prennent en charge la réception des mappages IP utilisateur à partir du connecteur Active Directory (AD) Umbrella et des clients Chromebook Umbrella uniquement sous une forme non chiffrée sur le port 443. Par conséquent, une condition préalable obligatoire au déploiement a été que le connecteur AD et les clients VA ou Chromebook et VA communiquent sur un réseau approuvé uniquement.

À partir de la version 2.7, les appareils virtuels Umbrella peuvent désormais recevoir des mappages utilisateur-IP AD à partir du connecteur AD sur HTTPS et, de la même manière, des mappages utilisateur-IP GSuite à partir de chaque client Umbrella Chromebook sur HTTPS.

Cet article détaille les étapes de configuration de chaque composant pour activer la communication HTTPS. Par défaut, la communication HTTPS est désactivée et le connecteur AD et les clients Chromebook communiquent avec l'appliance virtuelle sur HTTP uniquement.



Mise en garde : L'activation de cette fonctionnalité peut augmenter l'utilisation du processeur et de la mémoire sur l'appliance virtuelle et le connecteur AD parapluie et peut entraîner une réduction du débit DNS pour l'appliance virtuelle. Par conséquent, il est recommandé d'activer cette fonctionnalité uniquement si des exigences de conformité de votre organisation l'exigent.

Appareil virtuel

Ajouter une clé privée et un certificat à l'appliance virtuelle

Pour ajouter la clé privée et le certificat à l'appliance virtuelle :
1. Ouvrez le fichier de clé privée via l'éditeur de texte.

2. Sélectionnez tout, copiez, puis collez les guillemets doubles de cette commande :

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

Ajouter un certificat à la VA

Pour ajouter le certificat à l'appliance virtuelle :
1. Ouvrez le fichier de certificat via l'éditeur de texte.

2. Sélectionnez tout, copiez, puis collez les guillemets doubles pour la commande ci-dessous :

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

Activer HTTPS sur l'appliance virtuelle

Activez HTTPS sur l'appliance virtuelle à l'aide de cette commande :

```
config va ssl enable
```

Vérification de l'activation HTTPS

Vérifiez que HTTPS est activé à l'aide de la commande suivante :

```
config va show
```

Le résultat de cette commande peut inclure l'état HTTPS ainsi que les détails du certificat SSL.

Exemple de rapport :

```
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
```

La réception des événements via HTTPS peut prendre jusqu'à 20 minutes. Vous pouvez vérifier après environ 20 minutes en utilisant la commande `config va status`. L'état du connecteur Active Directory est jaune (bloqué) dans la période intermédiaire et passe à l'état vert une fois que l'appliance virtuelle commence à recevoir des événements via HTTPS.

Si vous souhaitez désactiver HTTPS et revenir à HTTP, utilisez la commande `config va ssl`

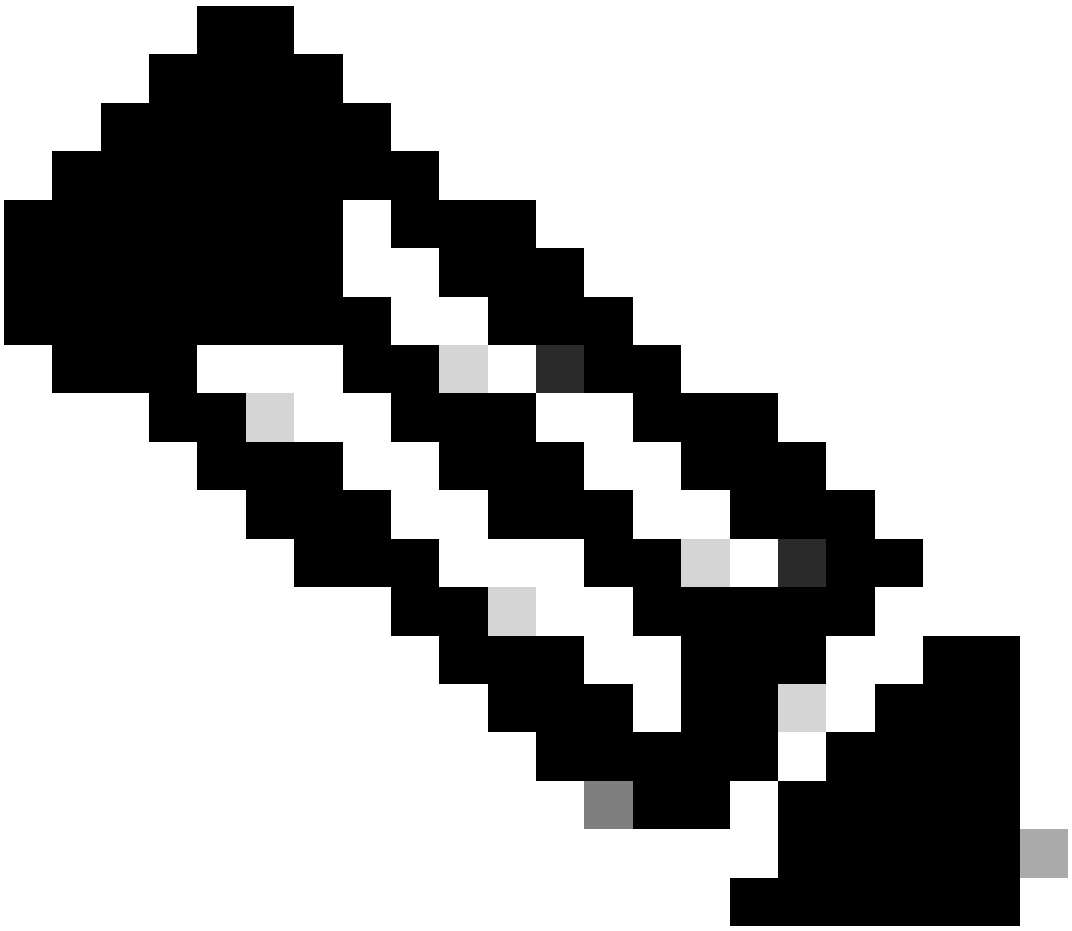
`disable`.

