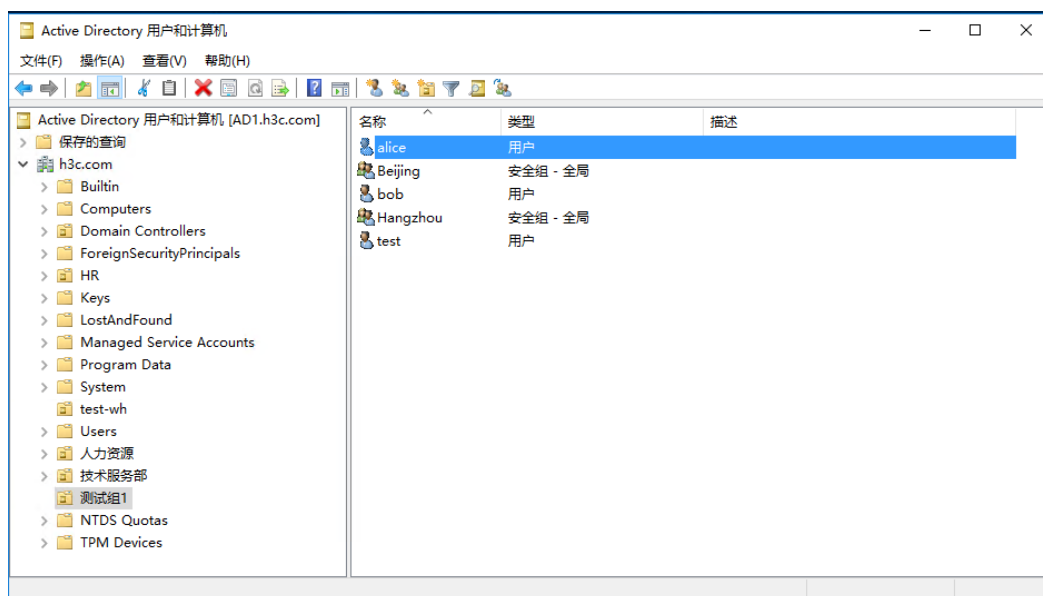


一、开始

SSL VPN 以 SSL (Secure Sockets Layer, 安全套接字层) 为基础提供远程的安全连接服务。用户可通过互联网, 使用 SSL 协议与远端的 SSL VPN 网关建立安全的连接, 同时 SSL VPN 网关负责对 SSL VPN 用户身份进行认证和授权, 用户身份认证且授权通过后, 便能访问对应的内网资源。用户认证包括: 用户名/密码认证、证书认证、用户名/密码和证书的组合认证。其中用户名/密码认证是最常见的, 通过配合 AAA (Authentication、Authorization、Accounting, 认证、授权、计费) 的网络安全管理机制, 对 SSL VPN 用户提供认证以及后续授权、计费等功能。AAA 可以通过多种协议来实现, 这些协议规定了设备与服务器之间如何传递用户信息。目前设备支持 RADIUS (Remote Authentication Dial-In User Service, 远程认证拨号用户服务) 协议、HWTACACS (HW Terminal Access Controller Access Control System, HW 终端访问控制器控制系统协议) 协议和 LDAP (Lightweight Directory Access Protocol, 轻量级目录访问协议) 协议。

本文主要讲述 SSL VPN 结合 LDAP 服务器进行认证和授权的排错步骤。LDAP (Lightweight Directory Access Protocol, 轻量级目录访问协议) 是一种目录访问协议, 用于提供跨平台的、基于标准的目录服务。它是在 X.500 协议的基础上发展起来的, 继承了 X.500 的优点, 并对 X.500 在读取、浏览和查询操作方面进行了改进, 适合于存储那些不经常改变的数据。LDAP 协议基于客户端/服务器架构提供目录服务功能, 所有的目录信息数据存储在 LDAP 服务器上。目前, Microsoft 的 Active Directory Server、IBM 的 Tivoli Directory Server 和 Sun 的 Sun ONE Directory Server 都是常用的 LDAP 服务器软件。

如下图所示, 以 Active Directory Server 为例, 其使用目录记录并管理系统中的组织信息、人员信息以及资源信息, 目录按照树型结构组织, 由多个条目 (Entry) 组成的。



