使用動態屬性對映的IOS裝置上的LDAP配置示例

目錄

簡介

本檔案介紹如何在Cisco IOS®前端上使用輕量型目錄存取通訊協定(LDAP)驗證，以及如何將預設的相對可分辨名稱(RDN)從一般名稱(CN)變更為sAMAccountName。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據執行Cisco IOS軟體版本15.0或更新版本的Cisco IOS裝置。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

核心問題

大多數具有LDAP的Microsoft Active Directory(AD)使用者通常將其RDN定義為sAMAccountName。如果使用身份驗證代理(auth-proxy)和自適應安全裝置(ASA)作為VPN客戶端的前端，則如果在定義AAA伺服器時定義AD伺服器型別，或者輸入ldap-naming-attribute 命令，則很容易解決此問題。但是在Cisco IOS軟體中，這兩種選項均不可用。預設情況下，Cisco IOS軟體使用AD中的CN屬性值進行使用者名稱身份驗證。例如，在AD中建立一個名為*John Fernandes*的使用者，但其使用者ID儲存為*jfern*。預設情況下，Cisco IOS軟體會檢查CN值。即，軟體檢查*John Fernandes*的使用者名稱身份驗證，而不是*jfern*的sAMAccountName值進行身份驗證。若要強制Cisco IOS軟體從sAMAccountName屬性值檢查使用者名稱，請使用動態屬性對映，如本檔案中所述。

解決方案

雖然Cisco IOS裝置不支援這些RDN修改方法，但是您可以在Cisco IOS軟體中使用動態屬性對映來獲得類似的結果。如果您在Cisco IOS頭端上輸入**show ldap attribute**命令，將會看到以下輸出：

LDAP屬性	**格式**	**AAA屬性**
airespaceBwDataBurstContract	烏龍	bsn-data-bandwidth-burst-control
userPassword	字串	密碼
airespaceBwRealBurstContract	烏龍	bsn-realtime-bandwidth-burst-c
員工型別	字串	員工型別
airespace服務型別	烏龍	service-type
airespaceACLName	字串	bsn-acl-name
priv-lvl	烏龍	priv-lvl
成員	字串DN	Supplicant客戶端組
cn	**字串**	**使用者名稱**
airespaceDSCP	烏龍	bsn-dscp
policyTag	字串	tag-name
airespaceQOSLevel	烏龍	bsn-qos-level
airespace8021PType	烏龍	bsn-8021p-type
airespaceBwRealAveContract	烏龍	bsn-realtime-bandwidth-average
airespaceVlan介面名稱	字串	bsn-vlan-interface-name
airespaceVapId	烏龍	bsn-wlan-id
airespaceBwDataAveContract	烏龍	bsn-data-bandwidth-average-con
sAMAccountName	字串	sam-account-name
meetingContactInfo	字串	contact-info
電話號碼	字串	電話號碼

從突出顯示的屬性可以看出，Cisco IOS網路接入裝置(NAD)將此屬性對映用於身份驗證請求和響應。基本上，Cisco IOS裝置中的動態LDAP屬性對映是雙向運行的。換句話說，屬性不僅在接收到響應時對映，而且在發出LDAP請求時對映。如果沒有任何使用者定義的屬性對映（NAD上的基本

LDAP配置），則在發出請求時會顯示以下日誌消息：

```
*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)
```

若要更改此行為並強制其使用sAMAccountName屬性進行使用者名稱驗證，請輸入**ldap attribute map username**命令以首先建立此動態屬性對映：

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

定義此屬性對映後，輸入attribute map *<dynamic-attribute-map-name>* 命令以將此屬性對映對映到所選AAA伺服器組(aaa-server)。

注意：為了簡化整個流程，思科錯誤ID CSCtr45874**(僅限**註冊客戶)已存檔。如果實施此增強請求，使用者將可以識別正在使用的LDAP伺服器型別，並自動更改某些預設對映以反映該特定伺服器使用的值。

設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

示例配置

本檔案會使用以下設定：

- 輸入以下命令以定義動態屬性對映：

```
ldap attribute map

   map type sAMAccountName username
```

- 輸入以下命令可定義AAA伺服器群組：

```
aaa group server ldap

   server
```

- 輸入以下命令以定義伺服器：

```
ldap server

   ipv4
   attribute map

   bind authentication root-dn password

   base-dn
```

- 輸入以下命令可定義要使用的身份驗證方法清單：

```
aaa authentication login group
```

廣告工具

若要檢查使用者的絕對區分名稱(DN)，請在AD命令提示符下輸入以下命令之一：

```
dsquery user -name user1
```

或

```
dsquery user -samid user1
```

注意：上面提到的「user1」位於regex字串中。您還可以使用regex字串作為"user*"，從使用者開始登記所有使用者名稱的DN。

若要登記單個使用者的所有屬性，請在AD命令提示符下輸入以下命令：

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

潛在問題

在LDAP部署中，首先執行搜尋操作，之後執行繫結操作。之所以執行此操作，是因為，如果在搜尋操作過程中返回了密碼屬性，則密碼驗證可以在LDAP客戶端本地完成，不需要額外的繫結操作。如果未返回password屬性，則可以稍後執行繫結操作。當您先執行搜尋操作，然後再執行繫結操作時，另一個優點是當使用者名稱（CN值）以基本DN字首時，搜尋結果中接收的DN可用作使用者DN，而不是形成DN。

將**authentication bind-first**命令與使用者定義屬性一起使用時，可能會出現問題，該屬性會更改使用者名稱屬性對映的位置。例如，如果使用此設定，可能會在驗證嘗試中看到失敗：

```
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
```

因此，您將看到`Invalid credentials Result code = 49`錯誤消息。日誌消息將類似於以下內容：

```
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
```

突出顯示的行表示身份驗證之前的初始繫結出現了什麼錯誤。如果從上述組態中移除**authentication bind-first**指令，此命令會正常運作。

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- **顯示ldap屬性**
- **show ldap server all**

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- debug ldap all
- debug ldap event
- debug aaa authentication
- debug aaa authorization

相關資訊

- AAA LDAP配置指南Cisco IOS版本15.1MT
- ASA 8.0:為WebVPN使用者配置LDAP身份驗證
- 技術支援與文件 - Cisco Systems