LDAP op IOS-apparaten met behulp van Configuratievoorbeeld van Dynamische kenmerken

Inhoud

Inleiding

Dit document beschrijft hoe u Lichtgewicht Directory Access Protocol (LDAP)-verificatie op Cisco IOS® head-ends kunt gebruiken en hoe u de standaard Relative Distributed Name (RDN) van Common Name (CN) in sAMAAccountName kunt wijzigen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op een Cisco IOS-apparaat dat Cisco IOS-softwarerelease 15.0 of hoger draait.

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 de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

kernvraagstuk

De meeste Microsoft Active Directory (AD) met LDAP gebruikers definiëren hun RDN doorgaans als sAMAcountName. Als u verificatieproxy (proxy-proxy) en adaptieve security applicatie (ASA) gebruikt als head-end voor uw VPN-clients, dan is dit gemakkelijk ingesteld als u het AD-servertype definieert wanneer u de AAA-server definieert of als u de ldap-name-attribuut **opdracht** invoert. In de Cisco IOS-software is echter geen van deze opties beschikbaar. Standaard gebruikt de Cisco IOS-software de GN-waarde in AD voor verificatie van gebruikersnaam. Een gebruiker wordt bijvoorbeeld in AD gemaakt als *John Fernandes*, maar zijn ID is opgeslagen als *jfern*. Standaard controleert de Cisco IOS-software de GN-waarde. Dat wil zeggen, de software controleert *John Fernandes* op authenticatie van gebruikersnaam en niet op de SAMAAccountName waarde van *jfern* voor authenticatie. Om de Cisco IOS-software te dwingen de gebruikersnaam van de ASAMAaccountName-waarde te controleren, gebruikt u dynamische attributenkaarten zoals in dit document beschreven.

Oplossing

Hoewel Cisco IOS-apparaten deze methoden van RDN-wijziging niet ondersteunen, kunt u dynamische attribuut maps in de Cisco IOS-software gebruiken om een vergelijkbaar resultaat te bereiken. Als u de opdracht **Show** Ldap attribuut op het Cisco IOS head-end invoert, ziet u deze uitvoer:

LDAP-kenmerk	Notatie	AAA-kenmerk
AironetBwDataBurstContract	langlopend	bsn-data-bandbreedte-burst-control
Wachtwoord voor gebruikers	String	wachtwoord
AironetBwRealBurstContract	langlopend	bsn-realtime-bandbreedte-burst-c
werknemerstype	String	van het type werknemer
Type vlucht	langlopend	servicetype
airespaceACLName	String	naam bsn-acl
priv-lvl	langlopend	priv-lvl
lid van	String-DNA	suppressiegroep
cn	**String**	**username**

airespaceDSCP	langlo pend	bsn-dscp
beleidslaag	String	merknaam
airespaceQOSLev el	langlo pend	niveau bsn-qos
Aironet 8021PType	langlo pend	BSN-8021p-type
AironetBwRealDri ve-contract	langlo pend	bsn-realtime-bandbreedte-gemiddelde
AironetVLANinterf aceName	String	bsn-VLAN-interface-naam
airespaceVapID	langlo pend	bsn-wlan-id
AironetBwDataAv eContract	langlo pend	bsn-data-bandbreedte-gemiddelde-pictogram
AMAaccountNaa m	String	naam van dezelfde rekening
Contactinformatie	String	contactgegevens
telefoonnummer	String	telefoonnummer

Zoals u kunt zien uit de eigenschap die wordt gemarkeerd, gebruikt Cisco IOS Network Access Devices (NAD) deze attributenkaart voor verificatieverzoeken en voor reacties. In feite functioneert een dynamische LDAP attribuut map in de Cisco IOS apparaatfuncties bidirectioneel. Met andere woorden, eigenschappen worden niet alleen in kaart gebracht wanneer een antwoord wordt ontvangen, maar ook wanneer LDAP - verzoeken worden verstuurd. Zonder een door de gebruiker gedefinieerde attribuekaart, een basis-LDAP-configuratie op de NAD, ziet u dit logbericht wanneer het verzoek wordt verstuurd:

```
*Jul 24 11:04:50.568: LDAP: Check the default map for aaa type=username
*Jul 24 11:04:50.568: LDAP: Ldap Search Req sent
ld 1054176200
base dn DC=csco,DC=com
scope 2
filter (&(objectclass=*)(cn=xyz))ldap_req_encode
put_filter "(&(objectclass=person)(cn=xyz))"
put_filter: AND
put_filter_list "(objectclass=person)(cn=xyz)"
put_filter "(objectclass=person)"
put_filter: simple
put_filter "(cn=xyz)"
put_filter: simple
Doing socket write
*Jul 24 11:04:50.568: LDAP: LDAP search request sent successfully (reqid:13)
```

Om dit gedrag te veranderen en het te dwingen om de SAMArekeningName eigenschap voor verificatie van een gebruikersnaam te gebruiken, **voert** u de opdracht voor de **ldap**-attribuut om deze dynamische attributenkaart te maken eerst in:

```
ldap attribute map username
   map type sAMAccountName username
```

Zodra deze attributenkaart is gedefinieerd, voer u de **attributenkaart in *<dynamisch-attribuut-map-name>*** opdracht om deze attributenkaart aan de geselecteerde AAA servergroep (a-server) in kaart te brengen.