(一) 目录结构

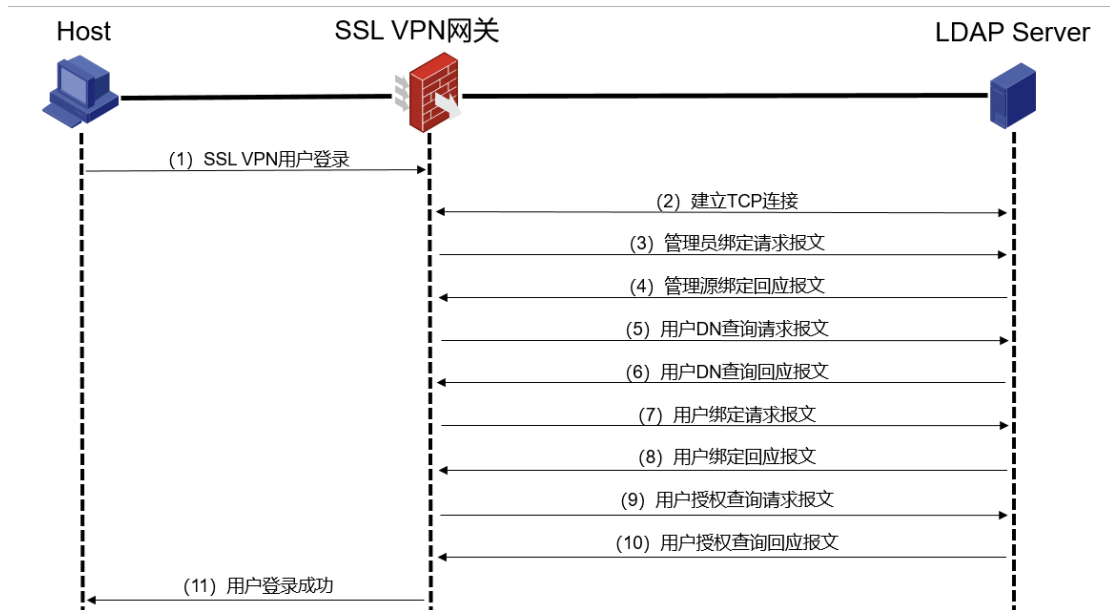
1. 目录树：在一个目录服务系统中，整个目录信息集可以表示为一个目录信息树，树中的每个节点是一个条目。
2. 条目：每个条目就是一条记录，每个条目有自己的唯一可区别的名称（DN）。
3. 对象类：与某个实体类型对应的一组属性，对象类是可以继承的，这样父类的必须属性也会被继承下来。
4. 属性：描述条目的某个方面的信息，一个属性由一个属性类型和一个或多个属性值组成，属性有必须属性和非必须属性。

(二) 常用关键字：DC、OU、CN、DN

关键字	英文全称
DC	Domain Component 域名的部分，其格式是将完整的域名分成几部分，如域名为 h3c.com 变成 dc=h3c,dc=com（一条记录的所属位置）
OU	Organization Unit 组织单位，组织单位可以包含其他各种对象（包括其他组织单元），如“安全产品支持部”（一条记录的所属组织）
CN	Common Name 公共名称，如“小胡”（一条记录的名称）
DN	Distinguished Name “CN=小胡,OU=安全产品支持部,OU=产品支持部,OU=技术支持中心,OU=技术服务部,DC=h3c,DC=com”，一条记录的位置（唯一）



AAA 可以使用 LDAP 协议对用户进行认证和授权服务，LDAP 协议中定义了多种操作来实现 LDAP 的各种功能，用于认证和授权的操作主要为绑定和查询。绑定操作的作用有两个：一是与 LDAP 服务器建立连接并获取 LDAP 服务器的访问权限；二是用于检查用户信息的合法性。查询操作就是构造查询条件，并获取 LDAP 服务器的目录资源信息的过程。使用 LDAP 协议进行认证和授权时，其基本的工作流程如下：



- (1) SSL VPN 用户发起连接请求，向 SSLVPN 网关（LDAP 客户端）发送用户名和密码。
- (2) LDAP 客户端收到请求之后，与 LDAP 服务器建立 TCP 连接。
- (3) LDAP 客户端以管理员 DN 和管理员 DN 密码为参数向 LDAP 服务器发送管理员绑定请求报文以获得查询权限。
- (4) LDAP 服务器进行绑定请求报文的处理。如果绑定成功，则向 LDAP 客户端发送绑定成功的回应报文。
- (5) LDAP 客户端以输入的用户名为参数，向 LDAP 服务器发送用户 DN 查询请求报文（User DN Search Request）。
- (6) LDAP 服务器收到查询请求报文后，根据报文中的查询起始地址、查询范围、以及过滤条件，对用户 DN 进行查找。如果查询成功，则向 LDAP 客户端发送查询成功的回应报文。查询得到的用户 DN 可以是一或多个。
- (7) LDAP 客户端以查询得到的用户 DN 和用户输入的密码为参数，向 LDAP 服务器发送用户 DN 绑定请求报文（User DN Bind Request），检查用户密码是否正确。

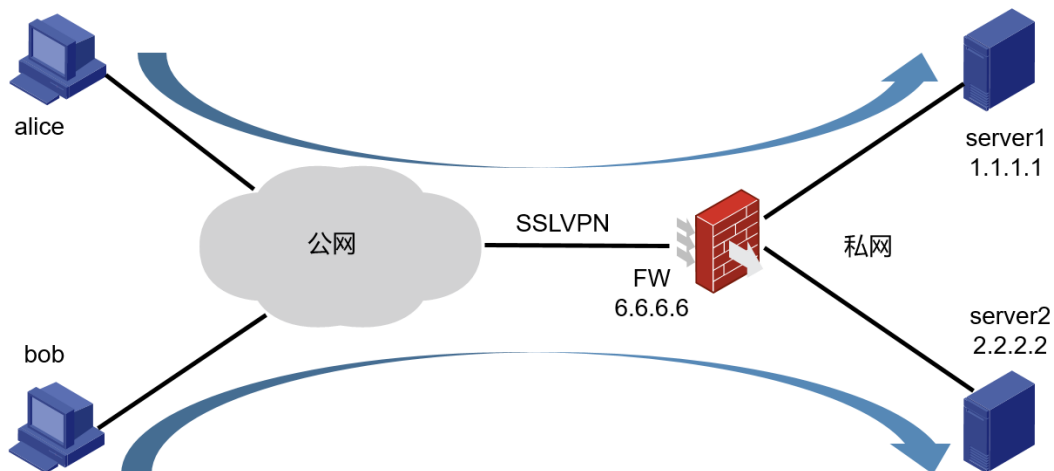
- (8) LDAP 服务器进行绑定请求报文的处理。
- 如果绑定成功，则向 LDAP 客户端发送绑定成功的回应报文。
 - 如果绑定失败，则向 LDAP 客户端发送绑定失败的回应报文。LDAP 客户端以下一个查询到的用户 DN（如果存在的话）为参数，继续向服务器发送绑定请求，直至有一个 DN 绑定成功，或者所有 DN 均绑定失败。如果所有用户 DN 都绑定失败，则 LDAP 客户端通知用户登录失败并拒绝用户接入。
- (9) LDAP 客户端以输入的用户名为参数（如果用户认证使用的是相同 LDAP 服务器，则以保存的绑定成功的用户 DN 为参数），向 LDAP 服务器发送授权查询请求报文。
- (10) LDAP 服务器收到查询请求报文后，根据报文中的查询起始地址、查询范围、过滤条件以及 LDAP 客户端关心的 LDAP 属性，对用户信息进行查找。如果查询成功，则向 LDAP 客户端发送查询成功的回应报文。
- (11) 认证和授权成功后，LDAP 客户端通知用户登录成功。

