Konfigurationsbeispiel für LDAP-Attributzuordnungen verwenden

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie jedes Microsoft/AD-Attribut einem Cisco-Attribut zugeordnet werden kann.

Vorgehensweise

1. Führen Sie auf dem Active Directory (AD)-/Lightweight Directory Access Protocol (LDAP)-Server folgende Schritte aus:Wählen Sie **user1 aus**.Klicken Sie mit der rechten Maustaste auf **> Eigenschaften**.Wählen Sie eine Registerkarte aus, die zum Festlegen eines Attributs verwendet werden soll (z. B. die Registerkarte Allgemein).Wählen Sie ein Feld bzw. Attribut, z. B. das Feld Office, aus, mit dem der Zeitbereich erzwungen werden soll, und geben Sie den Bannertext ein (z. B. Welcome to LDAP !!!!). Die Office-Konfiguration in der GUI wird im AD/LDAP-Attribut physicalDeliveryOfficeName gespeichert.
2. Ordnen Sie auf der Adaptive Security Appliance (ASA) zur Erstellung einer LDAP-Attributzuordnungstabelle das AD/LDAP-Attribut physicalDeliveryOfficeName dem ASA-Attribut Banner1 zu:

```
B200-54(config)# show run ldap
ldap attribute-map Banner
map-name physicalDeliveryOfficeName Banner1
```

3. Ordnen Sie die LDAP-Attributzuordnung dem aaa-server-Eintrag zu:

```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map Banner
```

4. Richten Sie die Remotezugriffssitzung ein, und vergewissern Sie sich, dass dem VPN-Benutzer das Banner Welcome to LDAP !!!! angezeigt wird.

Hinzufügen von LDAP-Benutzern zu einer bestimmten Gruppenrichtlinie (Beispiel)

In diesem Beispiel wird die Authentifizierung von user1 auf dem AD-LDAP-Server veranschaulicht. Der Feldwert für die Abteilung wird abgerufen, damit er einer ASA/PIX-Gruppenrichtlinie zugeordnet werden kann, aus der Richtlinien durchgesetzt werden können.

1. Auf dem AD/LDAP-Server:Wählen Sie **user1 aus**.Klicken Sie mit der rechten Maustaste auf **> Eigenschaften**.Wählen Sie eine Registerkarte aus, die zum Festlegen eines Attributs verwendet werden soll (z. B. die Registerkarte Organisation).Wählen Sie ein Feld bzw. Attribut, z. B. "Abteilung", aus, das zum Durchsetzen einer Gruppenrichtlinie verwendet werden soll, und geben Sie den Wert der Gruppenrichtlinie (Group-Policy1) auf der ASA/PIX ein. Die Abteilungskonfiguration auf der GUI wird in der AD/LDAP-Attributabteilung gespeichert.
2. Definieren Sie eine ldap-attribute-map-Tabelle.

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

3. Definieren Sie die Gruppenrichtlinie, Group_policy1, für die Appliance und die erforderlichen Richtlinienattribute.
4. Richten Sie den VPN-Remote-Zugriffstunnel ein, und überprüfen Sie, ob die Sitzung die Attribute von Group-Policy1 (und allen anderen anwendbaren Attributen von der Standardgruppenrichtlinie) übernimmt. **Hinweis**: Fügen Sie der Zuordnung bei Bedarf weitere Attribute hinzu. In diesem Beispiel wird nur das Minimum für die Steuerung dieser Funktion angezeigt (Platzieren Sie einen Benutzer in einer bestimmten ASA/PIX 7.1.x-Gruppenrichtlinie). Das dritte Beispiel zeigt diese Art von Karte.

Konfigurieren einer NOACCESS-Gruppenrichtlinie

Sie können eine NOACCESS-Gruppenrichtlinie erstellen, um die VPN-Verbindung abzulehnen, wenn der Benutzer keiner der LDAP-Gruppen angehört. Dieser Konfigurationsausschnitt wird als Referenz angezeigt:

```
group-policy NOACCESS internal
group-policy NOACCESS attributes
vpn-simultaneous-logins 0
vpn-tunnel-protocol IPSec webvpn
```

Sie müssen diese Gruppenrichtlinie als Standardgruppenrichtlinie auf die Tunnelgruppe anwenden. So können Benutzer, die eine Zuordnung aus der LDAP-Attributzuordnung erhalten, z. B. diejenigen, die einer gewünschten LDAP-Gruppe angehören, ihre gewünschten Gruppenrichtlinien abrufen, und Benutzer, die keine Zuordnung erhalten, z. B. diejenigen, die keiner der gewünschten LDAP-Gruppen angehören, erhalten die NOACCESS-Gruppenrichtlinie aus der Tunnelgruppe, die den Zugriff für sie blockiert.

