Konfigurationsbeispiel für LDAP auf IOS-Geräten mit dynamischen Attributzuordnungen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die LDAP-Authentifizierung (Lightweight Directory Access Protocol) auf Cisco IOS®-Headends verwendet und der Standard-RDN (Relative Distinguished Name) von Common Name (CN) in sAMAccountName geändert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem Cisco IOS-Gerät, auf dem Cisco IOS Software Release 15.0 oder höher ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Kernproblem

Die meisten Microsoft Active Directory (AD)-Benutzer mit LDAP-Benutzern definieren ihren RDN in der Regel als sAMAccountName. Wenn Sie den Authentifizierungsproxy (auth-proxy) und eine Adaptive Security Appliance (ASA) als Headend für Ihre VPN-Clients verwenden, kann dies leicht behoben werden, wenn Sie den AD-Servertyp definieren, wenn Sie den AAA-Server definieren, oder wenn Sie den **Befehl ldap-naming-attribute eingeben**. In der Cisco IOS-Software ist jedoch keine dieser Optionen verfügbar. Standardmäßig verwendet die Cisco IOS-Software den CN-Attributwert in AD für die Authentifizierung von Benutzernamen. Beispielsweise wird ein Benutzer in AD als *John Fernandes* erstellt, seine Benutzer-ID wird jedoch als *jfern* gespeichert. Standardmäßig überprüft die Cisco IOS-Software den CN-Wert. Das heißt, die Software überprüft *John Fernandes* auf die Benutzernamenauthentifizierung und nicht den sAMAccountName-Wert von *jfern* für die Authentifizierung. Um zu erzwingen, dass die Cisco IOS-Software den Benutzernamen vom sAMAccountName-Attributwert überprüft, verwenden Sie dynamische Attributzuordnungen, wie in diesem Dokument beschrieben.

Lösung

Obwohl Cisco IOS-Geräte diese Methoden der RDN-Änderung nicht unterstützen, können Sie in der Cisco IOS-Software dynamische Attributzuordnungen verwenden, um ein ähnliches Ergebnis zu erzielen. Wenn Sie den Befehl **show ldap attribute** im Cisco IOS-Headend eingeben, wird diese Ausgabe angezeigt:

LDAP-Attribut	Format	AAA-Attribut
airespaceBwDataBurstVertrag	unendlich	bsn- data-bandwidth-burst-contr
UserPassword	Zeichenfolge	Kennwort
airespaceBwRealBurstVertrag	unendlich	bsn-realtime-bandwidth-burst-c
Mitarbeitertyp	Zeichenfolge	Mitarbeitertyp
airespaceServiceType	unendlich	Servicetyp
airespaceACLName	Zeichenfolge	bsn-acl-Name
priv-lvl	unendlich	priv-lvl
Mitglied von	string DN	Supplicant-Gruppe
cn	**Zeichenfolge**	**Benutzername**
airDSCP	unendlic	bsn-dscp

	h	
policyTag	Zeichenfolge	Tag-Name
AirQOSL-Ebene	unendlich	bsn-qos-Ebene
Air8021PType	unendlich	bsn-8021p-Typ
airespaceBwRealAveVertrag	unendlich	bsn-Echtzeit-Bandbreite - Durchschnitt
airespaceVlanInterfaceName	Zeichenfolge	bsn-vlan-Schnittstellenname
airespaceVapID	unendlich	bsn-wlan-id
airBwDataAveVertrag	unendlich	bsn-data-bandwidth-average-con
sAMAccountName	Zeichenfolge	Kontoname
meetingContactInfo	Zeichenfolge	Kontaktinformationen
Telefonnummer	Zeichenfolge	Telefonnummer

Wie Sie aus dem hervorgehobenen Attribut sehen können, verwendet das Cisco IOS Network Access Device (NAD) diese Attributzuordnung für Authentifizierungsanforderungen und Antworten. Grundsätzlich funktioniert eine dynamische LDAP-Attributzuordnung im Cisco IOS-Gerät bidirektional. Mit anderen Worten, Attribute werden nicht nur beim Empfang einer Antwort, sondern auch beim Versenden von LDAP-Anforderungen zugeordnet. Ohne benutzerdefinierte Attributzuordnungen, eine grundlegende LDAP-Konfiguration im NAD, wird diese Protokollmeldung beim Versenden der Anforderung angezeigt:

```
*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)
```

Um dieses Verhalten zu ändern und zu erzwingen, das sAMAccountName-Attribut für die Überprüfung des Benutzernamens zu verwenden, geben Sie den Befehl **ldap attribute map username** ein, um diese dynamische Attributzuordnung zuerst zu erstellen:

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

Wenn diese Attributzuordnung definiert wurde, geben Sie den Befehl **attribute map *<dynamic-attribute-map-name>*** ein, um diese Attributzuordnung der ausgewählten AAA-Servergruppe (aaa-server) zuzuordnen.