本文致力于防火墙 SSL VPN 功能结合 Microsoft 的 Active Directory Server 进行认证和授权的排除步骤。

二、流程图说明

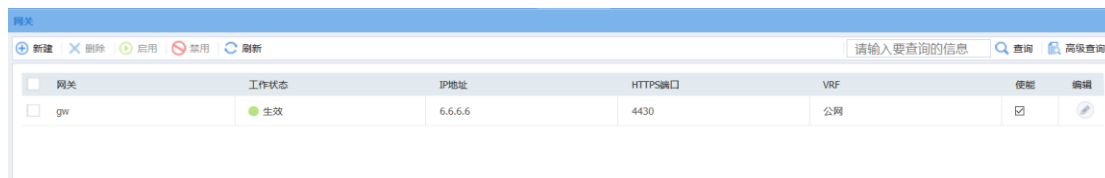
1, 检查本地认证和授权是否正常

如下图组网，用户 alice 和 bob 需要通过防火墙提供的 SSL VPN 网关接口来访问内网的服务器资源，且规定 alice 只能访问 server1，bob 只能访问 server2。



SSL VPN 本地认证时 Web 界面可以如下配置：

- (1) 创建 SSL VPN 网关，使用 FW 公网口地址，修改端口号为 4430。



- (2) 创建 SSL VPN 访问实例，ISP 认证域不勾选，缺省对接入用户使用本地认证和本地授权。



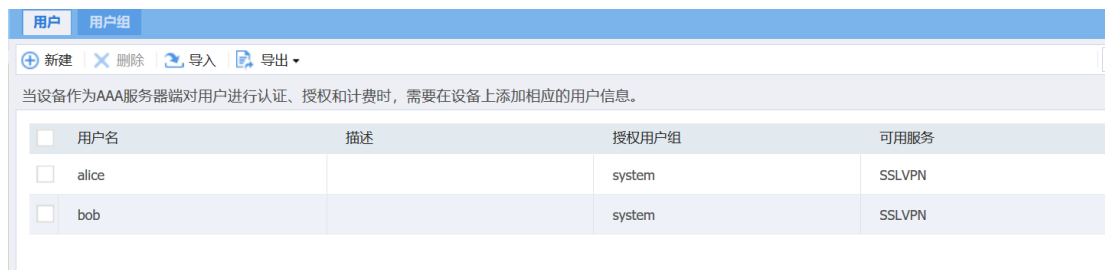
- (3) 业务选择为 IP 业务，创建两个 IP 接入资源，分别为 server1(1.1.1.1)和 server2(2.2.2.2)。



- (4) 创建两个资源组名为 pg1 和 pg2，pg1 调用 server1，pg2 调用 server2。



(5) 创建两个 SSL VPN 用户 alice 和 bob，分别关联 SSL VPN 策略组 pg1 和 pg2。



(6) 放通防火墙相关策略并进行拨号测试，以用户 alice 为例，拨号成功后可以正常访问 server1 (1.1.1.1)，但不能访问 server2 (2.2.2.2)。



2, 检查 LDAP 服务器是否可达

LDAP 协商过程使用目的端口 389 的 TCP 报文进行交互，首先我们需要检查此端口是否开放。如下：LDAP 服务器地址为 106.54.200.22，通过 telnet 命令查看 389 端口可以连接，连通性没有问题，连接之后服务器确保安全性主动关闭并提示：The connection was closed by the remote host!。

```
<H3C>
<H3C>telnet 106.54.200.22 389
Trying 106.54.200.22 ...
Press CTRL+K to abort
Connected to 106.54.200.22 ...

The connection was closed by the remote host!
<H3C>
```

如果端口无法连接，则会直接提示：Failed to connect to the remote host!。

```
<H3C>
<H3C>telnet 106.54.200.22 389
Trying 106.54.200.22 ...
Press CTRL+K to abort
Connected to 106.54.200.22 ...
Failed to connect to the remote host!
<H3C>
```

此时再检查两端的网络层是否互通，可以在 LDAP 客户端即防火墙上 ping LDAP 服务器的公网地址测试网络是否可达。如下：

```
<H3C>
<H3C>ping 106.54.200.22
Ping 106.54.200.22 (106.54.200.22): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 106.54.200.22 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
<H3C>%Dec 14 13:51:55:126 2019 H3C PING/6/PING_STATISTICS: -Context=1; Ping statistics for
106.54.200.22: 5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss.
```

