Configuratievoorbeeld van LDAP-kenmerken gebruiken

Inhoud

Inleiding

Dit document beschrijft hoe Microsoft/AD-kenmerken aan een Cisco-kenmerk kunnen worden toegewezen.

Procedure

1. Op de LDAP-server (Active Directory)/Lichtgewicht Directory Access Protocol:Kies **gebruiker1**.Klik met de rechtermuisknop **> Eigenschappen**.Kies een tabblad dat gebruikt moet worden om een kenmerk in te stellen (bijvoorbeeld het tabblad Algemeen).Kies een veld/attribuut, bijvoorbeeld het veld Office, dat gebruikt moet worden om tijdbereik af te dwingen en voer de bannertekst in (bijvoorbeeld Welkom bij LDAP !!!!). De Office-configuratie op de GUI wordt opgeslagen in het AD/LDAP-kenmerk PhysicalDeliveryOfficeName.
2. In de adaptieve security applicatie (ASA), om een LDAP attribuut mapping tabel te maken, brengt u het AD/LDAP attribuut PhysicalDeliveryOfficeName in kaart aan het ASA attribuut Banner1:

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

3. Koppel de LDAP-kenmerkkaart aan de aaaserver:

```
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. Stel de sessie voor externe toegang in en controleer of de Banner Welcome to LDAP !!!! aan de VPN-gebruiker wordt getoond.

Plaats LDAP-gebruikers in een specifiek groepsbeleid (generiek voorbeeld)

Dit voorbeeld demonstreert de authenticatie van user1 op de AD-LDAP server en haalt de waarde van het afdelingsveld op, zodat het kan worden toegewezen aan een ASA/PIX groep-beleid van waaruit beleid kan worden afgedwongen.

1. Op de AD/LDAP-server:Kies **gebruiker1**.Klik met de rechtermuisknop **> Eigenschappen**.Kies een tabblad dat gebruikt moet worden om een kenmerk in te stellen (bijvoorbeeld het tabblad Organisatie).Kies een veld/attribuut, bijvoorbeeld Department, dat gebruikt moet worden om een groepsbeleid af te dwingen en voer de waarde van het groepsbeleid (Group-Policy1) in op de ASA/PIX. De departementsconfiguratie op de GUI wordt opgeslagen in de AD/LDAP attributenafdeling.
2. Definieer een ldap-attribuut-map tabel.

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

3. Definieer het groepsbeleid, Group_policy1, voor het apparaat en de gewenste beleidskenmerken.
4. Stel de externe VPN-toegangstunnel in en controleer of de sessie de kenmerken van Group-Policy1 (en eventuele andere toepasselijke kenmerken van het standaardgroepsbeleid) erft. **Opmerking**: Voeg indien nodig meer attributen toe aan de kaart. Dit voorbeeld toont alleen het minimum om deze specifieke functie te besturen (plaats een gebruiker in een specifiek ASA/PIX 7.1.x groepsbeleid). Het derde voorbeeld toont dit type kaart.

Een beleid voor een NOACCESS-groep configureren

U kunt een NOACCESS-groepsbeleid maken om de VPN-verbinding te weigeren wanneer de gebruiker geen deel uitmaakt van een van de LDAP-groepen. Dit configuratiefragment wordt getoond voor uw verwijzing:

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

U moet dit groepsbeleid als standaardgroepsbeleid toepassen op de tunnelgroep. Dit stelt gebruikers die een afbeelding krijgen van de LDAP attributenkaart, bijvoorbeeld, degenen die behoren tot een gewenste LDAP groep, om hun gewenste groepsbeleid te krijgen, en gebruikers die geen afbeelding krijgen, bijvoorbeeld, degenen die niet behoren tot een van de gewenste

LDAP groepen, om NOACCESS groep-beleid van de tunnel-groep te krijgen, die de toegang voor hen blokkeert.

> **Tip**: Aangezien het kenmerk vpn-gelijktijdige-logins hier op 0 is ingesteld, moet het ook expliciet worden gedefinieerd in alle andere groepsbeleidsregels; anders kan het worden geërfd van het standaardgroepsbeleid voor die tunnelgroep, wat in dit geval het NOACCESS-beleid is.

Beleidshandhaving op basis van groepskenmerken (voorbeeld)

1. Stel op de AD-LDAP-server, Active Directory-gebruikers en computers een gebruikersrecord (VPNUserGroup) in dat een groep vertegenwoordigt waarin de VPN-kenmerken zijn geconfigureerd.
2. Op de AD-LDAP server, Active Directory Gebruikers en Computers, definieert het Departement van elk gebruikersrecord om in Stap 1 naar de groepsrecord (VPNUserGroup) te wijzen. De gebruikersnaam in dit voorbeeld is web1. **Opmerking**: Het AD-kenmerk van het ministerie werd alleen gebruikt omdat logischerwijs de afdeling verwijst naar het groepsbeleid. In werkelijkheid kan elk veld gebruikt worden. Het vereiste is dat dit veld moet worden toegewezen aan het Cisco VPN-kenmerk Group-Policy zoals in dit voorbeeld.
3. Definieer een ldap-attribuut-map tabel:

```
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)#
```

   De twee AD-LDAP attributen, Description and Office, (vertegenwoordigd door AD name en PhysicalDeliveryOfficeName) zijn de groepsrecord attributen (voor VPNUSerGroup) die in kaart worden gebracht aan Cisco VPN attributen Banner1 en IETF-Radius-Session-Timeout.Het departementsattribuut is voor het gebruikersverslag om aan de naam van extern groepsbeleid op ASA (VPNUSer) in kaart te brengen, die dan terug naar het verslag VPNuserGroup op de AD-LDAP server in kaart brengt, waar de attributen worden bepaald.**Opmerking**: het Cisco-kenmerk (Groepsbeleid) moet in de aldap-attribuut-map worden gedefinieerd. Zijn in kaart gebrachte AD-attributen kunnen om het even welk settable AD attribuut zijn. Dit voorbeeld gebruikt afdeling omdat het de meest logische naam is die verwijst naar groepsbeleid.
4. Configureer de aaa-server met de naam van de ldap-attribuut-map die moet worden gebruikt voor LDAP-verificatie, -autorisatie en -accounting (AAA) bewerkingen:

```
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. Definieer een tunnelgroep met LDAP-verificatie of LDAP-autorisatie. Voorbeeld met LDAP-verificatie. Voert authenticatie + (autorisatie) attribuut beleidshandhaving uit als attributen

worden gedefinieerd.

```
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)#
```

Voorbeeld met LDAP-autorisatie. Configuratie gebruikt voor digitale certificaten.

```
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. Bepaal een extern groepsbeleid. De naam van het groepsbeleid is de waarde van het AD-LDAP gebruikersrecord dat de groep vertegenwoordigt (VPNUserGroup).

```
5520-1(config)# show runn group-policy VPNUserGroup
group-policy VPNUserGroup external server-group LDAP-AD11
5520-1(config)#
```

7. Stel de tunnel in en controleer of de eigenschappen worden afgedwongen. In dit geval worden de Banner en Session-Timeout afgedwongen vanuit het VPN-gebruikersgroeprecord op de AD.

Active Directory-afdwingbaarheid van "Een statisch IP-adres toewijzen" voor IPsec- en SVC-tunnels

Het AD-kenmerk is msRADIUSFramedIPAddress. Het kenmerk is ingesteld in AD Gebruikerseigenschappen, tabblad Inbellen, Statisch IP-adres toewijzen.

Dit zijn de stappen:

1. Voer op de advertentieserver, onder Gebruikerseigenschappen, tabblad Inbellen, Een statisch IP-adres toewijzen, de waarde van het IP-adres in om deze toe te wijzen aan de IPsec/SVC-sessie (10.20.30.6).
2. Maak op de ASA een ldap-attribuut-map met deze afbeelding:

```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFramedIPAddress IETF-Radius-Framed-IP-Address
5540-1#
```

3. Controleer in de ASA of de VPN-adrestoewijzing zo is geconfigureerd dat deze vpn-addr-allocation-aaa omvat:

```
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. Stel de IPsec/SVC Remote Authority (RA)-sessies in en controleer of het display VPN-sessiondb remote|svc juist is door het toegewezen IP-veld (10.20.30.6).

Active Directory-afdwinging van "Remote Access Permission Dial-in, Allow/Deny Access"

Ondersteunt alle VPN Remote Access sessies: IPSec, WebVPN en SVC. Allow Access heeft een waarde van TRUE. Deny Access heeft een waarde van FALSE. De naam van het AD-kenmerk is msNPAllowDialin.

Dit voorbeeld toont de verwezenlijking van een ldap-attribuut-kaart aan die Cisco Tunneling-Protocollen gebruikt om te creëren toestaan Toegang (WAAR) en ontkennen (VALS) voorwaarden. Als u bijvoorbeeld het tunnelprotocol=L2TPover IPsec (8) in kaart brengt, kunt u een FALSE-voorwaarde maken als u probeert toegang voor WebVPN en IPsec af te dwingen. De omgekeerde logica is ook van toepassing.