Hinweis: Um diesen gesamten Prozess zu vereinfachen, wurde die Cisco Bug ID CSCtr45874 (nur registrierte Kunden) abgelegt. Wenn diese Erweiterungsanfrage implementiert wird, können Benutzer ermitteln, welche LDAP-Server verwendet werden, und einige dieser Standardzuordnungen werden automatisch geändert, um die von diesem Server verwendeten Werte wiederzugeben.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Beispielkonfiguration

In diesem Dokument werden folgende Konfigurationen verwendet:

- Geben Sie diesen Befehl ein, um die dynamische Attributzuordnung zu definieren:

```
ldap attribute map

   map type sAMAccountName username
```

- Geben Sie diesen Befehl ein, um die AAA-Servergruppe zu definieren:

```
aaa group server ldap

   server
```

- Geben Sie diesen Befehl ein, um den Server zu definieren:

```
ldap server

   ipv4
   attribute map

   bind authentication root-dn password

   base-dn
```

- Geben Sie diesen Befehl ein, um die Liste der zu verwendenden Authentifizierungsmethoden zu definieren:

```
aaa authentication login group
```

AD-Tools

Um den absoluten DN eines Benutzers zu überprüfen, geben Sie einen der folgenden Befehle über die AD-Eingabeaufforderung ein:

```
dsquery user -name user1
```

ODER

```
dsquery user -samid user1
```

Hinweis: "user1" oben erwähnt ist in regex String. Sie können auch alle DNs des Benutzernamens auflisten, die mit Benutzer beginnen, indem Sie die regex-Zeichenfolge als "user*" verwenden.

Um alle Attribute eines einzelnen Benutzers zu registrieren, geben Sie diesen Befehl über die AD-Eingabeaufforderung ein:

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

Potenzielle Probleme

Bei einer LDAP-Bereitstellung wird zuerst der Suchvorgang und später der Bindungsvorgang ausgeführt. Dieser Vorgang wird ausgeführt, da bei der Rückgabe des Kennwortattributs im Rahmen des Suchvorgangs die Kennwortüberprüfung lokal auf dem LDAP-Client durchgeführt werden kann und kein zusätzlicher Bindungsvorgang erforderlich ist. Wenn das Kennwort-Attribut nicht zurückgegeben wird, kann zu einem späteren Zeitpunkt eine Bindung ausgeführt werden. Ein weiterer Vorteil, wenn Sie zuerst den Suchvorgang und später den Bindungsvorgang ausführen, besteht darin, dass die im Suchergebnis empfangene DN als Benutzer-DN statt als Verzeichnisnummer verwendet werden kann, wenn dem Benutzernamen (CN-Wert) ein Basis-DN vorangestellt wird.

Es können Probleme auftreten, wenn der Befehl **authentication bind-first** zusammen mit einem benutzerdefinierten Attribut verwendet wird, das sich ändert, wenn die Zuordnung des username-Attributs angezeigt wird. Wenn Sie beispielsweise diese Konfiguration verwenden, ist bei Ihrem Authentifizierungsversuch wahrscheinlich ein Fehler aufgetreten:

```
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 Ergebnis wird die Fehlermeldung `Ungültige Anmeldeinformationen, Ergebniscode =49` angezeigt. Die Protokollmeldungen sehen ähnlich aus wie folgt:

```
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
```

Die hervorgehobenen Zeilen weisen darauf hin, was mit der ursprünglichen Bindung vor der Authentifizierung nicht stimmt. Es funktioniert einwandfrei, wenn Sie den Befehl **authentication bind-first** aus der oben beschriebenen Konfiguration entfernen.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **LDAP-Attribute anzeigen**
- **ldap server all anzeigen**

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debuggen ldap all**
- **debuggen ldap-Ereignis**

- debuggen aaa authentication
- debuggen aaa autorisierung

Zugehörige Informationen

- AAA LDAP-Konfigurationsleitfaden Cisco IOS Release 15.1MT
- ASA 8.0: Konfigurieren der LDAP-Authentifizierung für WebVPN-Benutzer
- Technischer Support und Dokumentation - Cisco Systems