N.B.: Om dit gehele proces gemakkelijker te maken, is Cisco bug-ID CSCtr45874 (alleen geregistreerde klanten) gedeponeerd. Als dit verbeteringsverzoek ten uitvoer wordt gelegd, zullen gebruikers kunnen identificeren welke soort LDAP server wordt gebruikt en zullen zij automatisch een aantal van deze standaardopgaven veranderen om de waarden weer te geven die door die specifieke server worden gebruikt.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Monsterconfiguratie

Dit document gebruikt deze configuraties:

- Typ deze opdracht om de dynamische attributenkaart te definiëren:

```
ldap attribute map

   map type sAMAccountName username
```

- Typ deze opdracht om de AAA-servergroep te definiëren:

```
aaa group server ldap

   server
```

- Typ deze opdracht om de server te definiëren:

```
ldap server

   ipv4
   attribute map

   bind authentication root-dn password

   base-dn
```

- Voer deze opdracht in om de lijst van te gebruiken authenticatiemethoden vast te stellen:

```
aaa authentication login group
```

AD-tools

Voer een van deze opdrachten in de AD-opdrachtmelding om de absolute naam (DN) van een gebruiker te controleren:

```
dsquery user -name user1
```

OF

```
dsquery user -samid user1
```

Opmerking: "user1" hierboven staat in regex string. U kunt ook alle DNA's van gebruikersnaam inschakelen door de regex string als user* te gebruiken.

Om alle eigenschappen van één enkele gebruiker in te schakelen, voer deze opdracht in vanuit de AD-opdrachtmelding:

```
dsquery * -filter "(&(objectCategory=Person)(sAMAccountName=username))" -attr *
```

Potentiële problemen

In een LDAP-toepassing wordt eerst de zoekhandeling uitgevoerd en wordt de bind-handeling later uitgevoerd. Deze handeling wordt uitgevoerd omdat, als de wachtwoordeigenschap als onderdeel van de zoekactie wordt teruggegeven, de wachtwoordverificatie lokaal op de LDAP-client kan worden uitgevoerd en er geen extra bind-handeling nodig is. Als de wachtwoordeigenschap niet wordt teruggegeven, kan een bindingshandeling later worden uitgevoerd. Een ander voordeel wanneer u eerst de zoekoperatie uitvoert en de bind operatie later, is dat DN die in het zoekresultaat wordt ontvangen, als gebruiker DN kan worden gebruikt in plaats van de vorming van een DN wanneer de gebruikersnaam (GN-waarde) met een basis DNA wordt voorgeprogrammeerd.

Er kunnen problemen zijn wanneer de opdracht **voor** de **verificatie bindt-eerste** wordt gebruikt samen met een door de gebruiker gedefinieerde eigenschap die verandert waar de gebruikersnaam map wijst. Bijvoorbeeld, als u deze configuratie gebruikt, zult u waarschijnlijk een mislukking in uw authenticatie poging zien:

```
ldap server ss-ldap
ipv4 192.168.1.3
attribute map ad-map
transport port 3268
bind authenticate root-dn CN=abcd,OU=Employees,OU=qwrt Users,DC=qwrt,DC=com
   password blabla
base-dn DC=qwrt,DC=com
authentication bind-first
ldap attribute-map ad-map
 map type sAMAccountName username
```

Als resultaat hiervan ziet u de `ongeldige geloofsbrieven, Resultaatcode =` 49 foutmelding. De

