セキュアクライアントVPNに対するASAでのLDAP属性マッピングの設定

内容

はじめに

このドキュメントでは、Active Directory(AD)グループに基づいてVPNグループポリシーを割り当てるようにCisco ASAでLDAP属性マッピングを設定する方法について説明します。

要件

Cisco ASAの要件

- サポートされているソフトウェアバージョンを実行しているCisco ASA
- ASAデバイスへの管理アクセス。

ネットワーク要件

- ASAにアクセス可能なActive Directory(AD)ドメイン。
- ADサーバでLDAP over SSL(LDAPS)が設定されている（デフォルトポートは636）。

クライアント要件

- クライアントデバイスにインストールされたセキュアクライアント。

使用するコンポーネント

このドキュメントの情報は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

設定手順

ステップ 1：グループポリシーの定義

グループポリシーは、VPNユーザの権限と制限を決定します。組織のアクセス要件に合わせて、必要なグループポリシーを作成します。

許可されたユーザのグループポリシーの作成

```
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
```

デフォルトのグループポリシーを作成してアクセスを拒否する。

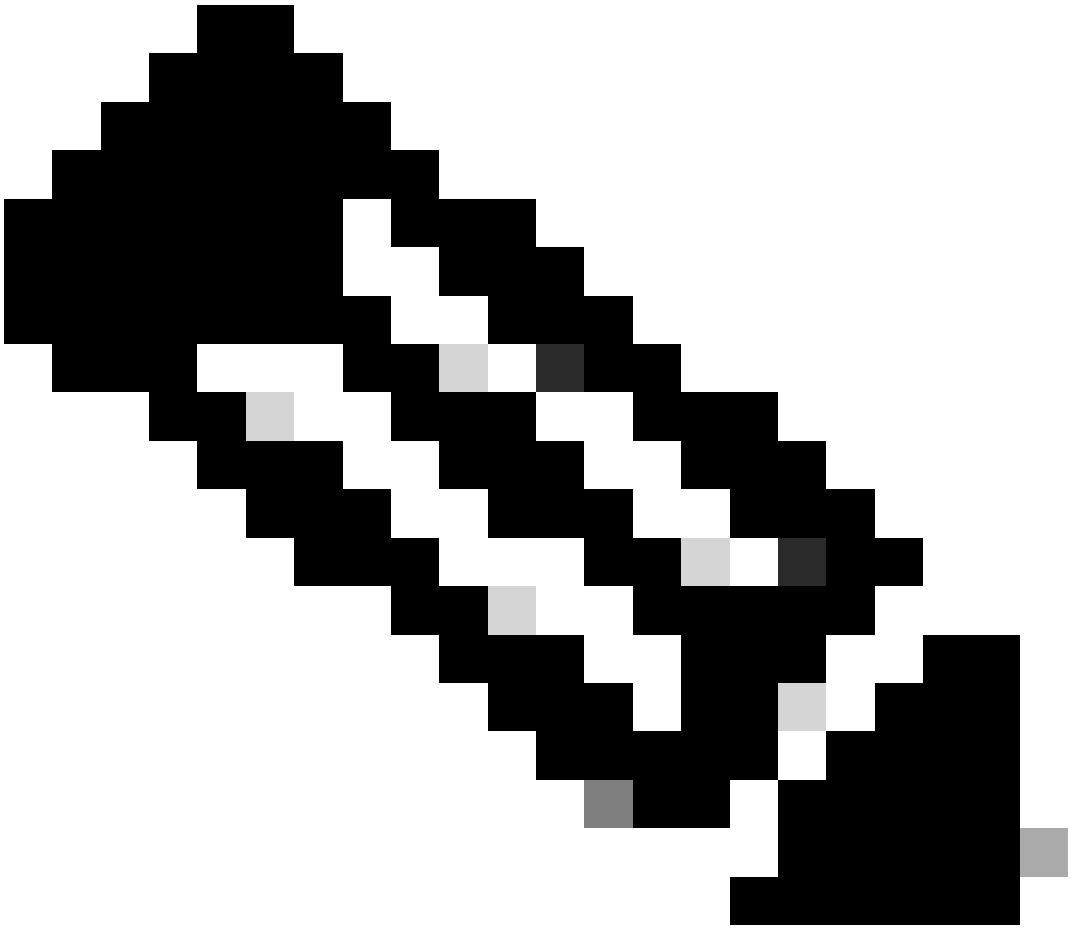
```
group-policy No_Access_Policy internal
group-policy No_Access_Policy attributes
  vpn-simultaneous-logins 0
```

ステップ 2：LDAP属性マップの設定

属性マップはLDAP属性をASA属性に変換し、ASAがユーザのLDAPグループメンバーシップに基づいてユーザを正しいグループポリシーに割り当てられるようにします。

```
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
```



注:LDAPグループの識別名(DN)は、常に二重引用符("")で囲む必要があります。 これにより、ASAがDN内のスペースと特殊文字を正しく解釈できるようになります。

ステップ 3：LDAP AAAサーバの設定

認証とグループマッピングのためにADサーバと通信するようにASAを設定します。

```
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
```

