Konfigurieren der LDAP-Attributzuordnung auf ASA für Secure Client VPN

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der LDAP-Attributzuordnung auf der Cisco ASA beschrieben, um VPN-Gruppenrichtlinien basierend auf Active Directory-Gruppen zuzuweisen.

Anforderungen

Cisco ASA-Anforderungen

- Cisco ASA mit einer unterstützten Softwareversion
- Administrator-Zugriff auf das ASA-Gerät

Netzwerkanforderungen

- Active Directory (AD)-Domäne, auf die die ASA zugreifen kann.
- LDAP über SSL (LDAPS), konfiguriert auf dem AD-Server (Standardport 636)

Client-Anforderungen

- Secure Client auf Client-Geräten installiert.

Verwendete Komponenten

Die Informationen in diesem Dokument sind nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurationsschritte

Schritt 1: Gruppenrichtlinien definieren

Gruppenrichtlinien bestimmen die Berechtigungen und Einschränkungen für VPN-Benutzer. Erstellen Sie die erforderlichen Gruppenrichtlinien, die an den Zugriffsanforderungen Ihres Unternehmens ausgerichtet sind.

Erstellen einer Gruppenrichtlinie für autorisierte Benutzer

```
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
```

Erstellen einer Standardgruppenrichtlinie für die Verweigerung des Zugriffs

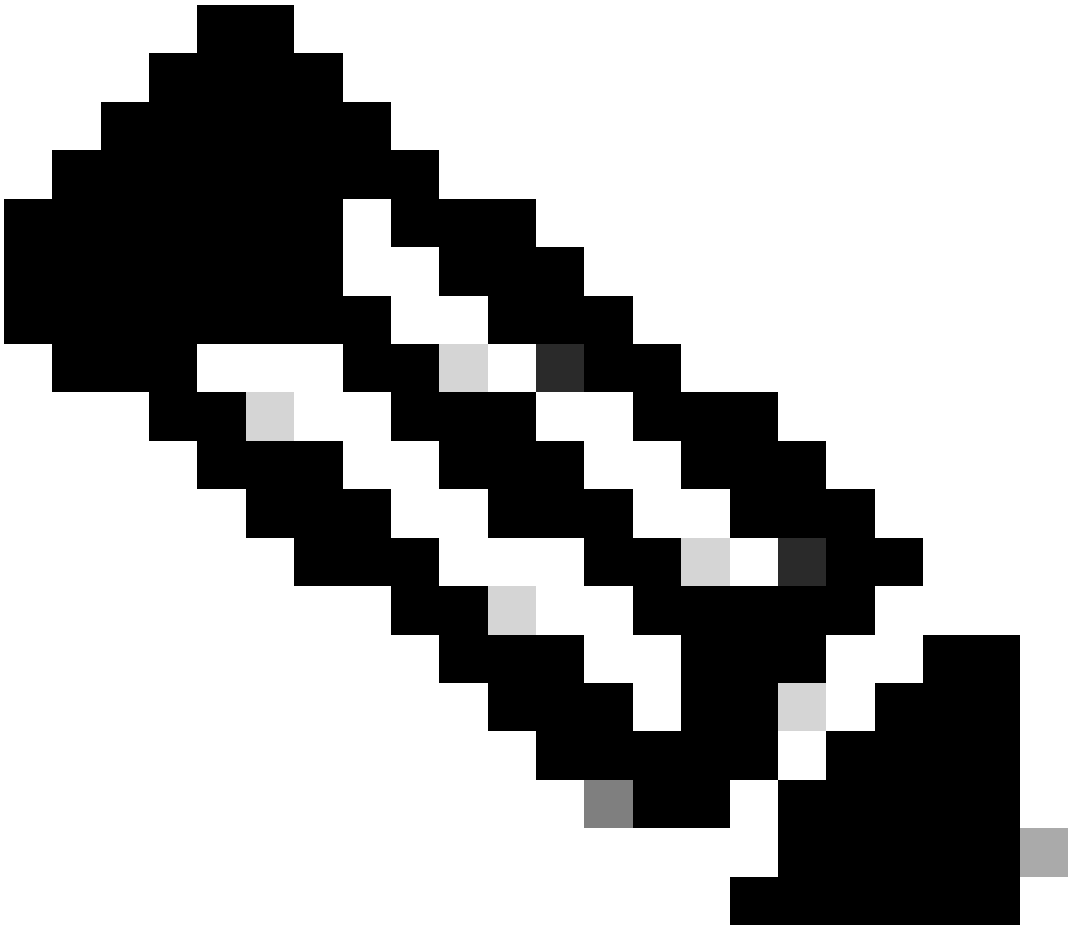
```
group-policy No_Access_Policy internal
group-policy No_Access_Policy attributes
  vpn-simultaneous-logins 0
```

Schritt 2: Konfigurieren der LDAP-Attributzuordnung

Die Attributzuordnung übersetzt LDAP-Attribute in ASA-Attribute, sodass die ASA Benutzer der richtigen Gruppenrichtlinie auf Grundlage ihrer LDAP-Gruppenmitgliedschaften zuweisen kann.

```
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
```



> Anmerkung: Der Distinguished Name (DN) der LDAP-Gruppe muss immer in doppelten Anführungszeichen ("") stehen. So wird sichergestellt, dass die ASA Leerzeichen und Sonderzeichen im DN richtig interpretiert.

