Configurer le mappage des attributs LDAP sur ASA pour le VPN client sécurisé

Table des matières

- Introduction
  - Exigences
    - Exigences Cisco ASA
    - Besoins réseau
    - Besoins des clients
  - Composants utilisés
- Configuration Steps
  - Étape 1 : définition des stratégies de groupe
  - Étape 2 : configuration du mappage d'attributs LDAP
  - Étape 3. Configuration du serveur AAA LDAP
  - Étape 4. Définition du groupe de tunnels
- Vérifier
  - Vérification de l'attribution de session VPN
- Dépannage
  - Activer le débogage LDAP
  - Établir une connexion VPN
  - Examiner le résultat du débogage
  - Désactiver le débogage après vérification
  - Problèmes courants

Introduction

Ce document décrit la configuration du mappage d'attributs LDAP sur Cisco ASA pour attribuer des stratégies de groupe VPN basées sur des groupes Active Directory.

Exigences

Exigences Cisco ASA

- Cisco ASA exécute une version logicielle prise en charge.
- Accès administratif au périphérique ASA.

Besoins réseau

- Domaine Active Directory (AD) accessible à l'ASA.
- LDAP sur SSL (LDAPS) configuré sur le serveur AD (port par défaut 636).

Besoins des clients

- Client sécurisé installé sur les périphériques clients.

Composants utilisés

Les informations contenues dans ce document ne sont pas limitées à des versions logicielles et matérielles spécifiques.

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.

Configuration Steps

Étape 1 : définition des stratégies de groupe

Les stratégies de groupe déterminent les autorisations et les restrictions pour les utilisateurs VPN. Créez les stratégies de groupe nécessaires qui s'alignent sur les exigences d'accès de votre organisation.

Créer une stratégie de groupe pour les utilisateurs autorisés

```
group-policy VPN_User_Policy internal
group-policy VPN_User_Policy attributes
  vpn-simultaneous-logins 3
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value SPLIT_TUNNEL_ACL
```

Créez une stratégie de groupe par défaut pour refuser l'accès.

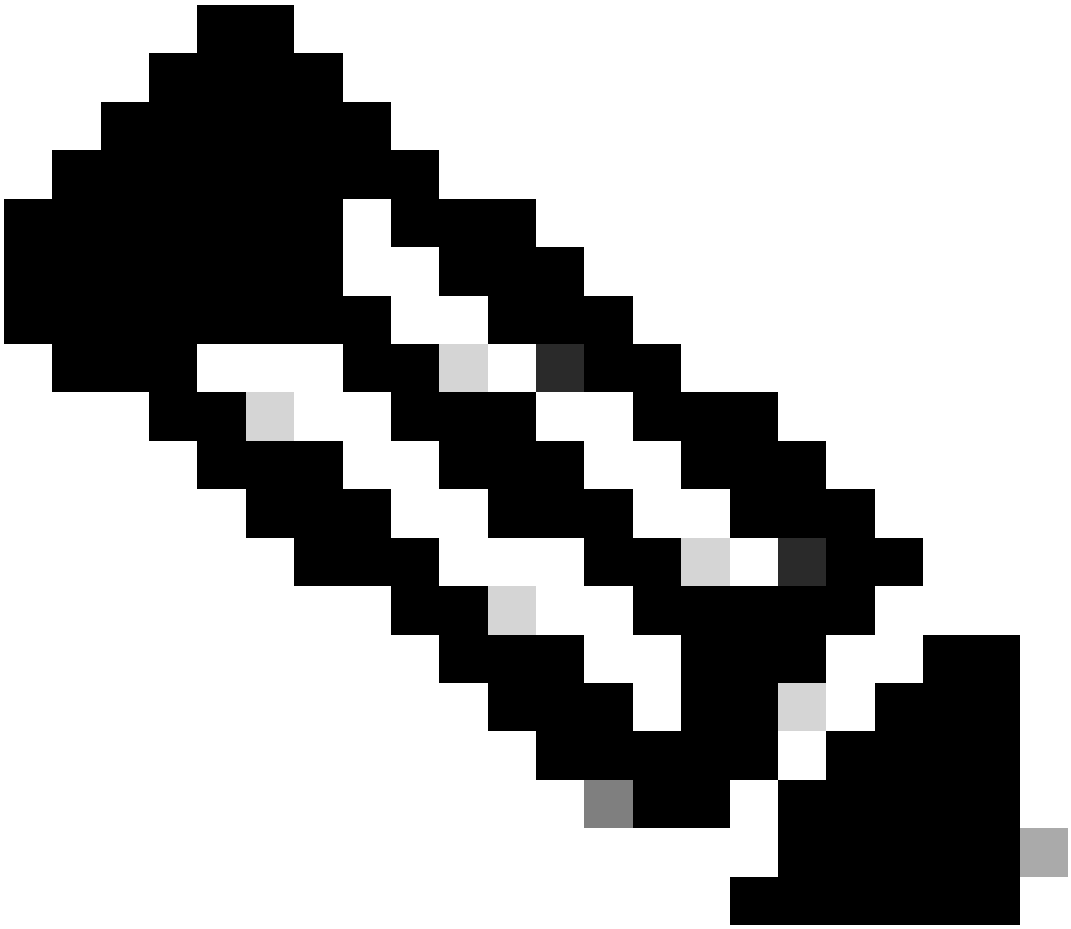
```
group-policy No_Access_Policy internal
group-policy No_Access_Policy attributes
  vpn-simultaneous-logins 0
```