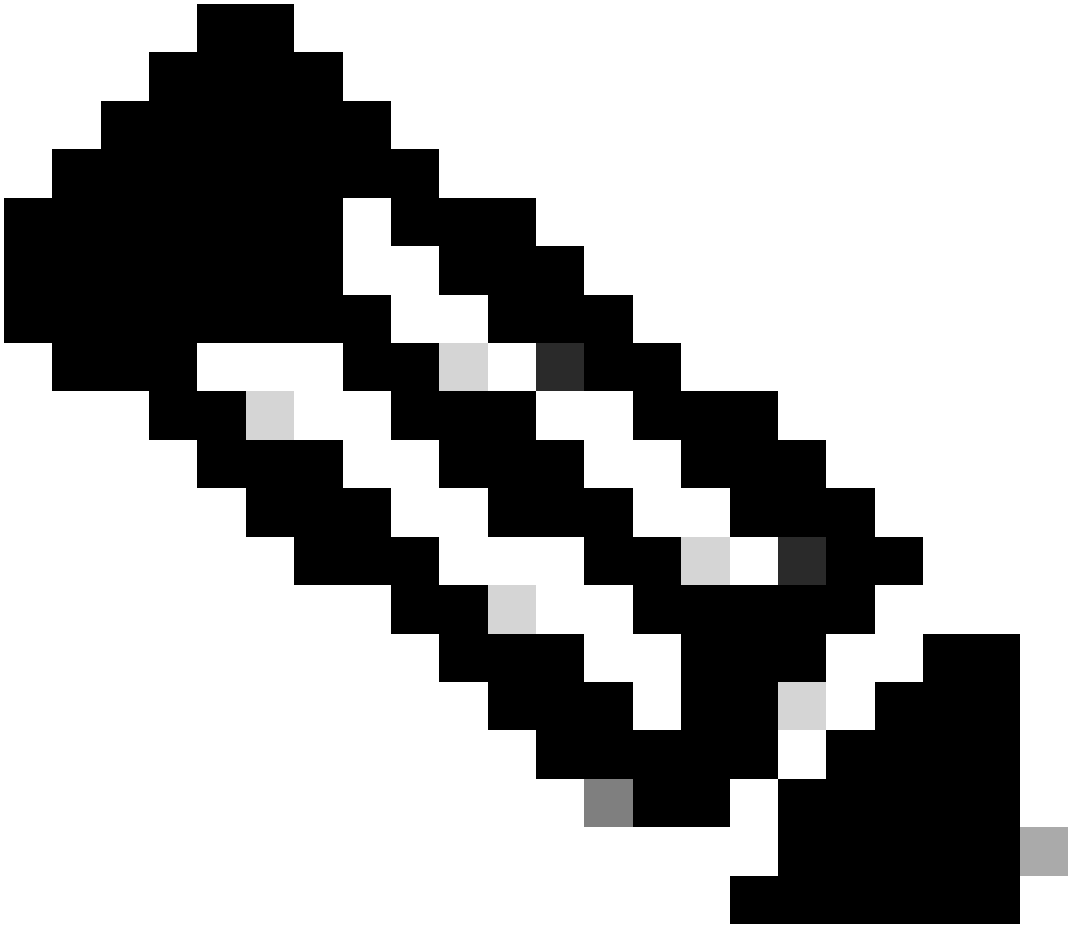
```
  ldap-attribute-map VPN_Access_Map
```

ステップ 4：トンネルグループの定義

トンネルグループはVPNパラメータを定義し、認証をLDAPサーバに結び付けます。

```
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
```



注:default-group-policyはNo_Access_Policyに設定され、LDAP属性マップの基準に一致し

ないユーザへのアクセスを拒否します。

確認

セットアップが完了したら、ユーザが正しく認証され、適切なグループポリシーが割り当てられていることを確認します。

VPNセッション割り当ての確認

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

<username>は実際のテストアカウントで置き換えます。

トラブルシュート

ここでは、設定に関するトラブルシューティングについて説明します。

LDAPデバッグの有効化

ユーザが期待どおりのグループポリシーを受信していない場合は、問題を特定するためにデバッグを有効にします。

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

VPN接続の開始

テストユーザに、Cisco Secure Clientを使用した接続を試してもらいます。

デバッグ出力の確認

Cisco ASAログを調べ、ユーザがActive Directory(AD)グループメンバーシップに基づいて正しいグループポリシーにマッピングされていることを確認します。

検証後のデバッグを無効にする

```
undebug all
```

一般的な問題

LDAP属性マッピングでは大文字と小文字が区別されます。map-value文のADグループ名が、大文字と小文字の区別を含めて正確に一致していることを確認してください。

ユーザが指定したADグループのダイレクトメンバーであることを確認します。入れ子になったグループメンバーシップは常に認識されるとは限らず、承認の問題を引き起こします。

どのマップ値の基準にも一致しないユーザは、default-group-policy（この場合はNo_Access_Policy）を受け取り、アクセスを防止します。

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。