目录

简介

本文描述如何使用在Cisco IOS头端的轻量级目录访问协议(LDAP)验证和更改默认相对辨别名称(RDN)从共同名称(CN)到sAMAccountName。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据运行Cisco IOS软件版本15.0或以上的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

多数Microsoft Active Directory (AD)与LDAP用户典型地定义了他们的RDN是sAMAccountName。

如果使用认证代理(验证代理)和可适应安全工具(ASA)作为头端您的VPN客户端，这容易地修复，如果定义了AD服务器类型，当您定义了AAA服务器时或，如果输入LDAP命名属性命令。然而，在Cisco IOS软件里，两个选项不是可用的。默认情况下， Cisco IOS软件在AD使用CN属性值用户名验证。例如，用户在AD创建作为*John Fernandes*，但是他的用户ID存储如*jfern*。默认情况下，Cisco IOS软件检查CN值。即用户名验证而不是sAMAccountName值的软件检查*John Fernandes* *jfern*验证的。为了强制Cisco IOS软件检查从sAMAccountName属性值的用户名，请使用动态属性地图详情参见本文。

解决方案

虽然Cisco IOS设备不支持RDN修改这些方法，您能在Cisco IOS软件里使用动态属性地图为了取得相同的结果。如果输入**show ldap属性**on命令Cisco IOS头端，您将看到此输出：

LDAP属性	**格式**	**AAA属性**
airespaceBwDataBurstContract	Ulong	BSN数据带宽突发流量contr
userPassword	字符串	密码
airespaceBwRealBurstContract	Ulong	BSN实时带宽突发流量C
employeeType	字符串	员工类型
airespaceServiceType	Ulong	服务类型
airespaceACLName	字符串	BSN ACL NAME
priv lvl	Ulong	priv lvl
memberOf	字符串DN	请求方组
cn	**字符串**	**用户名**
airespaceDSCP	Ulong	BSN dscp
policyTag	字符串	TAG NAME
airespaceQOSLevel	Ulong	BSN QoS级别
airespace8021PType	Ulong	bsn-8021p-type
airespaceBwRealAveContract	Ulong	BSN实时带宽平均值
airespaceVlanInterfaceName	字符串	BSN VLAN接口NAME
airespaceVapId	Ulong	BSN WLAN id
airespaceBwDataAveContract	Ulong	BSN数据带宽平均值CON
sAMAccountName	字符串	SAM帐户NAME
meetingContactInfo	字符串	联系信息
telephoneNumber	字符串	电话号码

正如你从突出显示的属性看到， Cisco IOS网络接入设备(纳季)使用此属性地图认证请求和答复。基本上，在Cisco IOS设备的一张动态LDAP属性地图作用双向。换句话说，属性被映射不仅，当答复接收时，而且，当LDAP请求被派出。没有任何用户定义的属性地图，当请求被派出时，在纳季的

一个基本IDAP配置，您看到此日志消息：

为了更改此行为和强制它使用sAMAccountName属性用户名验证，请输入**username命令ldap属性的地图**首先创建此动态属性地图：

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

一旦此属性地图定义，请输入**属性地图**<dynamic-attribute-map-name>命令映射此属性地图对选定AAA服务器组(aaa-server)。

注意： 为了使此整个过程更加容易，归档了Cisco Bug ID CSCtr45874 (仅限注册用户)。如果此增强请求实现，将允许用户识别使用什么样的LDAP服务器和自动地更改其中一些默认映射反射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（仅限注册用户）可获取有关本部分所使用命令的详细信息。

配置示例

本文档使用以下配置：

- 输入此命令为了定义动态属性地图：**ldap attribute map** <dynamic-attribute-map-name> **map type sAMAccountName username**
- 输入此命令为了定义AAA服务器组：**aaa group server ldap** <server-group-name> **server** <server-name>
- 输入此命令为了定义服务器：**ldap server** <server-name> **ipv4** <host-address> **attribute map** <dynamic-attribute-map-name> **bind authentication root-dn** <complete-dn-root-user> **password** <root-user-pwd> **base-dn** <complete-dn-search-base>
- 输入此命令为了定义认证方法列表使用：**aaa authentication login** <name> **group** <server-group-name>

AD工具

为了检查绝对Distinguised名称(DN)用户，请输入从AD prompt命令的这些命令之一：

```
dsquery user -name user1
```

或者

```
dsquery user -samid user1
```

注意： 以上提到的"user1"在REGEX字符串。您能也获得开始与用户的用户名的所有Dns通过使用REGEX字符串作为“user*”。

为了获得单个用户的所有属性，请输入从AD prompt命令的此命令：

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

潜在问题

在LDAP部署，搜索操作首先被执行，并且捆绑操作执行的以后。此操作被执行，因为，如果作为

搜索操作一部分，密码属性返回，密码验证在LDAP客户端可以完成本地，并且没有需要对于一额外的捆绑操作。如果密码属性没有返回，捆绑操作可以执行的以后。另一个优点，当您首先时执行搜索操作和后捆绑的操作是在搜索结果接收的DN可以使用作为用户DN而不是DN的形成，当用户名(CN值)时以基础DN前缀。

