# Cisco Umbrella sécurisé pour les déploiements d'appareils virtuels et de connecteurs AD

## Table des matières



## Introduction

Ce document décrit les meilleures pratiques et les recommandations relatives aux déploiements de Cisco Umbrella Virtual Appliance (VA) et de connecteurs Active Directory (AD) afin de limiter le risque d'attaques internes découlant de l'utilisation de ces composants.

L'appliance virtuelle exécute une version renforcée d'Ubuntu Linux 20.04. Les clients disposent d'un accès restreint à des fins de configuration et de dépannage uniquement. Aucun logiciel ou script supplémentaire ne peut être déployé sur l'appliance virtuelle par les clients.

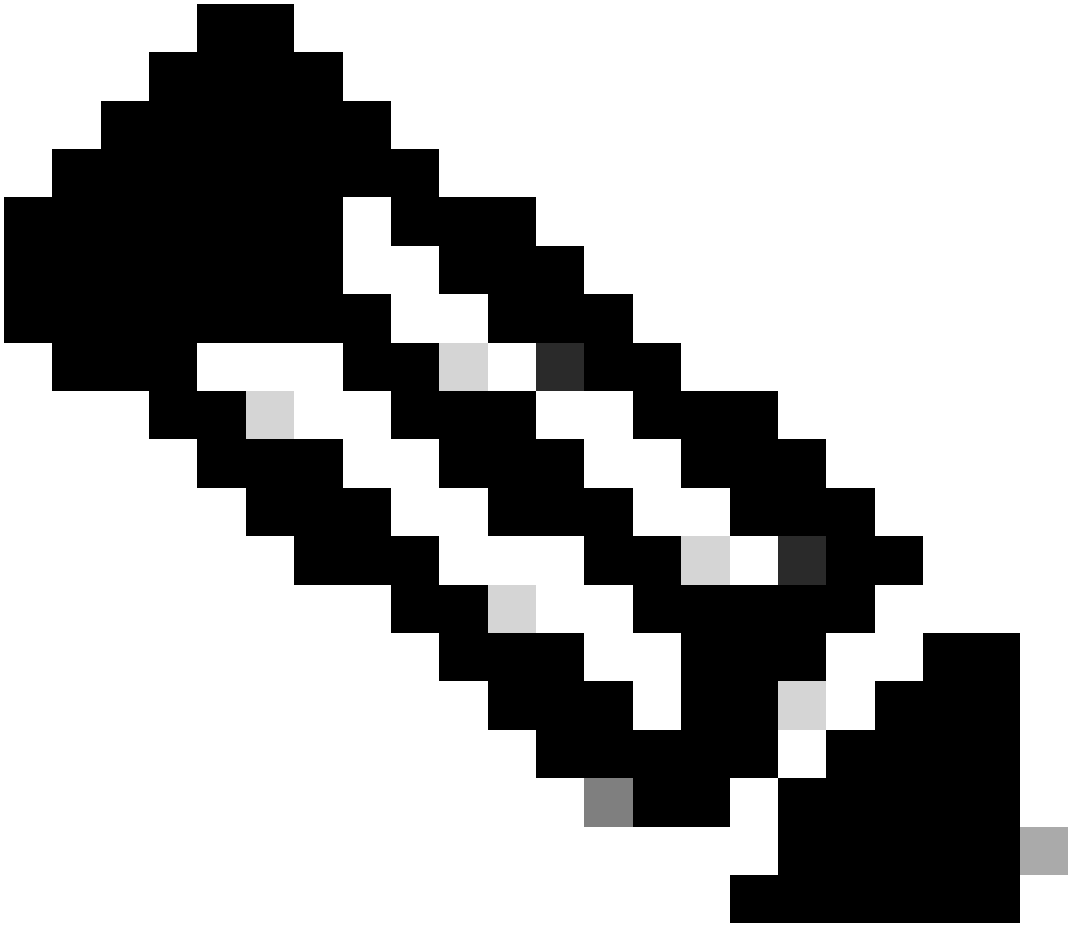
## Appliance virtuelle Cisco Umbrella

Gestion du fichier .tar :

- Le logiciel Cisco Umbrella Virtual Appliance (VA) est téléchargé à partir du tableau de bord Umbrella sous la forme d'un fichier .tar qui contient l'image VA réelle et une signature pour cette image.
- Cisco recommande de valider la signature pour vérifier l'intégrité de l'image VA.

Configuration des ports :

- Par défaut, lors du déploiement, seuls les ports 53 et 443 sont ouverts pour le trafic entrant.
- Si vous exécutez l'VA sur Azure, KVM, Nutanix, AWS ou GCP, le port 22 est également activé par défaut pour autoriser les connexions SSH pour configurer l'VA.
- Pour les serveurs virtuels exécutés sur VMware et Hyper-V, le port 22 est ouvert uniquement si la commande permettant d'activer SSH est exécutée sur le serveur virtuel.
- L'AV effectue des requêtes sortantes sur des ports/protocoles spécifiques vers les destinations mentionnées dans la documentation Umbrella.
- Cisco Umbrella recommande de configurer des règles sur votre pare-feu pour bloquer tout trafic provenant de vos VA vers toutes les autres destinations.



