使用动态属性映射的IOS设备上的LDAP配置示例

目录

简介

本文档介绍如何在Cisco IOS®头端上使用轻量级目录访问协议(LDAP)身份验证，并将默认的相对可分辨名称(RDN)从公用名(CN)更改为sAMAccountName。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于运行Cisco IOS软件版本15.0或更高版本的Cisco IOS设备。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

核心问题

大多数具有LDAP用户的Microsoft Active Directory(AD)通常将其RDN定义为sAMAccountName。如果将身份验证代理(auth-proxy)和自适应安全设备(ASA)用作VPN客户端的头端，则在定义AAA服务器时定义AD服务器类型或输入ldap-naming-attribute命令时，这很容易被修复。但是，在Cisco IOS软件中，这两种选项都不可用。默认情况下，Cisco IOS软件使用AD中的CN属性值进行用户名身份验证。例如，用户在AD中创建为John Fernandes，*但*其用户ID存储为*jfern*。默认情况下，Cisco IOS软件检查CN值。即，软件检查John Fernandes*的用*户名身份验证，而不检查jfern的sAMAccountName*值进*行身份验证。为了强制Cisco IOS软件从sAMAccountName属性值检查用户名，请使用动态属性映射，如本文档中所述。

解决方案

虽然Cisco IOS设备不支持这些RDN修改方法，但您可以在Cisco IOS软件中使用动态属性映射以实现类似结果。如果在Cisco IOS头端**上输入**show ldap attribute命令，您将看到以下输出：

LDAP属性	**格式**	**AAA属性**
airespaceBwDataBurstContract	乌隆	bsn- data-bandwidth-burst-contr
userPassword	字符串	密码
airespaceBwRealBurstContract	乌隆	bsn-realtime-bandwidth-burst-c
employeeType	字符串	员工类型
airespaceServiceType	乌隆	服务类型
airespaceACLName	字符串	bsn-acl-name
priv-lvl	乌隆	priv-lvl
memberOf	字符串DN	请求方组
cn	**字符串**	**用户名**
airespaceDSCP	乌隆	bsn-dscp
policyTag	字符串	tag-name
airespaceQOSLevel	乌隆	bsn-qos-level
airespace8021PType	乌隆	bsn-8021p-type
airespaceBwRealAveContract	乌隆	bsn-realtime-bandwidth-average
airespaceVlanInterfaceName	字符串	bsn-vlan-interface-name
airespaceVapId	乌隆	bsn-wlan-id
airespaceBwDataAveContract	乌隆	bsn-data-bandwidth-average-con
sAMAccountName	字符串	sam-account-name
meetingContactInfo	字符串	联系信息
电话号码	字符串	电话号码

从突出显示的属性中可以看到，Cisco IOS网络访问设备(NAD)使用此属性映射进行身份验证请求和响应。基本上，Cisco IOS设备中的动态LDAP属性映射双向运行。换句话说，属性不仅在收到响应

时映射，而且在LDAP请求发送出去时也映射。如果没有任何用户定义的属性映射（NAD上的基本LDAP配置），当请求发送出去时，您将看到以下日志消息：

```
*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)
```

要更改此行为并强制其使用sAMAccountName属性进行用户名验证，请先输入ldap属性**映射用户名**命令以创建此动态属性映射：

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

定义此属性映射后，输入***属性映射<dynamic-attribute-map-name>***命令，将此属性映射映射到所选AAA服务器组(aaa-server)。

注：为了简化整个流程，已提交Cisco Bug ID CSCtr45874(仅注册客户)。如果实施此增强请求，用户将能够识别正在使用的LDAP服务器类型，并自动更改其中一些默认映射以反映该特定服务器使用的值。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

配置示例

本文档使用以下配置：

- 输入此命令以定义动态属性映射：

```
ldap attribute map

   map type sAMAccountName username
```

- 输入以下命令以定义AAA服务器组：

```
aaa group server ldap
```

```
server
```

- 输入以下命令以定义服务器：

```
ldap server

   ipv4
   attribute map

   bind authentication root-dn password

   base-dn
```

- 输入此命令以定义要使用的身份验证方法列表：

```
aaa authentication login group
```

AD工具

要检查用户的绝对可分辨名称(DN)，请在AD命令提示符下输入以下命令之一：

```
dsquery user -name user1
```

或者

```
dsquery user -samid user1
```

注意：上面提到的“user1”是正则表达式字符串。您也可以使用正则表达式字符串作为“user*”，从用户开始登记用户名的所有DN。

要登记单个用户的所有属性，请在AD命令提示符下输入以下命令：

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

潜在问题

在LDAP部署中，首先执行搜索操作，然后执行绑定操作。执行此操作是因为，如果在搜索操作中返回密码属性，则可以在LDAP客户端本地执行密码验证，并且无需额外绑定操作。如果未返回密码属性，则稍后可以执行绑定操作。当您先执行搜索操作后再执行绑定操作时，另一个优势是，当用户名（CN值）前缀为基本DN时，搜索结果中收到的DN可用作用户DN，而不是形成DN。

当将authentication bind-first命令与用户定义的属性一起使用时，可能会出现一些问题，用户名属性映射的位置会发生更改。例如，如果使用此配置，则可能在身份验证尝试中看到失败：

```
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，您将看到“Invalid credentials， `Result code =49`”消息。日志消息将类似于以下内容：

```
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
```

突出显示的行指示身份验证前初始绑定的问题。如果从上述配置中删除**authentication bind-first**命令，它将正常工作。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show ldap attributes**
- **show ldap server all**

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意：在使用debug命令之前，请参阅有关Debug命**令的**重要信息。

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

相关信息

- AAA LDAP配置指南Cisco IOS版本15.1MT
- ASA 8.0：为 WebVPN 用户配置 LDAP 身份验证
- 技术支持和文档 - Cisco Systems