如果 ping 不可达，先排查一下安全域和安全策略的配置是否正确：

(1) 安全域的配置：首先需要检查相应的接口是否加入了安全域。

(2) 安全策略的配置：检查本地域和该安全域之间的安全策略是否放通。

如上图所示，本地测试是全放通策略，所以不存在安全策略阻断的问题。如果现场的安全策略配置十分明细且复杂，建议在 ping 测试结果中打开调试开关。

命令： `debugging security-policy packet ip acl XXXX`（acl 建议写明细规则）

```
<H3C>debugging security-policy packet ip acl 3999
This command is CPU intensive and might affect ongoing services. Are you sure you want to
continue? [Y/N]:Y
<H3C>terminal monitor
The current terminal is enabled to display logs.
<H3C>terminal debugging
The current terminal is enabled to display debugging logs.
```

如果调试中显示对应的流有 `The packet is denied`，说明的确是安全策略进行了阻断，需要再仔细检查一下策略的配置。关于防火墙安全策略不通排查，本文不再详细阐述。

- 确定 LDAP 客户端和 LDAP 服务器网络配置都没有问题，则需要排除中间链路问题，通过 `tracert` 命令，可以判断报文丢弃在哪一跳。
- 确定网络可达，但是端口依旧有问题，需要确认 LDAP 服务器是否修改过默认端口并检查对应的端口是否打开。

如果网络或端口不可达，在设备上打开 LDAP 的调试过程，会提示管理员绑定操作失败：
(Bind operation failed)。

```
*Dec 19 16:10:08:875 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Performing binding operation as administrator.
*Dec 19 16:10:19:322 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Bind operation failed.
*Dec 19 16:10:19:322 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Failed to perform binding operation as administrator.
*Dec 19 16:10:19:322 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Processing LDAP authentication.
*Dec 19 16:10:19:322 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 2.
```

同时设备上抓包可以看到目的为 TCP389 端口存在三次重传报文，如下：

No.	Time	Source	Destination	Protocol	Length	Info
42	6971.418452	6.6.6.6	106.54.200.22	TCP	74	50576 → 389 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 WS=8 SACK_PERM=1 TSval=6661816 TSecr=0
49	6974.417409	6.6.6.6	106.54.200.22	TCP	74	[TCP Retransmission] 50576 → 389 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 WS=8 SACK_PERM=1 TSval=6664816 TSecr=0
51	6977.617297	6.6.6.6	106.54.200.22	TCP	74	[TCP Retransmission] 50576 → 389 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 WS=8 SACK_PERM=1 TSval=6668016 TSecr=0
53	6980.817296	6.6.6.6	106.54.200.22	TCP	74	[TCP Retransmission] 50576 → 389 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 WS=8 SACK_PERM=1 TSval=6671216 TSecr=0

需要注意的是，在命令行配置中各模块相关之间的调用关系是通过每一个模块的命令行视图中通过调用其他模块的名称来实现的。比如：SSL VPN 访问实例视图中调用 ISP 认证域，ISP 认证域视图中调用 LDAP 方案，LDAP 方案视图中调用 LDAP 服务器。如果其中引用名称存在问题，比如 LDAP 方案中将 LDAP 服务器名称写错，如下：


```
[H3C]ldap scheme ldapscheme
[H3C-ldap-ldapscheme] authentication-server 1dapserver # 将字母l写成了数字1
[H3C-ldap-ldapscheme] authorization-server ldapservice
```

则会出现以下问题，提示无法获取服务器信息（Failed to get server info）。

```
[H3C-ldap-ldapscheme]*Dec 19 14:44:30:866 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Processing LDAP authentication.
*Dec 19 14:44:30:866 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authentication request successfully sent.
*Dec 19 14:44:30:866 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Processing AAA request data.
*Dec 19 14:44:30:866 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Failed to get server info.
*Dec 19 14:44:30:866 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Failed to start state machine.
*Dec 19 14:44:30:866 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Processing LDAP authentication.
*Dec 19 14:44:30:866 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 2.
```

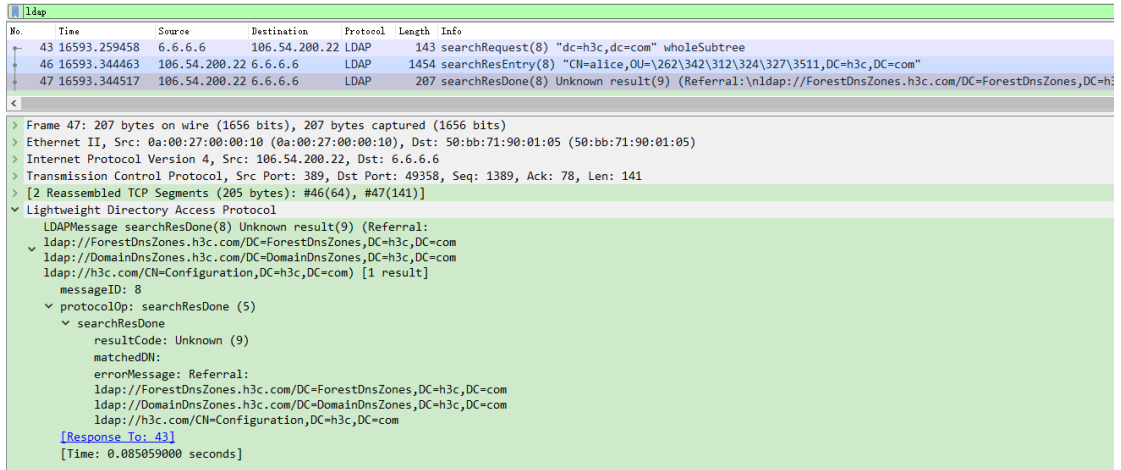
Web 界面各模块相互之间的引用关系是通过下拉框来进行选择的，建议在 web 界面进行相关配置。