Dit zijn de stappen:

1. Kies in de AD-servergebruiker1 Eigenschappen, Inbellen, de juiste optie Toegang toestaan of Toegang weigeren voor elke gebruiker. **Opmerking**: Als u de derde optie, Toegang beheren via het beleid voor externe toegang kiest, wordt er geen waarde teruggegeven van de AD-server, zodat de afgedwongen toegangsrechten zijn gebaseerd op de instelling van de interne groep-beleid van ASA/PIX.
2. Voor ASA, creeer een lap-attribuut-kaart met deze afbeelding:
   ```
   ldap attribute-map LDAP-MAP
   map-name msNPAllowDialin Tunneling-Protocols
   map-value msNPAllowDialin FALSE 8
   map-value msNPAllowDialin TRUE 20
   5540-1#
   ```
   Opmerking: Voeg indien nodig meer attributen toe aan de kaart. Dit voorbeeld toont alleen het minimum om deze specifieke functie te besturen (Toegang toestaan of weigeren op basis van inbellen).Wat betekent ldap-attribuut-map of forceert het?map-waarde msNPAlowDialin FALSE 8Toegang weigeren voor een gebruiker1. De FALSE-waardeomstandigheid wordt toegewezen aan het tunnelprotocol L2TPover IPsec (waarde 8).Toestaan van toegang voor gebruiker2 . De TRUE-waarde staat in kaart met het tunnelprotocol WebVPN + IPsec, (waarde 20).Een WebVPN/IPsec-gebruiker, die als gebruiker1 op AD is geauthenticeerd, zou falen vanwege een foutieve tunnelovereenkomst.Een L2TPover IPsec, dat als user1 op AD is geauthenticeerd, zou falen vanwege de regel Deny.Een WebVPN/IPsec-gebruiker, die als gebruiker2 op AD is geauthenticeerd, zou slagen (regel toestaan + overeenkomend tunnelprotocol).Een L2TPover IPsec, dat als user2 op AD is geauthenticeerd, zou falen vanwege een foutieve tunnelovereenkomst.
   Ondersteuning voor tunnelprotocol, zoals gedefinieerd in RFC's 2867 en 2868.

Active Directory-handhaving van "Lid van"/groepslidmaatschap om toegang toe te staan of te weigeren

Dit geval is nauw verwant aan geval 5, en voorziet in een logischere stroom, en is de aanbevolen methode, aangezien het de groepslidmaatschapscontrole als voorwaarde stelt.

1. Configureer de AD-gebruiker om lid te zijn van een specifieke groep. Gebruik een naam die de naam bovenaan de groepshiërarchie plaatst (ASA-VPN-Consultants). In AD-LDAP wordt groepslidmaatschap gedefinieerd door het AD attribuut memberOf. Het is belangrijk dat de groep bovenaan de lijst staat, omdat je op dit moment alleen de regels op de eerste groep/memberOf string kunt toepassen. In release 7.3 kunt u filtering en handhaving in meerdere groepen uitvoeren.
2. Voor ASA, creeer een ldap-attribuut-kaart met de minimumafbeelding:

```
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#
```

Opmerking: Voeg indien nodig meer attributen toe aan de kaart. Deze voorbeelden tonen slechts het minimum om deze specifieke functie (sta of ontken toegang toe die op het lidmaatschap van de Groep wordt gebaseerd) te controleren.Wat betekent ldap-attribuut-map of forceert het?Gebruiker=joe_consultant, onderdeel van AD, dat lid is van de AD-groep ASA-VPN-Consultants, kan alleen toegang krijgen als de gebruiker IPsec gebruikt (tunnelprotocol=4=IPSec).Gebruiker=joe_consultant, onderdeel van AD, kan VPN-toegang mislukken tijdens een andere client voor externe toegang (PPTP/L2TP, L2TP/IPSec, WebVPN/SVC, enzovoort).User=bill_the_hacker kan NIET worden toegestaan in aangezien de gebruiker geen AD-lidmaatschap heeft.

Active Directory-afdwinging van "aanmeldingstijden/tijdregels"

In deze gebruikscase wordt beschreven hoe de Time of Day-regels voor AD/LDAP moeten worden ingesteld en gehandhaafd.

Hier is de procedure om dit te doen:

1. Op de AD/LDAP-server:Kies de gebruiker.Klik met de rechtermuisknop **> Eigenschappen**.Kies een tabblad dat gebruikt moet worden om een kenmerk in te stellen (tabblad Voorbeeld. Algemeen).Kies een veld/kenmerk, bijvoorbeeld het veld Office, dat moet worden gebruikt om tijdbereik af te dwingen en voer de naam van het tijdbereik in (bijvoorbeeld Boston). De Office-configuratie op de GUI wordt opgeslagen in het AD/LDAP-kenmerk PhysicalDeliveryOfficeName.
2. Op de ASA Maak een LDAP attribuut mapping tabel.Stel het AD/LDAP-kenmerk "PhysicalDeliveryOfficeName" in op het ASA-kenmerk "Access-Hours".Voorbeeld:
```
B200-54(config-time-range)# show run ldap
ldap attribute-map TimeOfDay
map-name physicalDeliveryOfficeName Access-Hours
```
3. In de ASA, associeer de LDAP attributenkaart aan de aaa-server ingang:
```
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. Voor ASA, creeer een tijd-bereik voorwerp dat de naamwaarde heeft die aan de gebruiker wordt toegewezen (de waarde van het Bureau in stap 1):
```
B200-54(config-time-range)# show runn time-range
!
time-range Boston
periodic weekdays 8:00 to 17:00
!
```
5. De sessie voor externe VPN-toegang instellen: De sessie kan slagen als het binnen de tijdspanne gebeurt.De sessie kan mislukken als ze buiten het tijdbereik valt.

Gebruik de ldap-map Configuration om een gebruiker in een specifiek groep-beleid

te koppelen en gebruik het autorisatie-server-groep commando, in het geval van dubbele verificatie

1. In dit scenario wordt dubbele verificatie gebruikt. De eerste gebruikte verificatieserver is RADIUS en de tweede gebruikte verificatieserver is een LDAP-server. Configureer de LDAP-server en de RADIUS-server. Hierna volgt een voorbeeld:

```
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 *****
```

   Bepaal de LDAP attribuut-map. Hierna volgt een voorbeeld:

```
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
```

   Definieer de tunnelgroep en koppel de RADIUS- en LDAP-server aan voor verificatie. Hierna volgt een voorbeeld:

```
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
```

   Bekijk het groepsbeleid dat in de tunnelgroepsconfiguratie wordt gebruikt:

```
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
```

   Met deze configuratie werden AnyConnect-gebruikers die correct met het gebruik van LDAP-kenmerken waren toegewezen, niet in het groepsbeleid, Test-Policy-Safenet geplaatst. In plaats daarvan werden ze nog steeds geplaatst in het standaardgroepsbeleid, in dit geval NoAccess.Zie het fragment van debugs (debug ldap 255) en syslogs op niveau informatie:

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

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.
```

Deze syslogs tonen mislukking aangezien de gebruiker het NoAccess groep-beleid werd gegeven dat had gelijktijdige-login ingesteld op 0 alhoewel syslogs zeggen het een gebruiker specifieke groep-beleid terugwon.Om de gebruiker toegewezen te krijgen in het groepsbeleid, gebaseerd op de LDAP-map, moet u deze opdracht hebben: **autorisatie-server-groep test-ldap** (in dit geval is **test-ldap** de LDAP-servernaam). Hierna volgt een voorbeeld:

```
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. Als de eerste verificatieserver (RADIUS, in dit voorbeeld) de gebruikerspecifieke kenmerken heeft verzonden, bijvoorbeeld het kenmerk IEFT-klasse, dan kan de gebruiker worden toegewezen aan het groepsbeleid dat door RADIUS wordt verzonden. Dus hoewel de secundaire server een LDAP-kaart heeft geconfigureerd en de LDAP-kenmerken van de gebruiker de gebruiker in kaart brengen naar een ander groepsbeleid, kan het groepsbeleid dat door de eerste verificatieserver wordt verzonden, worden afgedwongen. Om de gebruiker in een groepsbeleid te plaatsen dat op de LDAP-kaartattributen is gebaseerd, moet u deze opdracht opgeven onder de tunnelgroep: **autorisatie-server-groep test-ldap**.
3. Als de eerste verificatieserver SDI of OTP is, die het gebruikerspecifieke kenmerk niet kan doorgeven, dan valt de gebruiker in het standaardgroepsbeleid van de tunnelgroep. In dit geval, NoAccess, ook al is de LDAP-afbeelding correct. In dit geval, zou u ook het bevel, **vergunning-server-groep test-ldap** nodig hebben, onder de tunnel-groep voor de gebruiker om in het juiste groep-beleid worden geplaatst.
4. Als beide servers dezelfde RADIUS- of LDAP-servers zijn, hebt u de opdracht **autorisatieserver-groep** niet nodig om de groepsbeleidsvergrendeling te laten werken.

Verifiëren

```
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
```

Problemen oplossen

Deze sectie bevat informatie om uw configuratie te troubleshooten.

Debug de LDAP-transactie

Deze debugs kunnen worden gebruikt om problemen met de DAP configuratie te isoleren:

- debug ldap 255
- debug datumspoor
- debug aaa authentication

ASA kan geen gebruikers vanaf LDAP-server verifiëren

Als ASA gebruikers van LDAP-server niet kan authenticeren, hier zijn een aantal voorbeelddebugs:

```
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
```

Op basis van deze debugs, is ofwel de LDAP Login DN-indeling onjuist of het wachtwoord is onjuist, dus controleer beide om het probleem op te lossen.

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.