Remarque : Toutes les communications HTTPS vers/depuis l'appliance virtuelle s'effectuent via TLS 1.2 uniquement. Les protocoles plus anciens ne sont pas utilisés.

---

Gestion des mots de passe :

- La connexion initiale sur l'appliance virtuelle nécessite un changement de mot de passe.
- Cisco recommande de faire pivoter régulièrement le mot de passe sur l'appliance virtuelle après ce changement de mot de passe initial.

Réduction des attaques DNS :

- Pour limiter le risque d'une attaque de déni de service interne sur le service DNS exécuté sur l'VA, vous pouvez configurer des limites de débit par IP pour le DNS sur l'VA.
- Cette option n'est pas activée par défaut et doit être explicitement configurée à l'aide des instructions documentées dans la documentation Umbrella.

Surveillance des VA sur SNMP :

- Si vous surveillez vos VA sur SNMP, Cisco Umbrella vous recommande d'utiliser SNMPv3 avec authentification et cryptage.
- Des instructions pour la même opération sont fournies dans la documentation Umbrella.
- Une fois que vous avez activé la surveillance SNMP, le port 161 de l'appliance virtuelle est ouvert pour le trafic entrant.
- Vous pouvez surveiller divers attributs tels que le CPU, la charge et la mémoire sur l'appliance virtuelle via SNMP.

Utilisation de l'intégration de Cisco AD avec les VA :

- Si vous utilisez les VA avec l'intégration Cisco Umbrella Active Directory, il est recommandé de régler (ou d'ajuster) la durée du cache utilisateur sur l'VA pour qu'elle corresponde à votre durée de bail DHCP.
- Reportez-vous aux instructions de l'appliance virtuelle : Réglage de la documentation des paramètres de caisse utilisateur. Cela réduit le risque d'attributions incorrectes de l'utilisateur.

Configuration de la journalisation d'audit :

- L'appliance virtuelle tient à jour un journal d'audit de toutes les modifications de configuration exécutées sur l'appliance virtuelle.
- Vous pouvez configurer la journalisation à distance de ce journal d'audit sur un serveur syslog selon les instructions de la documentation Umbrella.

Configuration des VA :

- Au moins deux VA doivent être configurés par site Umbrella, et l'adresse IP de ces deux VA peut être distribuée en tant que serveurs DNS aux points d'extrémité.
- Pour une redondance supplémentaire, vous pouvez configurer l'adressage Anycast sur l'appliance virtuelle. Cela permet à plusieurs VA de partager une seule adresse Anycast.
- Ainsi, vous pouvez déployer plusieurs serveurs virtuels tout en distribuant seulement deux adresses IP de serveur DNS à chaque point d'extrémité. En cas d'échec d'un VA, Anycast s'assure que les requêtes DNS sont acheminées vers l'autre VA qui partage la même adresse IP Anycast.
- En savoir plus sur les étapes de configuration d'Anycast sur l'appliance virtuelle.

# Configuration du connecteur Active Directory Cisco Umbrella

Créer un nom de compte personnalisé :

- L'une des meilleures pratiques pour le connecteur Cisco Umbrella AD consiste à utiliser un nom de compte personnalisé à la place du connecteur OpenDNS_Connector par défaut.
- Ce compte peut être créé avant le déploiement du connecteur et recevoir les autorisations requises.
- Le nom du compte doit être spécifié lors de l'installation du connecteur.

Configuration de LDAPS avec le connecteur AD :