Schritt 3: Konfigurieren des LDAP-AAA-Servers

Richten Sie die ASA für die Kommunikation mit dem AD-Server zur Authentifizierung und Gruppenzuordnung ein.

```
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
```

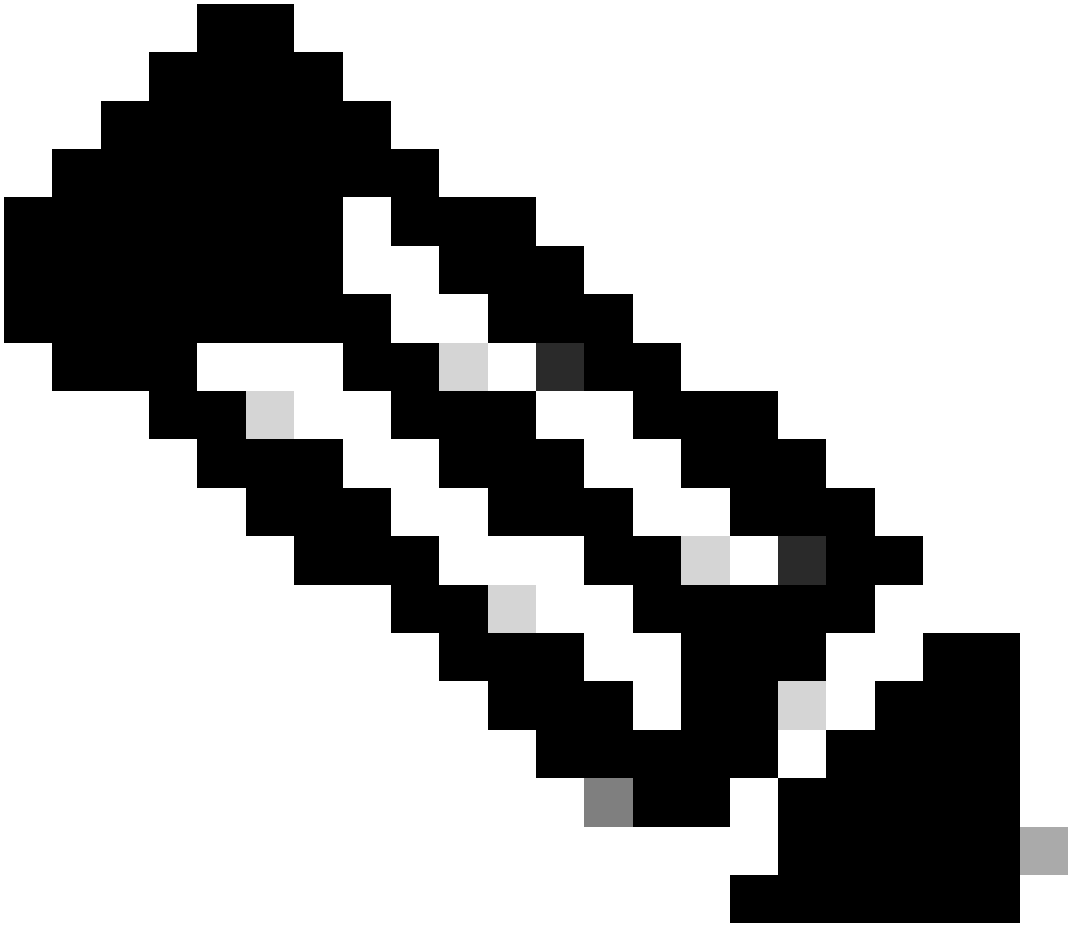
```
  ldap-naming-attribute sAMAccountName
  ldap-login-password ********
  ldap-login-dn CN=ldap_bind_user,OU=Service Accounts,DC=example,DC=com
  ldap-over-ssl enable
  ldap-attribute-map VPN_Access_Map
```

Schritt 4: Definieren der Tunnelgruppe

Die Tunnelgruppe definiert die VPN-Parameter und bindet die Authentifizierung an den 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
```



Anmerkung: Die Standardgruppenrichtlinie ist auf "No_Access_Policy" gesetzt, wodurch der Zugriff für Benutzer verweigert wird, die nicht mit den Zuordnungskriterien für LDAP-Attribute übereinstimmen.

Überprüfung

Überprüfen Sie nach Abschluss der Einrichtung, ob die Benutzer korrekt authentifiziert wurden, und weisen Sie ihnen die entsprechenden Gruppenrichtlinien zu.

VPN-Sitzungszuweisung überprüfen

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

Ersetzen Sie **<Benutzername>** durch das eigentliche Testkonto.

Fehlerbehebung

Verwenden Sie diesen Abschnitt, um Probleme mit Ihrer Konfiguration zu beheben.

LDAP-Debuggen aktivieren

Wenn Benutzer nicht die erwarteten Gruppenrichtlinien erhalten, aktivieren Sie das Debuggen, um Probleme zu identifizieren.

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

VPN-Verbindung initiieren

Lassen Sie einen Testbenutzer versuchen, über den Cisco Secure Client eine Verbindung herzustellen.

Debug-Ausgabe überprüfen

Überprüfen Sie die Cisco ASA-Protokolle, um sicherzustellen, dass der Benutzer der richtigen Gruppenrichtlinie basierend auf seiner Active Directory (AD)-Gruppenmitgliedschaft zugeordnet ist.

Debuggen nach der Überprüfung deaktivieren

```
undebug all
```

Häufige Probleme

Bei LDAP-Attributzuordnungen wird die Groß-/Kleinschreibung berücksichtigt. Stellen Sie sicher, dass die AD-Gruppennamen in den Map-Value-Anweisungen genau übereinstimmen, einschließlich der Groß-/Kleinschreibung.

Überprüfen, ob Benutzer direkte Mitglieder der angegebenen AD-Gruppen sind. Verschachtelte Gruppenmitgliedschaften werden nicht immer erkannt, was zu Autorisierungsproblemen führt.

Benutzer, die keine Zuordnungswertkriterien erfüllen, erhalten die default-group-policy (in diesem Fall No_Access_Policy), wodurch der Zugriff verhindert wird.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.