Esempio di configurazione di LDAP sui dispositivi IOS che utilizzano mappe di attributi dinamici

Sommario

Introduzione

In questo documento viene descritto come utilizzare l'autenticazione LDAP (Lightweight Directory Access Protocol) sugli headend Cisco IOS® e modificare l'RDN (Relative Distinguished Name) predefinito da CN (Common Name) a sAMAccountName.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, è stato usato un dispositivo Cisco IOS con software Cisco IOS versione 15.0 o successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Problema principale

La maggior parte degli utenti di Microsoft Active Directory (AD) con LDAP in genere definisce il proprio RDN come sAMAccountName. Se si utilizzano il proxy di autenticazione (auth-proxy) e un'appliance ASA (Adaptive Security Appliance) come headend per i client VPN, la soluzione è semplice se si definisce il tipo di server AD quando si definisce il server AAA o si immette il comando ldap-naming-attribute. Tuttavia, nel software Cisco IOS, nessuna di queste opzioni è disponibile. Per impostazione predefinita, il software Cisco IOS utilizza il valore dell'attributo CN in Active Directory per l'autenticazione del nome utente. Ad esempio, in Active Directory un utente viene creato come *John Fernandes*, ma il relativo ID utente viene memorizzato come *jfern*. Per impostazione predefinita, il software Cisco IOS controlla il valore CN. In altre parole, il software controlla *John Fernandes* per l'autenticazione del nome utente e non il valore sAMAccountName di *jfern* per l'autenticazione. Per forzare il software Cisco IOS a controllare il nome utente dal valore dell'attributo sAMAccountName, utilizzare le mappe di attributi dinamici come descritto in questo documento.

Soluzione

Sebbene i dispositivi Cisco IOS non supportino questi metodi di modifica RDN, è possibile utilizzare le mappe di attributi dinamici nel software Cisco IOS per ottenere un risultato simile. Se si immette il comando **show ldap attribute** sull'headend Cisco IOS, viene visualizzato questo output:

Attributo LDAP	Formato	Attributo AAA
ContrattoAirespaceBwDataBurst	Ulong	bsn-data-bandwidth-burst-contr
PasswordUtente	Stringa	password
ContrattoAirespaceBwRealBurst	Ulong	bsn-realtime-bandwidth-burst-c
employeeType	Stringa	tipo di dipendente
TipoServizioAirespace	Ulong	service-type
nomeACLairespace	Stringa	nome-bsn-acl
priv-lvl	Ulong	priv-lvl
memberOf	DN stringa	supplicant-group

cn	String a	username
airespaceDSCP	Ulong	bsn-dscp
tagcriteri	String a	nome-tag
airespaceQOSLevel	Ulong	livello bsn-qos
TipoAirespace8021PT	Ulong	tipo bsn-8021p
AirespaceBwRealAveContratto	Ulong	media larghezza di banda in tempo reale bsn
NomeInterfacciaVlanAirespace	String a	bsn-vlan-interface-name
IDSapAirespace	Ulong	bsn-wlan-id
AirespaceBwDataAveContratto	Ulong	bsn-data-bandwidth-average-con
NomeAccountAMA	String a	sam-account-name
meetingContactInfo	String a	informazioni-contatto
numerotelefono	String a	numero di telefono

Come si può vedere dall'attributo evidenziato, il dispositivo NAD (Network Access Device) di Cisco IOS utilizza questa mappa per le richieste di autenticazione e le risposte. Fondamentalmente, una mappa degli attributi LDAP dinamica nel dispositivo Cisco IOS funziona in modo bidirezionale. In altre parole, gli attributi vengono mappati non solo quando si riceve una risposta, ma anche quando si inviano richieste LDAP. Senza una mappa attributi definita dall'utente, una configurazione LDAP di base nel NAD, viene visualizzato questo messaggio di log quando la richiesta viene inviata:

```
*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)
```

Per modificare questo comportamento e forzarlo a utilizzare l'attributo sAMAccountName per la verifica del nome utente, immettere il comando **ldap attribute map username** per creare prima questa mappa attributi dinamica:

```
ldap attribute map username
```

```
map type sAMAccountName username
```

Dopo aver definito la mappa attributi, immettere il comando attribute map *<dynamic-attribute-map-name>* per mappare la mappa attributi al gruppo di server AAA selezionato (aaa-server).

Nota: per semplificare l'intero processo, è stato archiviato l'ID bug Cisco CSCtr45874 (solo utenti registrati). Se questa richiesta di miglioramento viene implementata, consentirà agli utenti di identificare il tipo di server LDAP utilizzato e di modificare automaticamente alcune di queste mappe predefinite per riflettere i valori utilizzati da quel particolare server.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di configurazione

Nel documento vengono usate queste configurazioni:

- Immettere questo comando per definire la mappa attributi dinamica:

```
ldap attribute map

   map type sAMAccountName username
```

- Immettere questo comando per definire il gruppo di server AAA:

```
aaa group server ldap

   server
```

- Immettere questo comando per definire il server:

```
ldap server

   ipv4
   attribute map

   bind authentication root-dn password

   base-dn
```

- Immettere questo comando per definire l'elenco dei metodi di autenticazione da utilizzare:

```
aaa authentication login group
```

Strumenti AD

Per controllare il nome distinto (DN) assoluto di un utente, immettere uno dei seguenti comandi dal prompt dei comandi di Active Directory:

```
dsquery user -name user1
```

O

```
dsquery user -samid user1
```

Nota: "user1" menzionato sopra è nella stringa regex. È inoltre possibile integrare tutti i DN del nome utente che iniziano con user utilizzando la stringa regex come "user*".

Per integrare tutti gli attributi di un singolo utente, immettere questo comando dal prompt dei comandi di Active Directory:

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

Problemi potenziali

In una distribuzione LDAP, l'operazione di ricerca viene eseguita per prima, mentre l'operazione di associazione viene eseguita successivamente. Questa operazione viene eseguita perché, se l'attributo password viene restituito come parte dell'operazione di ricerca, la verifica della password può essere eseguita localmente sul client LDAP e non è necessaria un'operazione di binding aggiuntiva. Se l'attributo password non viene restituito, è possibile eseguire un'operazione di associazione in un secondo momento. Un altro vantaggio quando si esegue prima l'operazione di ricerca e successivamente l'operazione di associazione consiste nel fatto che il DN ricevuto nel risultato della ricerca può essere utilizzato come DN utente anziché come formazione di un DN quando il nome utente (valore CN) è preceduto da un DN di base.

Quando si utilizza il comando **authentication bind-first** insieme a un attributo definito dall'utente, è possibile che si verifichino dei problemi che modificano il punto in cui punta la mappa degli attributi username. Ad esempio, se si utilizza questa configurazione, è probabile che si verifichi un errore nel tentativo di autenticazione:

```
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
```

Di conseguenza, verrà visualizzato il messaggio di errore `Credenziali non valide, codice risultato`

=49. I messaggi di log saranno simili ai seguenti:

```
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
```

Le righe evidenziate indicano gli errori dell'associazione iniziale prima dell'autenticazione. Per il corretto funzionamento, rimuovere il comando **authentication bind-first** dalla configurazione precedente.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **mostra attributi ldap**
- **mostra tutto il server ldap**

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug ldap all**
- **debug evento ldap**
- **debug autenticazione aaa**
- **autorizzazione debug aaa**

Informazioni correlate

- Guida alla configurazione di AAA LDAP - Cisco IOS release 15.1MT
- ASA 8.0: Configura autenticazione LDAP per utenti WebVPN
- Documentazione e supporto tecnico – Cisco Systems