3, 检查 LDAP 版本号是否配置正确

目前设备仅支持 LDAPv2 和 LDAPv3 两个协议版本，Microsoft 的 LDAP 服务器只支持 LDAPv3 版本，设备上配置的 LDAP 版本号需要与服务器支持的版本号保持一致，即 LDAPv3 版本。如果版本不匹配，则 LDAP 协议报文交互过程无法建立，从而导致 SSL VPN 用户无法进行认证。可以在命令行下通过 `debugging ldap all` 来查看，如过有以下报错，则需要检查配置中 LDAP 版本是否配置正确。

```
PAM_LDAP:Keep state authentication searching for incomplete searching.
*Dec 17 21:16:38:992 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Get result message errno = -18
*Dec 17 21:16:38:992 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:User alice search done.
*Dec 17 21:16:38:992 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Failed to search users.
*Dec 17 21:16:38:993 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Processing LDAP authentication.
*Dec 17 21:16:38:993 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.
```

同时抓包结果 LDAP 只有三条交互报文，且第三条提示 Unknown result(9)。



No.	Time	Source	Destination	Protocol	Length	Info
43	16593.259458	6.6.6.6	106.54.200.22	LDAP	143	searchRequest(8) "dc=h3c,dc=com" wholeSubtree
46	16593.344463	106.54.200.22	6.6.6.6	LDAP	1454	searchResEntry(8) "CN=alice,OU=\\262\\342\\312\\324\\327\\3511,DC=h3c,DC=com"
47	16593.344517	106.54.200.22	6.6.6.6	LDAP	207	searchResDone(8) Unknown result(9) (Referral: nldap://ForestDnsZones.h3c.com/DC=ForestDnsZones,DC=h3c,DC=com)

Frame 47: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits) on interface 0
Ethernet II, Src: 0a:00:27:00:00:10 (0a:00:27:00:00:10), Dst: 50:bb:71:90:01:05 (50:bb:71:90:01:05)
Internet Protocol Version 4, Src: 106.54.200.22, Dst: 6.6.6.6
Transmission Control Protocol, Src Port: 389, Dst Port: 49358, Seq: 1389, Ack: 78, Len: 141
[2 Reassembled TCP Segments (205 bytes): #46(64), #47(141)]
Lightweight Directory Access Protocol
LDAPMessage searchResDone(8) Unknown result(9) (Referral: ldap://ForestDnsZones.h3c.com/DC=ForestDnsZones,DC=h3c,DC=com)
ldap://DomainDnsZones.h3c.com/DC=DomainDnsZones,DC=h3c,DC=com
ldap://h3c.com/CN=Configuration,DC=h3c,DC=com [1 result]
messageID: 8
protocolOp: searchResDone (5)
searchResDone
resultCode: Unknown (9)
matchedDN:
errorMessage: Referral:
ldap://ForestDnsZones.h3c.com/DC=ForestDnsZones,DC=h3c,DC=com
ldap://DomainDnsZones.h3c.com/DC=DomainDnsZones,DC=h3c,DC=com
ldap://h3c.com/CN=Configuration,DC=h3c,DC=com
[Response To: 43]
[Time: 0.085059000 seconds]

4, 修改 LDAP 版本号

设备上修改 LDAP 版本号配置比较简单，既可以在命令行进行修改，如下：

```
[H3C]ldap server ldapserver
[H3C-ldap-server-ldapserver]protocol-version v3
# 或者删除协议版本，使其直接恢复到缺省 v3
[H3C-ldap-server-ldapserver]undo protocol-version
```

同时也可以可以在 Web 界面进行修改，在“对象->用户->认证管理->LDAP->LDAP 方案->编辑 LDAP 方案”中，将 LDAP 版本号选择为 V3 并点击确定按钮。

5, 检查 LDAP 管理员是否配置正确

LDAP 客户端以 LDAP 管理员 DN 和管理员 DN 密码为参数向 LDAP 服务器发送管理员绑定请求报文获得查询权限，现网一般用一个只读用户名密码而非服务器管理员（Administrator 账户）作为 LDAP 管理源账户用于设备和 LDAP 服务器绑定，且此用户不是最终的接入用户。LDAP 服务器进行绑定请求报文的处理，如果绑定成功，则向 LDAP 客户端发送绑定成功的回应报文。

如果管理员账号用户名或者密码错误，调试信息和抓包文件会有以下提示：

```

*Dec 14 15:34:41:618 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Performing binding operation as administrator.
*Dec 14 15:34:42:986 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Administrator's binding operation completed.
*Dec 14 15:34:42:986 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Response timeout timer successfully created.
*Dec 14 15:34:43:042 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Get result message errno = 49
*Dec 14 15:34:43:042 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Failed to perform binding operation as administrator.
*Dec 14 15:34:43:043 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Processing LDAP authentication.
*Dec 14 15:34:43:043 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.