Étape 2 : configuration du mappage d’attributs LDAP

Le mappage d'attributs traduit les attributs LDAP en attributs ASA, ce qui permet à l'ASA d'affecter les utilisateurs à la stratégie de groupe correcte en fonction de leurs appartenances au groupe LDAP.

```
ldap attribute-map VPN_Access_Map
```

```
  map-name  memberOf Group-Policy
  map-value memberOf "CN=VPN_Users,OU=Groups,DC=example,DC=com" VPN_User_Policy
```



> Remarque : Le nom distinctif (DN) du groupe LDAP doit toujours être placé entre guillemets doubles (""). Cela garantit que l'ASA interprète correctement les espaces et les caractères spéciaux dans le DN.

Étape 3. Configuration du serveur AAA LDAP

Configurez l'ASA pour communiquer avec le serveur AD pour l'authentification et le mappage de groupe.

```
aaa-server AD_LDAP_Server protocol ldap
aaa-server AD_LDAP_Server (inside) host 192.168.1.10
  ldap-base-dn dc=example,dc=com
  ldap-scope subtree
```

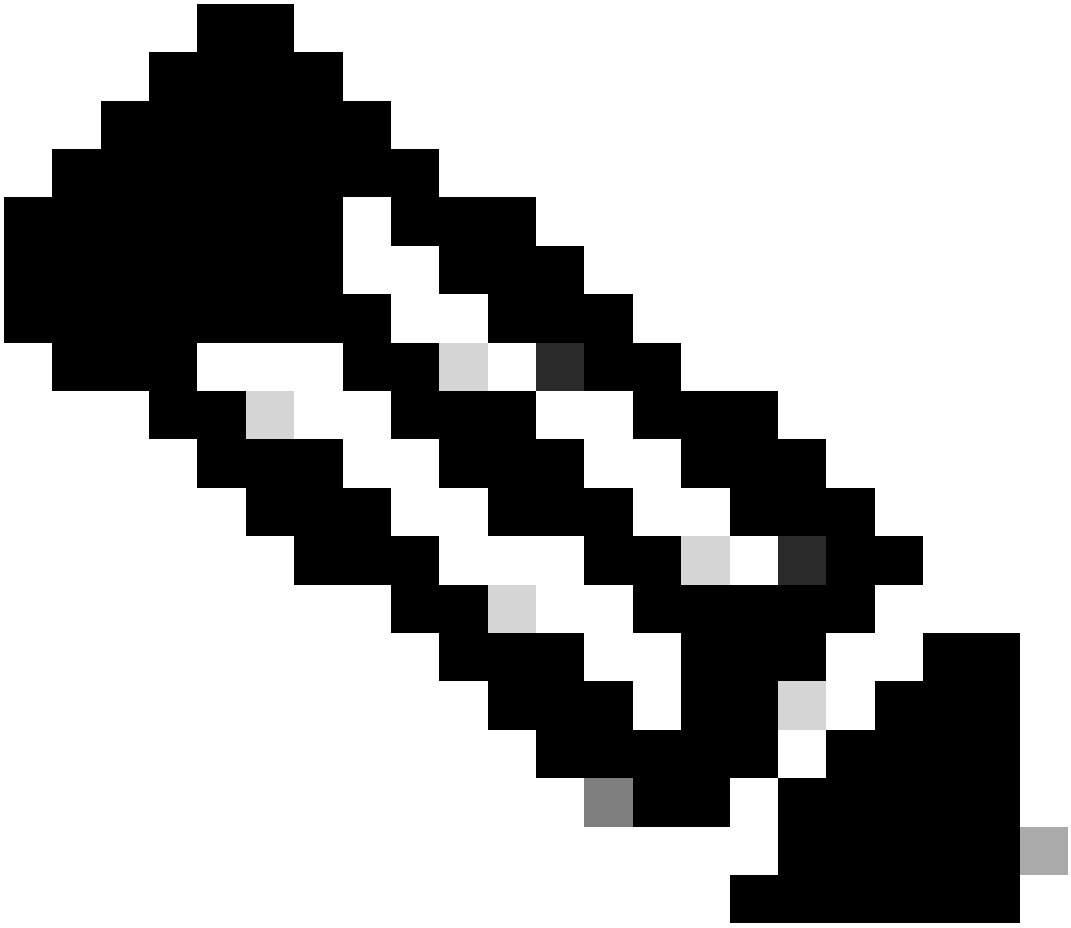
```
  ldap-naming-attribute sAMAccountName
  ldap-login-password ********
  ldap-login-dn CN=ldap_bind_user,OU=Service Accounts,DC=example,DC=com
  ldap-over-ssl enable
  ldap-attribute-map VPN_Access_Map
```

Étape 4. Définition du groupe de tunnels

Le groupe de tunnels définit les paramètres VPN et lie l'authentification au serveur LDAP.

```
tunnel-group VPN_Tunnel type remote-access
tunnel-group VPN_Tunnel general-attributes
  address-pool VPN_Pool
  authentication-server-group AD_LDAP_Server
  default-group-policy No_Access_Policy

tunnel-group VPN_Tunnel webvpn-attributes
  group-alias VPN_Tunnel enable
```



Remarque : La stratégie de groupe par défaut est définie sur No_Access_Policy, refusant l'accès aux utilisateurs ne correspondant à aucun critère de mappage d'attribut LDAP.