也许有问题，当**验证BIND第一**命令与更改的一个用户定义的属性一起时使用用户名属性地图指向的地方。例如，如果使用此配置，您可能看到您的认证尝试的一失败：

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

结果，您将看到=49错误消息。日志消息将看起来类似于这些：

```
Oct  4 13:03:08.503: LDAP: LDAP: Queuing AAA request 0 for processingOct  4 13:03:08.503: LDAP:
Received queue event, new AAA requestOct  4 13:03:08.503: LDAP: LDAP authentication requestOct
4 13:03:08.503: LDAP: Attempting first  next available LDAP serverOct  4 13:03:08.503: LDAP: Got
next LDAP server :ss-ldapOct  4 13:03:08.503: LDAP: First Task: Send bind req
Oct  4 13:03:08.503: LDAP: Authentication policy: bind-firstOct  4 13:03:08.503: LDAP: Dynamic map
configuredOct  4 13:03:08.503: LDAP: Dynamic map found for aaa type=usernameOct  4 13:03:08.503:
LDAP: Bind: User-DN=sAMAccountName=abcd,DC=qwrt,DC=com
ldap_req_encodeDoing socket writeOct  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 serverOct  4 13:03:08.951: LDAP: Received socket eventOct  4
13:03:08.951: LDAP: Checking the conn statusOct  4 13:03:08.951: LDAP: Socket read event
socket=0Oct  4 13:03:08.951: LDAP: Found socket ctxOct  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_resultwait4msg (timeout 0 sec, 1 usec)ldap_select_fd_wait
(select)ldap_read_activity lc 0x296EA104Doing socket readLDAP-TCP:Bytes read =
109ldap_match_request succeeded for msgid 36 h 0changing lr 0x300519E0 to COMPLETE as no
continuationsremoving request 0x300519E0 from list as lm 0x296C5170 all
0ldap_msgfreeldap_msgfreeOct  4 13:03:08.951: LDAP:LDAP Messages to be processed: 1Oct  4
13:03:08.951: LDAP: LDAP Message type: 97Oct  4 13:03:08.951: LDAP: Got ldap transaction context
from reqid    36ldap_parse_resultOct  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 =49Oct  4 13:03:08.951: LDAP: LDAP Bind operation result : failed
Oct  4 13:03:08.951: LDAP:
Restoring root bind status of the connectionOct  4 13:03:08.951: LDAP: Performing Root-Dn bind
operationldap_req_encodeDoing socket writeOct  4 13:03:08.951: LDAP: Root Bind on
CN=abcd,DC=qwrt,DC=cominitiated.ldap_msgfreeOct  4 13:03:08.951: LDAP: Closing transaction and
reporting error to AAAOct  4 13:03:08.951: LDAP: Transaction context removed from list [ldap
reqid=36]Oct  4 13:03:08.951: LDAP: Notifying AAA: REQUEST FAILEDOct  4 13:03:08.951: LDAP:
Received socket eventOct  4 13:03:09.491: LDAP: Received socket eventOct  4 13:03:09.491: LDAP:
Checking the conn statusOct  4 13:03:09.491: LDAP: Socket read event socket=0Oct  4
13:03:09.491: LDAP: Found socket ctxOct  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_resultwait4msg
(timeout 0 sec, 1 usec)ldap_select_fd_wait (select)ldap_read_activity lc 0x296EA104Doing socket
readLDAP-TCP:Bytes read= 22ldap_match_request succeeded for msgid 37 h 0changing lr 0x300519E0
to COMPLETE as no continuationsremoving request 0x300519E0 from list as lm 0x296C5170 all
0ldap_msgfreeldap_msgfreeOct  4 13:03:09.495: LDAP: LDAP Messages to be processed: 1Oct  4
13:03:09.495: LDAP: LDAP Message type: 97Oct  4 13:03:09.495: LDAP: Got ldap transaction context
from reqid    37ldap_parse_resultOct  4 13:03:09.495: LDAP: resultCode:    0     (Success)P:
Received Bind    ResponseOct  4 13:03:09.495: LDAP: Received Root Bind Response
ldap_parse_resultOct  4 13:03:09.495: LDAP: Ldap Result Msg: SUCCESS, Result code =0Oct  4
13:03:09.495: LDAP: Root DN bind Successful on:CN=abcd,DC=qwrt,DC=comOct  4 13:03:09.495: LDAP:
Transaction context removed from list [ldap reqid=37]ldap_msgfreeldap_resultwait4msg (timeout 0
sec, 1 usec)ldap_select_fd_wait (select)ldap_err2stringOct  4 13:03:09.495: LDAP: Finished
processing ldap msg, Result:SuccessOct  4 13:03:09.495: LDAP: Received socket event
```

选中项目线路指示什么在最初的捆绑是错误的在验证前。如果从上述配置，删除**验证BIND第一**命令它将适当地运作。

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属性**
- **show ldap server全部**

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

- **调试ldap全部**
- **调试ldap事件**
- debug aaa authentication
- debug aaa authorization

相关信息

- AAA IDAP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