```

No.	Time	Source	Destination	Protocol	Length	Info
334	1919.423791	6.6.6.6	106.54.200.22	LDAP	133	bindRequest(2) "cn=administrator",cn=users,dc=h3c,dc=com" simple
337	1919.511991	106.54.200.22	6.6.6.6	LDAP	176	bindResponse(2) invalidCredentials (80090308: LdapErr: DSID-0C09042A,
339	1919.512356	6.6.6.6	106.54.200.22	LDAP	73	unbindRequest(3)
561	2141.750853	6.6.6.6	106.54.200.22	LDAP	133	bindRequest(2) "cn=administrator",cn=users,dc=h3c,dc=com" simple
562	2141.827290	106.54.200.22	6.6.6.6	LDAP	176	bindResponse(2) invalidCredentials (80090308: LdapErr: DSID-0C09042A,
564	2141.827667	6.6.6.6	106.54.200.22	LDAP	73	unbindRequest(3)

> Frame 562: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)

> Ethernet II, Src: 0a:00:27:00:00:10 (0a:00:27:00:00:10), Dst: 50:bb:71:90:01:05 (50:bb:71:90:01:05)

> Internet Protocol Version 4, Src: 106.54.200.22, Dst: 6.6.6.6

> Transmission Control Protocol, Src Port: 389, Dst Port: 25413, Seq: 1, Ack: 68, Len: 110

Lightweight Directory Access Protocol

- LDAPMessage bindResponse(2) invalidCredentials (80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext error, data 52 messageID: 2
 - protocolOp: bindResponse (1)
 - bindResponse
 - resultCode: invalidCredentials (49)
 - matchedDN:
 - errorMessage: 80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext error, data 52e, v3839
 - [Response To: 561]
 - [Time: 0.076437000 seconds]

可以看见账号输入异常时 LDAP 服务器给我们返回错误码为 `invalidCredentials (49)`，此结果代码表示客户端试图绑定一组无法用于身份验证的凭据。可能返回此结果代码的一些潜在原因是：

- 绑定请求针对不存在的用户。
- 客户端试图使用不正确的密码进行身份验证。
- 客户端尝试使用包含无法成功验证的非密码凭据的 SASL 绑定请求进行身份验证。
- 绑定请求的目标是由于某种原因不允许进行身份验证的用户（例如，因为帐户已被锁定、用户密码已过期等）。

请仔细检查管理员用户是否存在上述问题并进行整改。

如果不使用管理员（Administrator）账号，在使用其他 `login-dn` 账号需要保证 DN 目录

中没有中文，否则 LDAP 服务器的返回码依旧为 `invalidCredentials` (49)。以 CN=alice,OU=测试组 1,DC=h3c,DC=com 为例，调试信息和抓包情况如下：

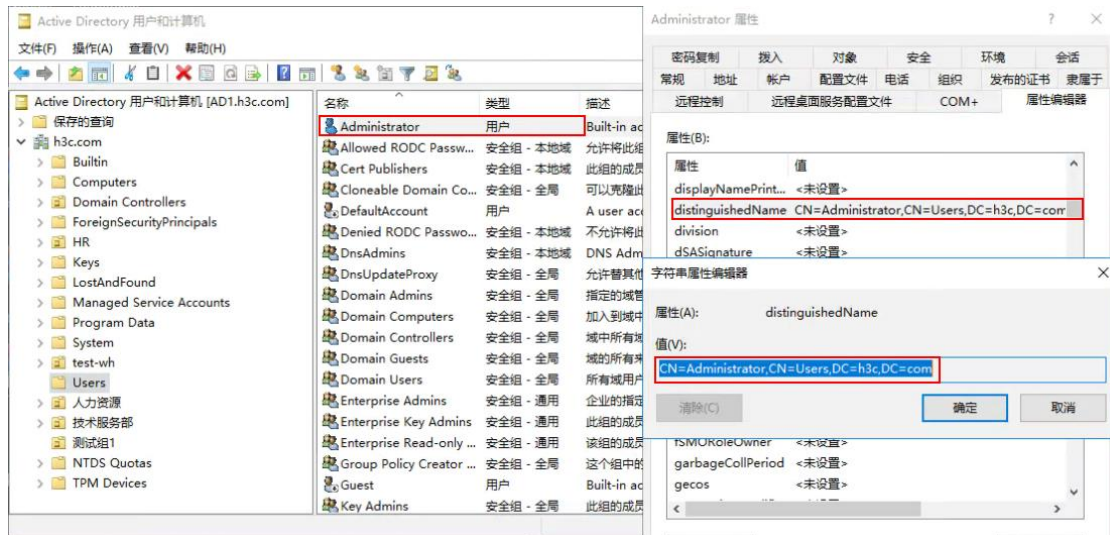
```
*Dec 19 09:28:33:044 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Executing bind operation, DN is cn=alice,ou=测试组 1,dc=h3c,dc=com.
*Dec 19 09:28:33:044 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Performing binding operation as administrator.
*Dec 19 09:28:34:167 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Administrator's binding operation completed.
*Dec 19 09:28:34:168 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Response timeout timer successfully created.
*Dec 19 09:28:34:245 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Get result message errno = 49
*Dec 19 09:28:34:245 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Failed to perform binding operation as administrator.
*Dec 19 09:28:34:245 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Processing LDAP authentication.
*Dec 19 09:28:34:245 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.
```