Si vous souhaitez réactiver HTTPS, vous devez ajouter à nouveau la clé privée et le certificat, puis utiliser la commande `config va enable`.

Active Directory

Si vous utilisez un certificat CA signé pour chaque VA, assurez-vous que le certificat racine et les certificats CA d'émission pour chaque certificat VA sont installés sur chaque système exécutant le connecteur AD sur le même site que l'VA.

Si vous utilisez un certificat auto-signé pour chaque VA, assurez-vous que chaque certificat VA est installé sur chaque système exécutant le connecteur AD dans le même site Umbrella que la VA.



> Remarque : Seuls les certificats pour les VA du même site Umbrella que le connecteur AD doivent être installés sur le connecteur AD.

La synchronisation de l'état HTTPS avec Umbrella, qui est ensuite synchronisé avec le connecteur Active Directory, peut prendre jusqu'à 20 minutes. Par conséquent, le connecteur peut prendre jusqu'à 20 minutes pour commencer à envoyer des données à l'appliance virtuelle via HTTPS. Tous les mappages utilisateur-IP envoyés au cours de cette période sont ignorés par l'appliance virtuelle. Il est donc recommandé de modifier la configuration de l'appliance virtuelle uniquement pendant les heures d'indisponibilité, lorsqu'aucune connexion utilisateur n'est attendue.

Client Android Umbrella

Si vous utilisez des certificats signés par une autorité de certification pour les appareils Android, assurez-vous que le certificat racine et les certificats d'autorité de certification d'émission pour chaque certificat d'autorité de certification sont envoyés et installés sur chaque appareil Android.

Si vous utilisez des certificats auto-signés pour les appareils Android, assurez-vous que chaque certificat VA est envoyé et installé sur chaque appareil Android.

Une fois le certificat disponible, le client Umbrella Android peut commencer à utiliser ce certificat pour configurer un canal HTTPS avec l'AV.

Umbrella Chromebook Client

Si vous utilisez des certificats signés par une autorité de certification pour les VA, assurez-vous que le certificat racine et les certificats d'autorité de certification d'émission pour chaque certificat VA sont envoyés et installés sur chaque Chromebook.

Si vous utilisez des certificats auto-signés pour les VA, assurez-vous que chaque certificat VA est envoyé et installé sur chaque Chromebook.

Une fois le certificat disponible, le client Umbrella Chromebook peut commencer à utiliser ce certificat pour configurer un canal HTTPS avec le VA.

Pour plus d'informations, référez-vous à l'article Umbrella Chromebook Client : Envoi de mappages utilisateur-IP sur un canal sécurisé vers l'appliance virtuelle Umbrella.