> **Tipp:** Da das Attribut "vpn-simultan-logins" hier auf 0 gesetzt ist, muss es auch in allen anderen Gruppenrichtlinien explizit definiert werden. Andernfalls kann es von der standardmäßigen Gruppenrichtlinie für diese Tunnelgruppe geerbt werden, die in diesem Fall die NOACCESS-Richtlinie ist.

Richtliniendurchsetzung für gruppenbasierte Attribute (Beispiel)

1. Richten Sie auf dem AD-LDAP-Server, Active Directory-Benutzer und -Computer, einen Benutzerdatensatz (VPNUserGroup) ein, der eine Gruppe darstellt, in der die VPN-Attribute konfiguriert sind.
2. Definieren Sie auf dem AD-LDAP-Server, Active Directory-Benutzer und -Computer, das Feld Abteilung jedes Benutzerdatensatzes, sodass dieser in Schritt 1 auf den Gruppendatensatz (VPNUserGroup) verweist. Der Benutzername in diesem Beispiel lautet web1. **Hinweis**: Das AD-Attribut der Abteilung wurde nur verwendet, weil sich die logische Abteilung auf die Gruppenrichtlinie bezieht. In Wirklichkeit könnte jedes Feld genutzt werden. Dieses Feld muss dem Cisco VPN-Attribut "Group-Policy" (Gruppenrichtlinie) zugeordnet werden, wie in diesem Beispiel gezeigt.
3. Definieren Sie eine ldap-attribute-map-Tabelle:

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department IETF-Radius-Class
map-name description\Banner1
map-name physicalDeliveryOfficeName IETF-Radius-Session-Timeout
5520-1(config)#
```

   Die beiden AD-LDAP-Attribute Description und Office (dargestellt durch AD-Namen description und PhysicalDeliveryOfficeName) sind die Gruppendatensatzattribute (für VPNUSerGroup), die den Cisco VPN-Attributen Banner1 und IETF-Radius-Session-Timeout zugeordnet sind.Das Attribut "department" dient dazu, den Benutzerdatensatz dem Namen der externen Gruppenrichtlinie auf der ASA (VPNUSer) zuzuordnen. Dieser wird dann dem Datensatz "VPNuserGroup" auf dem AD-LDAP-Server zugeordnet, auf dem die Attribute definiert sind.**Hinweis**: Das Cisco-Attribut (Gruppenrichtlinie) muss in der ldap-attribute-map definiert werden. Sein zugeordnetes AD-Attribut kann ein beliebiges einstellbares AD-Attribut sein. In diesem Beispiel wird "department" verwendet, da es sich um den logischsten Namen für die Gruppenrichtlinie handelt.
4. Konfigurieren Sie den aaa-Server mit dem Namen ldap-attribute-map, der für die LDAP-AAA-Vorgänge (Authentication, Authorization, and Accounting) verwendet werden soll:

```
5520-1(config)# show runn aaa-server LDAP-AD11
aaa-server LDAP-AD11 protocol ldap
aaa-server LDAP-AD11 host 10.148.1.11
ldap-base-dn cn=Users,dc=nelson,dc=cisco,dc=com
ldap-scope onelevel
ldap-naming-attribute sAMAccountName
ldap-login-password altiga
```