Vérifier

Une fois l'installation terminée, vérifiez que les utilisateurs sont correctement authentifiés et que les stratégies de groupe appropriées leur sont affectées.

Vérification de l'attribution de session VPN

```
show vpn-sessiondb anyconnect filter name
```

Remplacez <username> par le compte de test réel.

Dépannage

Utilisez cette section pour dépanner votre configuration.

Activer le débogage LDAP

Si les utilisateurs ne reçoivent pas les stratégies de groupe attendues, activez le débogage pour identifier les problèmes.

```
debug ldap 255
debug aaa common 255
debug aaa shim 255
```

Établir une connexion VPN

Demandez à un utilisateur test de tenter de se connecter à l'aide de Cisco Secure Client.

Examiner le résultat du débogage

Vérifiez les journaux Cisco ASA pour vous assurer que l'utilisateur est mappé à la stratégie de groupe correcte en fonction de son appartenance au groupe Active Directory (AD).

Désactiver le débogage après vérification

```
undebug all
```

Problèmes courants

Les mappages d'attributs LDAP sont sensibles à la casse. Assurez-vous que les noms de groupe AD dans les instructions map-value correspondent exactement, en tenant compte de la casse.

Vérifiez que les utilisateurs sont des membres directs des groupes AD spécifiés. Les appartenances à des groupes imbriqués ne sont pas toujours reconnues, ce qui entraîne des problèmes d'autorisation.

Les utilisateurs ne correspondant à aucun critère de valeur de mappage reçoivent la stratégie de groupe par défaut (No_Access_Policy dans ce cas), ce qui empêche l'accès.

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.