No.	Time	Source	Destination	Protocol	Length	Info
77	1245.568128	6.6.6.6	106.54.200.22	LDAP	126	bindRequest(2) "cn=alice,ou=\262\342\312\324\327\3511,dc=h3c,dc=com" simple
79	1246.038089	106.54.200.22	6.6.6.6	LDAP	176	bindResponse(2) invalidCredentials (80090308: LdapErr: DSID-0C09042A, comment: Accept
81	1246.039061	6.6.6.6	106.54.200.22	LDAP	73	unbindRequest(3)


```
> Frame 79: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)
> Ethernet II, Src: 0a:00:27:00:00:10 (0a:00:27:00:00:10), Dst: 50:bb:71:90:01:05 (50:bb:71:90:01:05)
> Internet Protocol Version 4, Src: 106.54.200.22, Dst: 6.6.6.6
> Transmission Control Protocol, Src Port: 389, Dst Port: 43981, Seq: 1, Ack: 61, Len: 110
< Lightweight Directory Access Protocol
  < LDAPMessage bindResponse(2) invalidCredentials (80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext error, data 52e, v3839)
    messageID: 2
    < protocolOp: bindResponse (1)
      < bindResponse
        resultCode: invalidCredentials (49)
        matchedDN:
          errorMessage: 80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext error, data 52e, v3839
          [Response To: 77]
          [Time: 0.469961000 seconds]
```

6, 修改 LDAP 管理员

本文档测试环境中，我们使用 Administrator 用户来获取查询权限，如下图所示该用户在 Active Directory Server 中的 DN 为: CN=Administrator,CN=Users,DC=h3c,DC=com。



在命令行下为 LDAP 服务器配置 login-dn 账号如下，注意规范填写完整 DN 路径。

```
[H3C]ldap server ldapserver
[H3C-ldap-server-ldapserver]login-dn cn=administrator,cn=users,dc=h3c,dc=com
[H3C-ldap-server-ldapserver]login-password simple 123456
```

也可以在 Web 界面进行配置，如下在“对象->用户->认证管理->LDAP->LDAP 方案->编辑 LDAP 方案中”正确填写管理员 DN 和管理员密码，然后点击确定。

7, 检查 LDAP 起始 DN 是否配置正确

用户查询的起始 DN 即 base-dn，指定登录用户在此目录范围内进行搜索，缺省情况下未指定用户查询的起始 DN。

生产环境中，LDAP 服务器上的目录结构可能具有很深的层次，如果从根目录进行用户 DN 的查找，耗费的时间将会较长，因此必须配置用户查找的起始 DN（非根目录），以提高查找效率，但是设备目前起始 DN 不支持配置路径中含有中文。

(1) 如下设备上配置起始 DN 为 OU=测试组 1,DC=h3c,DC=com，则无法进行用户查询操作。

```
[H3C]ldap server ldapserver
[H3C-ldap-server-ldapserver]search-base-dn ou=测试组 1,dc=h3c,dc=com
```

同时在设备上调试和抓包信息会有如下显示：

```

*Dec 18 19:46:15:793 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP[Authen]:Search base DN is ou=1,dc=h3c,dc=com.
*Dec 18 19:46:15:793 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Response timeout timer successfully created.
*Dec 18 19:46:15:881 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Get result message errno = 32
*Dec 18 19:46:15:881 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:User alice search done.
*Dec 18 19:46:15:881 2019 H3C LDAP/7/ERROR: -Context=1;
  PAM_LDAP:Failed to search users.
*Dec 18 19:46:15:881 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Processing LDAP authentication.
*Dec 18 19:46:15:881 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.

```

No.	Time	Source	Destination	Protocol	Length	Info
58	9194.893240	6.6.6.6	106.54.200.22	LDAP	132	bindRequest(8) "cn=administrator,cn=users,dc=h3c,dc=com" simple
60	9195.026638	106.54.200.22	6.6.6.6	LDAP	88	bindResponse(8) success
62	9195.027571	6.6.6.6	106.54.200.22	LDAP	154	searchRequest(9) "ou=1262\342\312\324\327\3511,dc=h3c,dc=com" wholeSubtree
66	9195.273132	106.54.200.22	6.6.6.6	LDAP	202	searchResDone(9) noSuchObject (0000208D: NameErr: DSID-03100241, problem 2001 (NO_OBJECT), data


```

> Frame 66: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits)
> Ethernet II, Src: 0a:00:27:00:00:10 (0a:00:27:00:00:10), Dst: 50:bb:71:90:01:05 (50:bb:71:90:01:05)
> Internet Protocol Version 4, Src: 106.54.200.22, Dst: 6.6.6.6
> Transmission Control Protocol, Src Port: 389, Dst Port: 25442, Seq: 23, Ack: 155, Len: 136
< Lightweight Directory Access Protocol
  LDAPMessage searchResDone(9) noSuchObject (0000208D: NameErr: DSID-03100241, problem 2001 (NO_OBJECT), data 0, best match of:
    "DC=h3c,DC=com"
  ) [0 results]
    messageID: 9
    < protocolOp: searchResDone (5)
      < searchResDone
        resultCode: noSuchObject (32)
        matchedDN: DC=h3c,DC=com
        errorMessage: 0000208D: NameErr: DSID-03100241, problem 2001 (NO_OBJECT), data 0, best match of:
          "DC=h3c,DC=com"

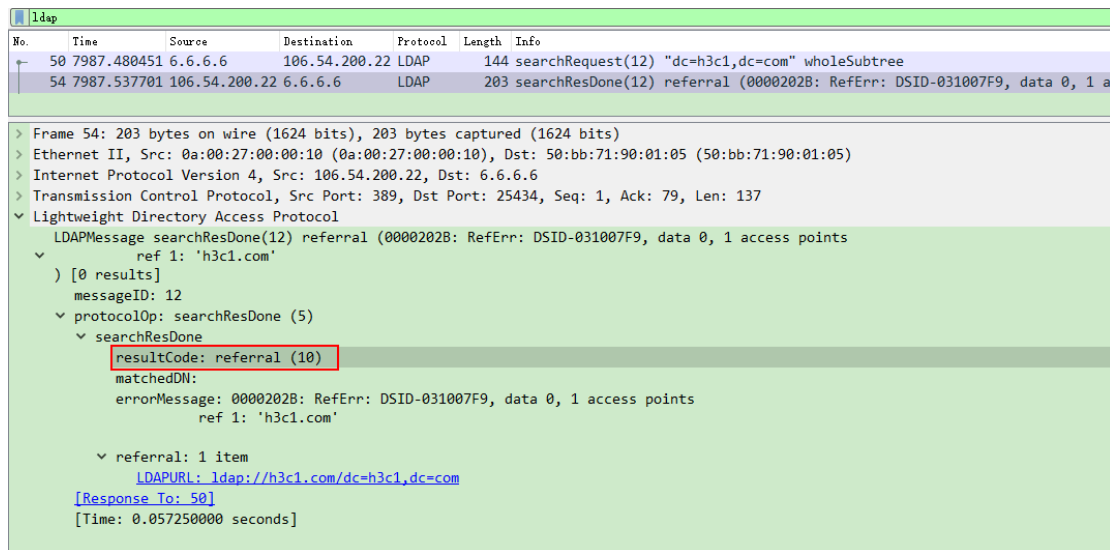
[Response To: 62]
[Time: 0.245561000 seconds]