```
ldap-login-dn cn=Administrator,cn=Users,dc=nelson,dc=cisco,dc=com
ldap-attribute-map Our-AD-Map
5520-1(config)#
```

5. Definieren Sie eine Tunnelgruppe mit entweder LDAP-Authentifizierung oder LDAP-Autorisierung. Beispiel mit LDAP-Authentifizierung. Erzwingung von Richtlinien für Authentifizierungs- und (Autorisierungs-)Attribute, wenn Attribute definiert sind
```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group LDAP-AD11
accounting-server-group RadiusACS28
5520-1(config)#
```
Beispiel mit LDAP-Autorisierung. Für digitale Zertifikate verwendete Konfiguration.
```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group none
authorization-server-group LDAP-AD11
accounting-server-group RadiusACS28
authorization-required
authorization-dn-attributes ea
5520-1(config)#
```
6. Definieren einer externen Gruppenrichtlinie Der Name der Gruppenrichtlinie ist der Wert des AD-LDAP-Benutzerdatensatzes, der die Gruppe darstellt (VPNUserGroup).
```
5520-1(config)# show runn group-policy VPNUserGroup
group-policy VPNUserGroup external server-group LDAP-AD11
5520-1(config)#
```
7. Richten Sie den Tunnel ein, und überprüfen Sie, ob Attribute durchgesetzt werden. In diesem Fall werden Banner und Sitzungstimeout vom VPNuserGroup-Datensatz im AD erzwungen.

Active Directory-Durchsetzung von "Zuweisen einer statischen IP-Adresse" für IPsec- und SVC-Tunnel

Das AD-Attribut lautet msRADIUSFramedIPAddress. Das Attribut wird in den AD-Benutzereigenschaften, auf der Registerkarte Einwählen und unter Statische IP-Adresse zuweisen konfiguriert.

So gehen Sie vor:

1. Geben Sie auf dem AD-Server unter Benutzereigenschaften, Registerkarte Einwählen, Statische IP-Adresse zuweisen den Wert der IP-Adresse ein, die der IPsec/SVC-Sitzung zugewiesen werden soll (10.20.30.6).
2. Erstellen Sie auf der ASA eine ldap-attribute-map mit der folgenden Zuordnung:
```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFramedIPAddress IETF-Radius-Framed-IP-Address
5540-1#
```
3. Überprüfen Sie auf der ASA, ob die VPN-Adresszuweisung für "vpn-addr-assign-aaa" konfiguriert ist:
```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```
4. Richten Sie die IPsec/SVC Remote Authority (RA)-Sitzungen ein, und überprüfen Sie mit show vpn-sessiondb remote|svc, ob das Feld Zugewiesene IP korrekt ist (10.20.30.6).

Active Directory-Durchsetzung von "Remote Access Permission Dial-in, Allow/Deny Access"

Unterstützt alle VPN Remote Access-Sitzungen: IPSec, WebVPN und SVC. Allow Access hat den Wert TRUE. 'Zugriff verweigern' hat den Wert FALSE. Der AD-Attributname lautet msNPAllowDialin.

In diesem Beispiel wird die Erstellung einer LDAP-Attributzuordnung veranschaulicht, die mithilfe der Cisco Tunneling-Protokolle die Allow Access (TRUE)- und Deny (FALSE)-Bedingungen erstellt. Wenn Sie beispielsweise das tunnel-protocol=L2TPover IPsec (8) zuordnen, können Sie eine FALSE-Bedingung erstellen, wenn Sie versuchen, den Zugriff für WebVPN und IPsec durchzusetzen. Auch die umgekehrte Logik gilt.

So gehen Sie vor:

1. Wählen Sie auf dem AD-Server user1 Properties, Dial-In (Einwählen) die entsprechende Option zum Zulassen des Zugriffs oder Verweigern des Zugriffs für jeden Benutzer aus.
   Hinweis: Wenn Sie die dritte Option, Zugriff über die RAS-Richtlinie steuern, auswählen, wird vom AD-Server kein Wert zurückgegeben. Die durchgesetzten Berechtigungen basieren daher auf der Einstellung der internen Gruppenrichtlinie von ASA/PIX.
2. Erstellen Sie auf der ASA eine ldap-attribute-map mit folgender Zuordnung:
   ```
   ldap attribute-map LDAP-MAP
   map-name msNPAllowDialin Tunneling-Protocols
   map-value msNPAllowDialin FALSE 8
   map-value msNPAllowDialin TRUE 20
   5540-1#
   ```
   Hinweis: Fügen Sie der Zuordnung bei Bedarf weitere Attribute hinzu. In diesem Beispiel wird nur das Minimum für die Steuerung dieser Funktion angezeigt (Zulassen oder Verweigern des Zugriffs basierend auf der Einwahleinstellung).Was bedeutet "ldap-attribute-map" und was wird durchgesetzt?Kartenwert msNPAllowDialin FALSE 8Zugriff für einen Benutzer verweigern1. Die Bedingung für den FALSE-Wert entspricht dem Tunnelprotokoll L2TPoverIPsec (Wert 8).Zugriff für Benutzer zulassen2. Der TRUE-Wert entspricht dem Tunnelprotokoll WebVPN + IPsec (Wert 20).Ein WebVPN/IPsec-Benutzer, der auf AD als user1 authentifiziert wird, schlägt aufgrund der Tunnel-Protokoll-Diskrepanz fehl.Ein L2TPoverIPsec, das auf AD als user1 authentifiziert wird, würde aufgrund der Deny-Regel fehlschlagen.Ein WebVPN/IPsec-Benutzer, der auf AD als user2 authentifiziert wurde, würde erfolgreich sein (Regel zulassen + übereinstimmendes Tunnelprotokoll).Ein L2TPoverIPsec, das auf AD als user2 authentifiziert wird, würde aufgrund der Tunnel-Protokoll-Diskrepanz fehlschlagen.
   Unterstützung für Tunnel Protocol, wie in RFCs 2867 und 2868 definiert.