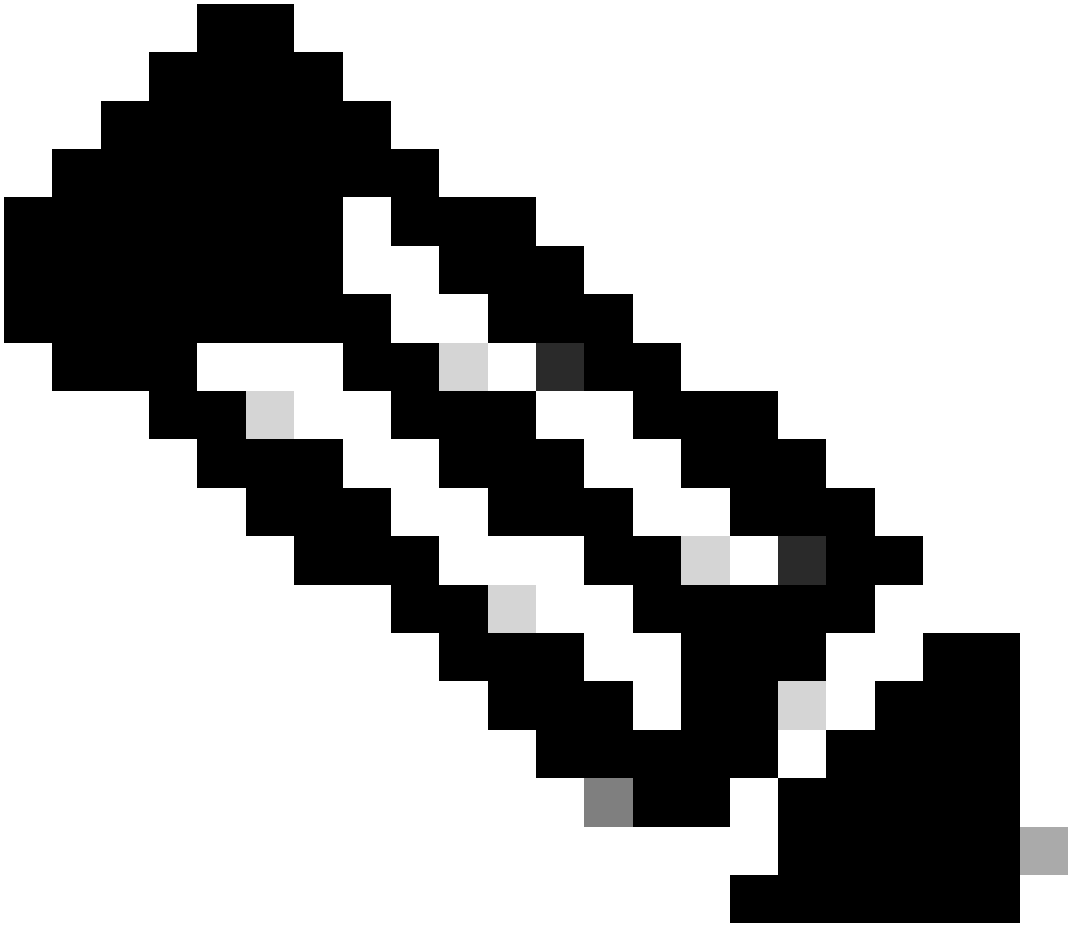
- Le connecteur AD Umbrella tente de récupérer des informations de groupe d'utilisateurs sur LDAPS (données transmises sur un canal sécurisé), faute de quoi il bascule vers LDAP sur Kerberos (chiffrement au niveau paquet) ou LDAP sur NTLM (authentification uniquement, pas de chiffrement) dans cet ordre.
- Cisco Umbrella recommande de configurer des LDAPS sur vos contrôleurs de domaine afin que le connecteur puisse récupérer ces informations sur un canal chiffré.

Gestion du fichier .ldif :

- Par défaut, le connecteur stocke les détails des utilisateurs et des groupes récupérés des contrôleurs de domaine dans un fichier .ldif localement.
- Comme il peut s'agir d'informations sensibles stockées en texte brut, vous pouvez restreindre l'accès au serveur qui exécute le connecteur.
- Au moment de l'installation, vous pouvez également choisir de ne pas stocker les fichiers .ldif localement.

Configuration des ports :

- Comme le connecteur est un service Windows, il n'active/désactive aucun port sur l'ordinateur hôte. Cisco Umbrella recommande d'exécuter le service Cisco Umbrella AD Connector sur un serveur Windows dédié.
- Tout comme le VA, le connecteur effectue des requêtes sortantes sur des ports/protocoles spécifiques vers les destinations mentionnées dans la documentation Umbrella. Cisco Umbrella recommande de configurer des règles sur votre pare-feu pour bloquer tout trafic provenant de vos connecteurs vers toutes les autres destinations.



Remarque : Toutes les communications HTTPS vers/depuis le connecteur se font uniquement via TLS 1.2. Les protocoles plus anciens ne sont pas utilisés.

---

Gestion du mot de passe du connecteur :

- Cisco recommande de faire pivoter régulièrement le mot de passe du connecteur.
- Pour ce faire, modifiez le mot de passe du compte de connecteur dans Active Directory, puis mettez à jour le mot de passe à l'aide de l'outil « PasswordManager » dans le dossier du connecteur.

Réception des mappages utilisateur-IP :

- Par défaut, le connecteur communique une adresse IP privée.
- AD envoie les mappages utilisateur à l'AV en texte clair.
- Vous pouvez choisir de configurer l'appliance virtuelle et le connecteur pour qu'ils communiquent sur un canal chiffré, conformément aux instructions décrites dans cet article de la Base de connaissances.

Gestion des certificats :

- La gestion et la révocation des certificats sont hors du champ d'application de l'AV et vous êtes chargé de vous assurer que la dernière chaîne de certificats est présente sur l'AV et le connecteur, le cas échéant.
- La configuration d'un canal chiffré pour cette communication a un impact sur les performances de la baie virtuelle et du connecteur.

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.