Séquence de configuration

Une fois que HTTPS est activé sur l'AV, l'AV n'accepte pas les mappages utilisateur-IP envoyés en texte clair sur HTTP. Par conséquent, toutes les connexions utilisateur envoyées via HTTP sont ignorées et l'attribution d'utilisateur pour les requêtes DNS de ces utilisateurs n'est pas disponible. Il est donc recommandé de configurer ces composants dans l'ordre suivant :

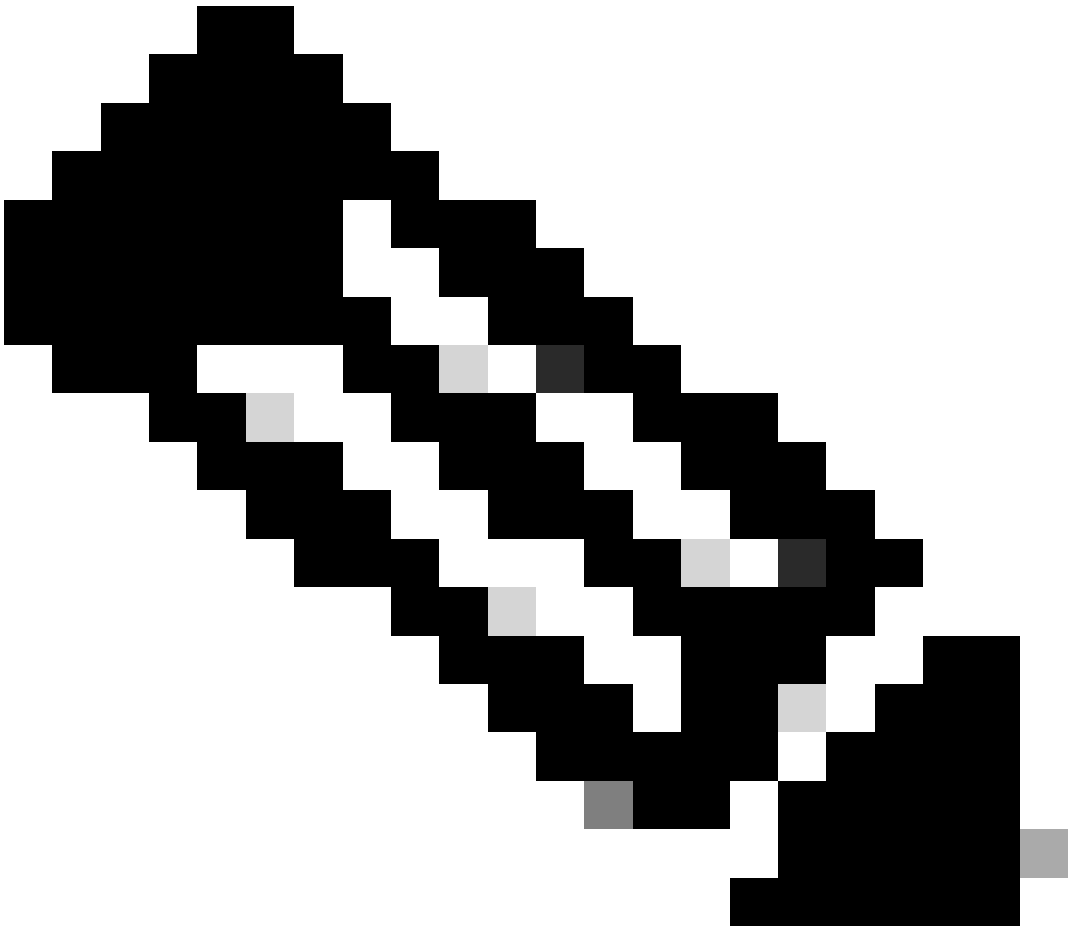
1. Créez le certificat et la clé privée pour chaque VA sur la base d'un certificat signé par l'autorité de certification ou auto-signé.

2. Ajoutez respectivement le certificat et la clé privée à chaque VA.

3. Assurez-vous que le certificat racine et les certificats parents intermédiaires pour chaque

certificat VA (ou certificat auto-signé VA) sont installés sur chaque système exécutant le connecteur AD sur le même site que l'VA, et sur chaque Chromebook.

4. Pendant les heures d'indisponibilité, activez HTTPS sur l'appliance virtuelle.



Remarque : Le certificat sur le VA doit être remplacé avant son expiration, et les certificats parent et racine intermédiaires doivent être installés sur le connecteur AD et les clients Umbrella Chromebook. Si cela n'est pas fait, les clients Connecteur AD et Umbrella Chromebook ne sont pas en mesure de communiquer avec la VA.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.