Active Directory-Durchsetzung von "Member Of"/Gruppenmitgliedschaft zum Zulassen oder Verweigern des Zugriffs

Dieser Fall steht in engem Zusammenhang mit Fall 5 und bietet einen logischeren Ablauf. Dies ist die empfohlene Methode, da die Gruppenmitgliedschaftsprüfung als Bedingung festgelegt wird.

1. Konfigurieren Sie den AD-Benutzer als Mitglied einer bestimmten Gruppe. Verwenden Sie einen Namen, der sie an die Spitze der Gruppenhierarchie setzt (ASA-VPN-Consultants). In AD-LDAP wird die Gruppenmitgliedschaft durch das AD-Attribut memberOf definiert. Es ist

wichtig, dass die Gruppe an der Spitze der Liste steht, da Sie die Regeln derzeit nur auf die erste group/memberOf-Zeichenfolge anwenden können. In Version 7.3 können Sie die Filterung und Durchsetzung mehrerer Gruppen durchführen.

2. Erstellen Sie auf der ASA eine ldap-attribute-map mit der minimalen Zuordnung:
```
ldap attribute-map LDAP-MAP
map-name memberOf Tunneling-Protocols
map-value memberOf cn=ASA-VPN-Consultants,cn=Users,dc=abcd,dc=com 4
5540-1#
```
Hinweis: Fügen Sie der Zuordnung bei Bedarf weitere Attribute hinzu. In diesem Beispiel wird nur das Minimum für die Steuerung dieser Funktion angezeigt (Zulassen oder Verweigern des Zugriffs basierend auf der Gruppenmitgliedschaft).Was bedeutet "ldap-attribute-map" und was wird durchgesetzt?User=joe_consultant, ein Teil von AD, das Mitglied der AD-Gruppe ASA-VPN-Consultants ist, kann nur auf IPsec (tunnel-protocol=4=IPSec) zugreifen.User=joe_consultant, Teil von AD, kann den VPN-Zugriff während eines anderen RAS-Clients (PPTP/L2TP, L2TP/IPSec, WebVPN/SVC usw.) versagen.User=bill_the_hacker kann NICHT zugelassen werden, da der Benutzer keine AD-Mitgliedschaft hat.

Active Directory-Durchsetzung von "Anmeldezeiten/Tageszeitregeln"

In diesem Anwendungsfall wird beschrieben, wie Sie die Tageszeitregeln für AD/LDAP einrichten und durchsetzen.

Gehen Sie folgendermaßen vor:

1. Auf dem AD/LDAP-Server:Wählen Sie den Benutzer aus.Klicken Sie mit der rechten Maustaste auf **> Eigenschaften**.Wählen Sie eine Registerkarte, die verwendet werden soll, um ein Attribut festzulegen (Beispiel: Registerkarte Allgemein).Wählen Sie ein Feld bzw. ein Attribut, z. B. das Feld Office, aus, das zum Erzwingen des Zeitbereichs verwendet werden soll, und geben Sie den Namen des Zeitbereichs ein (z. B. Boston). Die Office-Konfiguration in der GUI wird im AD/LDAP-Attribut physicalDeliveryOfficeName gespeichert.
2. Auf der ASA Erstellen Sie eine LDAP-Attributzuordnungstabelle.Ordnen Sie das AD/LDAP-Attribut "physicalDeliveryOfficeName" dem ASA-Attribut "Access-Hours" zu.Beispiel:
```
B200-54(config-time-range)# show run ldap
ldap attribute-map TimeOfDay
map-name physicalDeliveryOfficeName Access-Hours
```
3. Ordnen Sie auf der ASA die LDAP-Attributzuordnung dem aaa-server-Eintrag zu:
```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map TimeOfDay
```
4. Erstellen Sie auf dem ASA-Gerät ein Zeitbereichsobjekt mit dem dem Benutzer zugewiesenen Namenswert (Office-Wert in Schritt 1):
```
B200-54(config-time-range)# show runn time-range
!
time-range Boston
periodic weekdays 8:00 to 17:00
!
```
5. Einrichten der VPN-Remotezugriffssitzung: Die Sitzung kann erfolgreich sein, wenn sie

