Toewijzing van LDAP-kenmerken configureren op ASA voor beveiligde client-VPN

Inhoud

- Inleiding
  - Vereisten
    - Cisco ASA-vereisten
    - Netwerkvereisten
    - Clientvereisten
  - Gebruikte componenten
- Configuratiestappen
  - Stap 1. Definieer groepsbeleid
  - Stap 2. Configureer de LDAP Attribute Map
  - Stap 3. Configureer de LDAP AAA-server
  - Stap 4. Bepaal de tunnelgroep
- Verifiëren
  - Controleer de VPN-sessietoewijzing
- Problemen oplossen
  - LDAP-debugging inschakelen
  - Een VPN-verbinding starten
  - Beoordeel debug-uitvoer
  - Debuggen na verificatie uitschakelen
  - Veelvoorkomende problemen

Inleiding

Dit document beschrijft het configureren van LDAP-attribuuttoewijzing op Cisco ASA om VPN-groepsbeleid toe te wijzen op basis van Active Directory-groepen.

Vereisten

Cisco ASA-vereisten

- Cisco ASA ondersteunt een softwareversie.
- Administratieve toegang tot het ASA-apparaat.

Netwerkvereisten

- Active Directory (AD)-domein toegankelijk voor de ASA.
- LDAP over SSL (LDAPS) geconfigureerd op de AD-server (standaardpoort 636).

Clientvereisten

- Beveiligde client geïnstalleerd op clientapparaten.

Gebruikte componenten

De informatie in dit document is niet beperkt tot specifieke software- en hardwareversies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratiestappen

Stap 1. Definieer groepsbeleid

Groepsbeleid bepaalt de machtigingen en beperkingen voor VPN-gebruikers. Maak de nodige groepsbeleidsregels die op de toegangsvereisten van uw organisatie zijn afgestemd.

Een groepsbeleid voor geautoriseerde gebruikers maken

```
 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
```

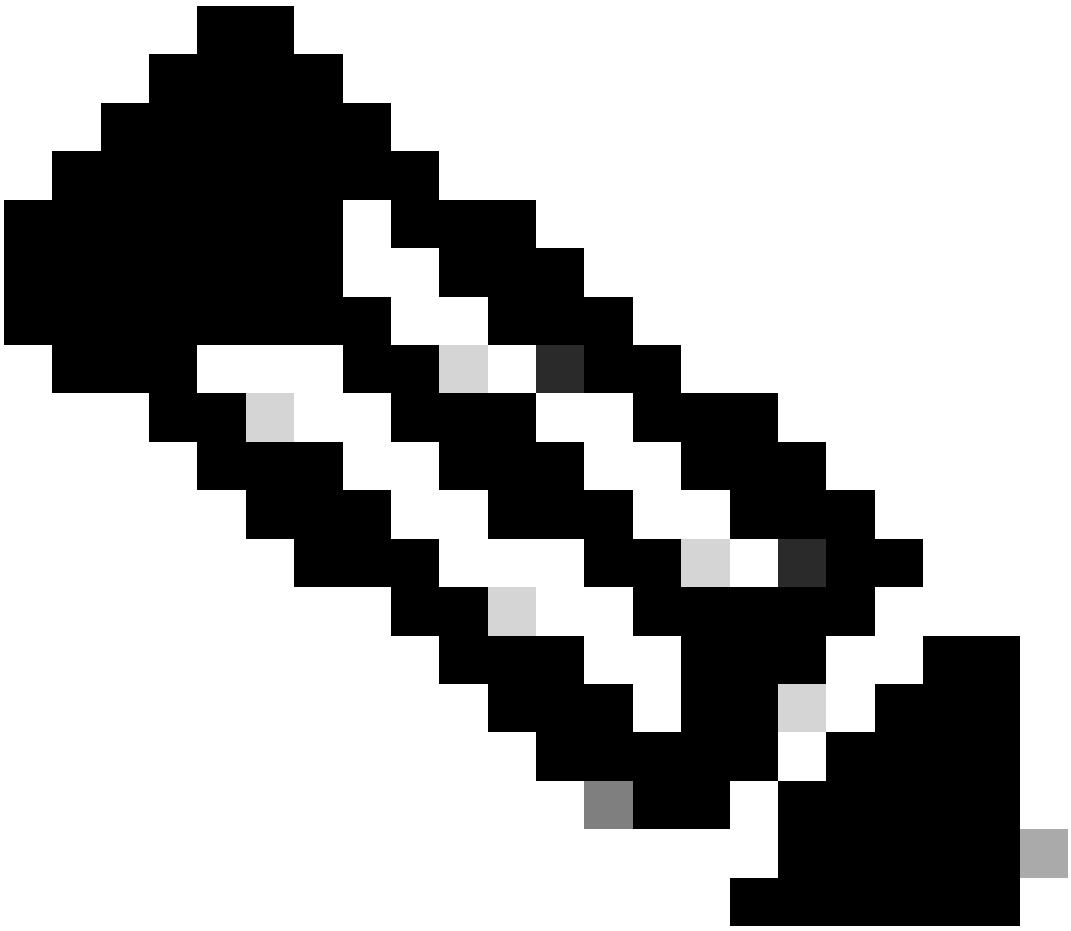
Maak een standaardgroepsbeleid om toegang te weigeren.