logberichten lijken op deze berichten:

```
Oct  4 13:03:08.503: LDAP: LDAP: Queuing AAA request 0 for processing
Oct  4 13:03:08.503: LDAP: Received queue event, new AAA request
Oct  4 13:03:08.503: LDAP: LDAP authentication request
Oct  4 13:03:08.503: LDAP: Attempting first  next available LDAP server
Oct  4 13:03:08.503: LDAP: Got next LDAP server :ss-ldap
Oct  4 13:03:08.503: LDAP: First Task: Send bind req
Oct  4 13:03:08.503: LDAP: Authentication policy: bind-first
Oct  4 13:03:08.503: LDAP: Dynamic map configured
Oct  4 13:03:08.503: LDAP: Dynamic map found for aaa type=username
Oct  4 13:03:08.503: LDAP: Bind: User-DN=sAMAccountName=abcd,DC=qwrt,DC=com
ldap_req_encode
Doing socket write
Oct  4 13:03:08.503: LDAP:  LDAP bind request sent successfully (reqid=36)
Oct  4 13:03:08.503: LDAP: Sent the LDAP request to server
Oct  4 13:03:08.951: LDAP: Received socket event
Oct  4 13:03:08.951: LDAP: Checking the conn status
Oct  4 13:03:08.951: LDAP: Socket read event socket=0
Oct  4 13:03:08.951: LDAP: Found socket ctx
Oct  4 13:03:08.951: LDAP: Receive event: read=1, errno=9 (Bad file number)
Oct  4 13:03:08.951: LDAP: Passing the client ctx=314BA6ECldap_result
wait4msg (timeout 0 sec, 1 usec)
ldap_select_fd_wait (select)
ldap_read_activity lc 0x296EA104
Doing socket read
LDAP-TCP:Bytes read = 109
ldap_match_request succeeded for msgid 36 h 0
changing lr 0x300519E0 to COMPLETE as no continuations
removing request 0x300519E0 from list as lm 0x296C5170 all 0
ldap_msgfree
ldap_msgfree
Oct  4 13:03:08.951: LDAP:LDAP Messages to be processed: 1
Oct  4 13:03:08.951: LDAP: LDAP Message type: 97
Oct  4 13:03:08.951: LDAP: Got ldap transaction context from reqid
   36ldap_parse_result
Oct  4 13:03:08.951: LDAP: resultCode:    49     (Invalid credentials)
Oct  4 13:03:08.951: LDAP: Received Bind Responseldap_parse_result
   ldap_err2string
Oct  4 13:03:08.951: LDAP: Ldap Result Msg: FAILED:Invalid credentials,
   Result code =49
Oct  4 13:03:08.951: LDAP: LDAP Bind operation result : failed
Oct  4 13:03:08.951: LDAP: Restoring root bind status of the connection
Oct  4 13:03:08.951: LDAP: Performing Root-Dn bind operationldap_req_encode
Doing socket write
Oct  4 13:03:08.951: LDAP: Root Bind on CN=abcd,DC=qwrt,DC=com
initiated.ldap_msgfree
Oct  4 13:03:08.951: LDAP: Closing transaction and reporting error to AAA
Oct  4 13:03:08.951: LDAP: Transaction context removed from list [ldap reqid=36]
Oct  4 13:03:08.951: LDAP: Notifying AAA: REQUEST FAILED
Oct  4 13:03:08.951: LDAP: Received socket event
Oct  4 13:03:09.491: LDAP: Received socket event
Oct  4 13:03:09.491: LDAP: Checking the conn status
Oct  4 13:03:09.491: LDAP: Socket read event socket=0
Oct  4 13:03:09.491: LDAP: Found socket ctx
Oct  4 13:03:09.495: LDAP: Receive event: read=1, errno=9 (Bad file number)
Oct  4 13:03:09.495: LDAP: Passing the client ctx=314BA6ECldap_result
wait4msg (timeout 0 sec, 1 usec)
ldap_select_fd_wait (select)
ldap_read_activity lc 0x296EA104
Doing socket read
LDAP-TCP:Bytes read= 22
```

```
ldap_match_request succeeded for msgid 37 h 0
changing lr 0x300519E0 to COMPLETE as no continuations
removing request 0x300519E0 from list as lm 0x296C5170 all 0
ldap_msgfree
ldap_msgfree
Oct  4 13:03:09.495: LDAP: LDAP Messages to be processed: 1
Oct  4 13:03:09.495: LDAP: LDAP Message type: 97
Oct  4 13:03:09.495: LDAP: Got ldap transaction context from reqid
   37ldap_parse_result
Oct  4 13:03:09.495: LDAP: resultCode:    0     (Success)P: Received Bind
   Response
Oct  4 13:03:09.495: LDAP: Received Root Bind Response ldap_parse_result
Oct  4 13:03:09.495: LDAP: Ldap Result Msg: SUCCESS, Result code =0
Oct  4 13:03:09.495: LDAP: Root DN bind Successful on:CN=abcd,DC=qwrt,DC=com
Oct  4 13:03:09.495: LDAP: Transaction context removed from list [ldap reqid=37]
ldap_msgfree
ldap_result
wait4msg (timeout 0 sec, 1 usec)
ldap_select_fd_wait (select)
ldap_err2string
Oct  4 13:03:09.495: LDAP: Finished processing ldap msg, Result:Success
Oct  4 13:03:09.495: LDAP: Received socket event
```

De gemarkeerde lijnen geven aan wat er mis is met de eerste bind voor authenticatie. Het zal goed werken als u de **authenticatie bindt-eerste** opdracht uit de bovenstaande configuratie verwijdert.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **ldap-eigenschappen tonen**
- **ldap server all tonen**

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor probleemoplossing

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **streep ldap**
- **debug ldap**
- **debug van verificatie**
- **debug AAA-autorisatie**

Gerelateerde informatie

- AAA LDAP configuratie Guide Cisco IOS release 15.1MT
- ASA 8.0: LDAP-verificatie voor WebVPN-gebruikers configureren
- Technische ondersteuning en documentatie – Cisco Systems