innerhalb des Zeitbereichs liegt.Die Sitzung kann fehlschlagen, wenn sie außerhalb des Zeitbereichs liegt.

Verwenden Sie die ldap-map-Konfiguration, um einen Benutzer einer bestimmten Gruppenrichtlinie zuzuordnen, und verwenden Sie im Fall einer doppelten Authentifizierung den Befehl "authentication-server-group".

1. In diesem Szenario wird die doppelte Authentifizierung verwendet. Der erste verwendete Authentifizierungsserver ist RADIUS, und der zweite verwendete Authentifizierungsserver ist ein LDAP-Server. Konfigurieren Sie den LDAP- und den RADIUS-Server. Hier ein Beispiel:

```
ASA5585-S10-K9# show runn aaa-server
aaa-server test-ldap protocol ldap
aaa-server test-ldap (out) host 10.201.246.130
 ldap-base-dn cn=users, dc=htts-sec, dc=com
 ldap-login-password *****
 ldap-login-dn cn=Administrator, cn=Users, dc=htts-sec, dc=com
 server-type microsoft
 ldap-attribute-map Test-Safenet-MAP
aaa-server test-rad protocol radius
aaa-server test-rad (out) host 10.201.249.102
 key *****
```

   Definieren Sie die LDAP-Attributzuordnung. Hier ein Beispiel:

```
ASA5585-S10-K9# show runn ldap
ldap attribute-map Test-Safenet-MAP
map-name memberOf IETF-Radius-Class
map-value memberOf "CN=DHCP Users,CN=Users,DC=htts-sec,DC=com" Test-Policy-Safenet
```

   Definieren Sie die Tunnelgruppe, und ordnen Sie den RADIUS- und LDAP-Server für die Authentifizierung zu. Hier ein Beispiel:

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

   Zeigen Sie die Gruppenrichtlinie an, die in der Tunnelgruppenkonfiguration verwendet wird:

```
ASA5585-S10-K9# show runn group-policy
group-policy NoAccess internal
group-policy NoAccess attributes
wins-server none
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 0
default-domain none
group-policy Test-Policy-Safenet internal
group-policy Test-Policy-Safenet attributes
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 15
vpn-idle-timeout 30
vpn-tunnel-protocol ikev1 ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Safenet-Group-Policy-SplitAcl
default-domain none
```

   Bei dieser Konfiguration wurden AnyConnect-Benutzer, die der Verwendung von LDAP-Attributen korrekt zugeordnet wurden, nicht in der Gruppenrichtlinie "Test-Policy-Safenet" platziert. Stattdessen wurden sie immer noch in die Standard-Gruppenrichtlinie, in diesem

Fall NoAccess, eingefügt.Siehe den Ausschnitt der debugs (debug ldap 255) und syslogs auf der Informationsebene:

```
--------------------------------------------------------------------------------

memberOf: value = CN=DHCP Users,CN=Users,DC=htts-sec,DC=com

[47]                        mapped to IETF-Radius-Class: value = Test-Policy-Safenet

[47]                        mapped to LDAP-Class: value = Test-Policy-Safenet

--------------------------------------------------------------------------------

Syslogs :

%ASA-6-113004: AAA user authentication Successful : server = 10.201.246.130 : user =
test123

%ASA-6-113003: AAA group policy for user test123 is set to Test-Policy-Safenet

%ASA-6-113011: AAA retrieved user specific group policy (Test-Policy-Safenet) for user =
test123

%ASA-6-113009: AAA retrieved default group policy (NoAccess) for user = test123

%ASA-6-113013: AAA unable to complete the request Error : reason = Simultaneous logins
exceeded for user : user = test123

%ASA-6-716039: Group <DfltGrpPolicy> User <test123> IP <10.116.122.154> Authentication:
rejected, Session Type: WebVPN.
```