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

Stap 2. Configureer de LDAP Attribute Map

De attributenkaart vertaalt LDAP attributen naar ASA attributen, waardoor de ASA gebruikers kan toewijzen aan het juiste groepsbeleid op basis van hun LDAP groepslidmaatschap.

```
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
```



Opmerking: De kenmerkende naam (DN) van de LDAP-groep moet altijd worden ingesloten door dubbele aanhalingstekens (""). Dit zorgt ervoor dat ASA spaties en speciale tekens in de DN correct interpreteert.

Stap 3. Configureer de LDAP AAA-server

Stel de ASA in om met de AD-server te communiceren voor verificatie en groepstoewijzing.

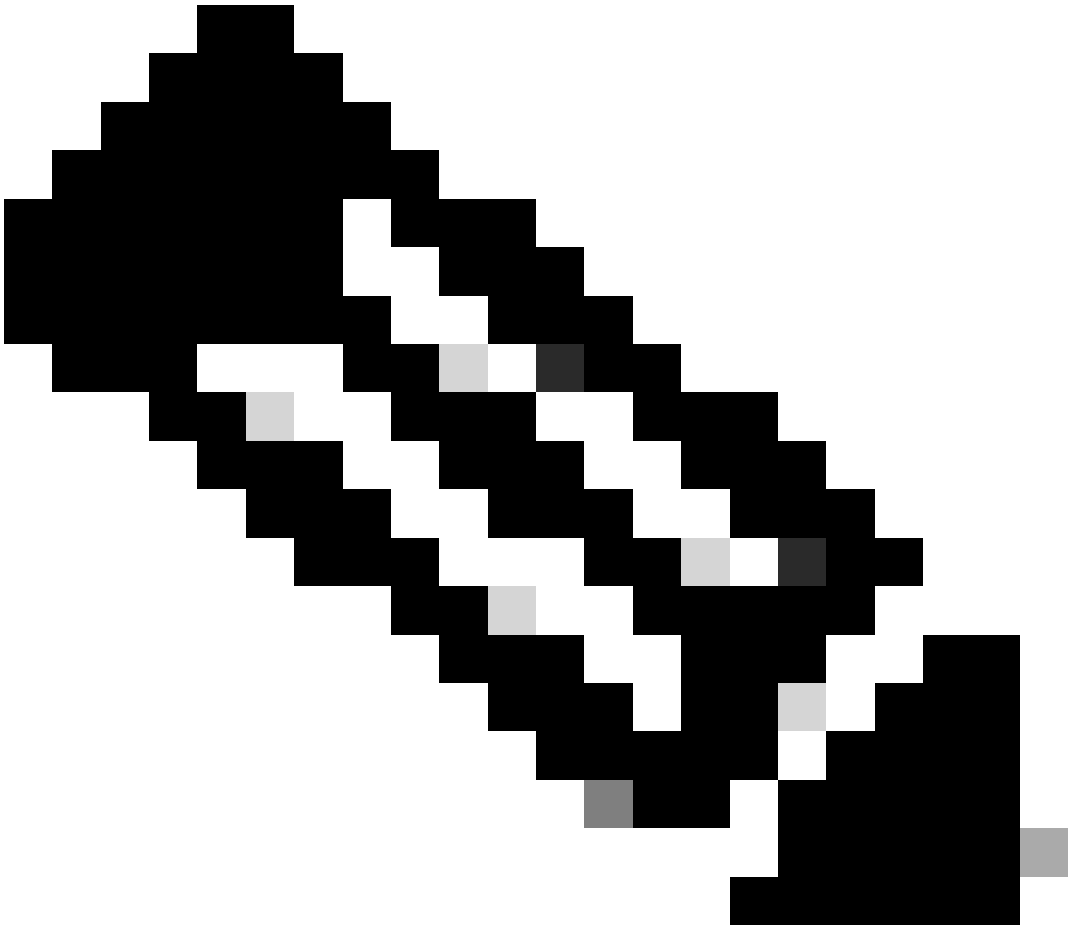
```
aaa-server AD_LDAP_Server protocol ldap
aaa-server AD_LDAP_Server (inside) host 192.168.1.10
  ldap-base-dn dc=example,dc=com
  ldap-scope subtree
  ldap-naming-attribute sAMAccountName
  ldap-login-password ********
  ldap-login-dn CN=ldap_bind_user,OU=Service Accounts,DC=example,DC=com
  ldap-over-ssl enable
  ldap-attribute-map VPN_Access_Map
```

Stap 4. Bepaal de tunnelgroep

De tunnelgroep definieert de VPN-parameters en verbindt de verificatie met de LDAP-server.

```
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
```



Opmerking: Het standaard-groep-beleid is ingesteld op No_Access_Policy, het ontkennen van toegang tot gebruikers die niet voldoen aan enige LDAP attribuut map criteria.

Verifiëren