Diese Syslogs zeigen einen Fehler an, da dem Benutzer die NoAccess-Gruppenrichtlinie zugewiesen wurde, für die simultane Anmeldung auf 0 gesetzt war, obwohl Syslogs angeben, dass eine benutzerspezifische Gruppenrichtlinie abgerufen wurde.Um den Benutzer anhand der LDAP-Zuordnung in der Gruppenrichtlinie zuweisen zu lassen, benötigen Sie den folgenden Befehl: **authorization-server-group test-ldap (**in diesem Fall ist **test-ldap** der LDAP-Servername). Hier ein Beispiel:

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
authorization-server-group test-ldap
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

2. Wenn nun der erste Authentifizierungsserver (in diesem Beispiel RADIUS) die benutzerspezifischen Attribute gesendet hat, z. B. das IEFT-class-Attribut, kann der Benutzer der von RADIUS gesendeten Gruppenrichtlinie zugeordnet werden. Obwohl also auf dem sekundären Server eine LDAP-Zuordnung konfiguriert ist und die LDAP-Attribute des Benutzers den Benutzer einer anderen Gruppenrichtlinie zuordnen, kann die vom ersten Authentifizierungsserver gesendete Gruppenrichtlinie durchgesetzt werden. Damit der Benutzer anhand des LDAP-Zuordnungsattributs in eine Gruppenrichtlinie eingefügt wird, müssen Sie diesen Befehl unter tunnel-group: **authorization-server-group test-ldap** angeben.
3. Wenn der erste Authentifizierungsserver SDI oder OTP ist, der das benutzerspezifische Attribut nicht übergeben kann, fällt der Benutzer in die Standardgruppenrichtlinie der Tunnelgruppe. In diesem Fall ist NoAccess, obwohl die LDAP-Zuordnung richtig ist. In diesem Fall benötigen Sie außerdem den Befehl **authorization-server-group test-ldap** unter

der tunnel-group, damit der Benutzer in die richtige Gruppenrichtlinie aufgenommen wird.
4. Wenn beide Server dieselben RADIUS- oder LDAP-Server sind, benötigen Sie den Befehl **authentication-server-group** nicht, damit die Gruppenrichtliniensperre funktioniert.

Überprüfung

```
ASA5585-S10-K9# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : test123                  Index        : 2
Assigned IP  : 10.34.63.1             Public IP    : 10.116.122.154
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : 3DES 3DES 3DES         Hashing      : SHA1 SHA1 SHA1
Bytes Tx     : 14042                  Bytes Rx     : 8872
Group Policy : Test-Policy-Safenet    Tunnel Group : Test_Safenet
Login Time   : 10:45:28 UTC Fri Sep 12 2014
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Fehlerbehebung

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

Debuggen der LDAP-Transaktion

Diese Debugs können verwendet werden, um Probleme mit der DAP-Konfiguration zu isolieren:

- debug ldap 255
- debug dap trace
- debuggen aaa-Authentifizierung

ASA kann keine Benutzer vom LDAP-Server authentifizieren

Falls die ASA keine Benutzer vom LDAP-Server authentifizieren kann, sind hier einige Beispiele für Fehlerbehebungen:

```
ldap 255 output:[1555805] Session Start[1555805] New request Session, context
0xcd66c028, reqType = 1[1555805]
Fiber started[1555805] Creating LDAP context with uri=ldaps://172.30.74.70:636
[1555805] Connect to LDAP server:
ldaps://172.30.74.70:636, status = Successful[1555805] supportedLDAPVersion:
value = 3[1555805]
supportedLDAPVersion: value = 2[1555805] Binding as administrator[1555805]
Performing Simple
authentication for sysservices to 172.30.74.70[1555805] Simple authentication
for sysservices returned code (49)
Invalid credentials[1555805] Failed to bind as administrator returned code
(-1) Can't contact LDAP server[1555805]
Fiber exit Tx=222 bytes Rx=605 bytes, status=-2[1555805] Session End
```

Bei diesen Fehlerbehebungen ist entweder das LDAP-Anmelde-DN-Format falsch oder das Kennwort falsch. Überprüfen Sie daher beide, um das Problem zu beheben.

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.