Controleer na het voltooien van de installatie of de gebruikers correct zijn geverifieerd en het juiste groepsbeleid hebben toegewezen.

Controleer de VPN-sessietoewijzing

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

Vervang **<**gebruikersnaam**>** door de eigenlijke testaccount.

Problemen oplossen

Deze sectie bevat informatie om uw configuratie te troubleshooten.

LDAP-debugging inschakelen

Als de gebruikers niet het verwachte groepsbeleid ontvangen, laat het zuiveren toe om kwesties te identificeren.

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

Een VPN-verbinding starten

Laat een testgebruiker proberen verbinding te maken met Cisco Secure-client.

Beoordeel debug-uitvoer

Controleer de Cisco ASA-logbestanden om er zeker van te zijn dat de gebruiker is toegewezen aan het juiste groepsbeleid op basis van hun groepslidmaatschap van Active Directory (AD).

Debuggen na verificatie uitschakelen

```
undebug all
```

Veelvoorkomende problemen

LDAP-attribuuttoewijzingen zijn hoofdlettergevoelig. Zorg ervoor dat de AD-groepsnamen in de map-waarde statements exact overeenkomen, inclusief hoofdlettergevoeligheid.

Controleer of de gebruikers rechtstreeks lid zijn van de opgegeven AD-groepen. Nested groepslidmaatschap wordt niet altijd erkend, wat leidt tot autorisatieproblemen.

Gebruikers die niet voldoen aan enige kaart-waarde criteria ontvangen het standaard-groep-beleid (No_Access_Policy in dit geval), het voorkomen van toegang.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.