```

可以看见 LDAP 服务器给我们返回的 resultCode 为 noSuchObject (32)。由于设备对这一项中文编码有问题，发送给 LDAP 服务器时将无法被识别，noSuchObject 对于搜索请求，它指示搜索基准 DN 所针对的条目不存在或者没有权限访问。

(2) 如果用户查询的起始 DN 不正确，在设备上调试和抓包信息会有如下显示：

```
*Dec 18 19:28:45:827 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP[Authen]:Search base DN is dc=h3c1,dc=com.
*Dec 18 19:28:45:827 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Response timeout timer successfully created.
*Dec 18 19:28:45:916 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Get result message errno = 10
*Dec 18 19:28:45:916 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:User alice search done.
*Dec 18 19:28:45:916 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Failed to search users.
*Dec 18 19:28:45:916 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Processing LDAP authentication.
*Dec 18 19:28:45:916 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.
```



可以看见 LDAP 服务器给我们返回的 resultCode 为 referral (10)，同时伴随着一条 LDAP 错误信息提示 errorMessage: 0000202B: RefErr: DSID-031007F9, data 0, 1 access points ref 1: 'h3c1.com'，该信息表示我们所设置的起始 DN (DC=h3c1, DC=com) 在 LDAP 服务器不存在。

(3) 如果配置的起始 DN 在 LDAP 服务器上的确存在，但是登录用户不在此目录下，同样用户无法登录，设备上调试和抓包信息如下，提示起始 DN 搜索为空。

```

*Dec 18 19:37:02:080 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP[Authen]:Search base DN is cn=users,dc=h3c,dc=com.
*Dec 18 19:37:02:080 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Response timeout timer successfully created.
*Dec 18 19:37:02:215 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Get result message errno = 0
*Dec 18 19:37:02:215 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:User alice search done.
*Dec 18 19:37:02:215 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP[State]:State switch from authentication searching to binding user.
*Dec 18 19:37:02:215 2019 H3C LDAP/7/ERROR: -Context=1;
  PAM_LDAP:Failed to bind user alice for the result of searching DN is NULL.
*Dec 18 19:37:02:215 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Processing LDAP authentication.
*Dec 18 19:37:02:215 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.

```

No.	Time	Source	Destination	Protocol	Length	Info
51	8753.806878	6.6.6.6	106.54.200.22	LDAP	132	bindRequest(2) "cn=administrator,cn=users,dc=h3c,dc=com" simple
53	8753.870509	106.54.200.22	6.6.6.6	LDAP	88	bindResponse(2) success
55	8753.871262	6.6.6.6	106.54.200.22	LDAP	152	searchRequest(3) "cn=users,dc=h3c,dc=com" wholeSubtree
57	8753.925249	106.54.200.22	6.6.6.6	LDAP	88	searchResDone(3) success [0 results]


```

> Frame 57: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
> Ethernet II, Src: 0a:00:27:00:00:10 (0a:00:27:00:00:10), Dst: 50:bb:71:90:01:05 (50:bb:71:90:01:05)
> Internet Protocol Version 4, Src: 106.54.200.22, Dst: 6.6.6.6
> Transmission Control Protocol, Src Port: 389, Dst Port: 25437, Seq: 23, Ack: 153, Len: 22
< Lightweight Directory Access Protocol
  < LDAPMessage searchResDone(3) success [0 results]
    messageID: 3
    < protocolOp: searchResDone (5)
      < searchResDone
        resultCode: success (0)
        matchedDN:
        errorMessage:
      [Response To: 55]
      [Time: 0.053987000 seconds]

```

8, 修改 LDAP 起始 DN

本文测试环境以 DC=h3c,DC=com 为例，命令行配置如下：

```

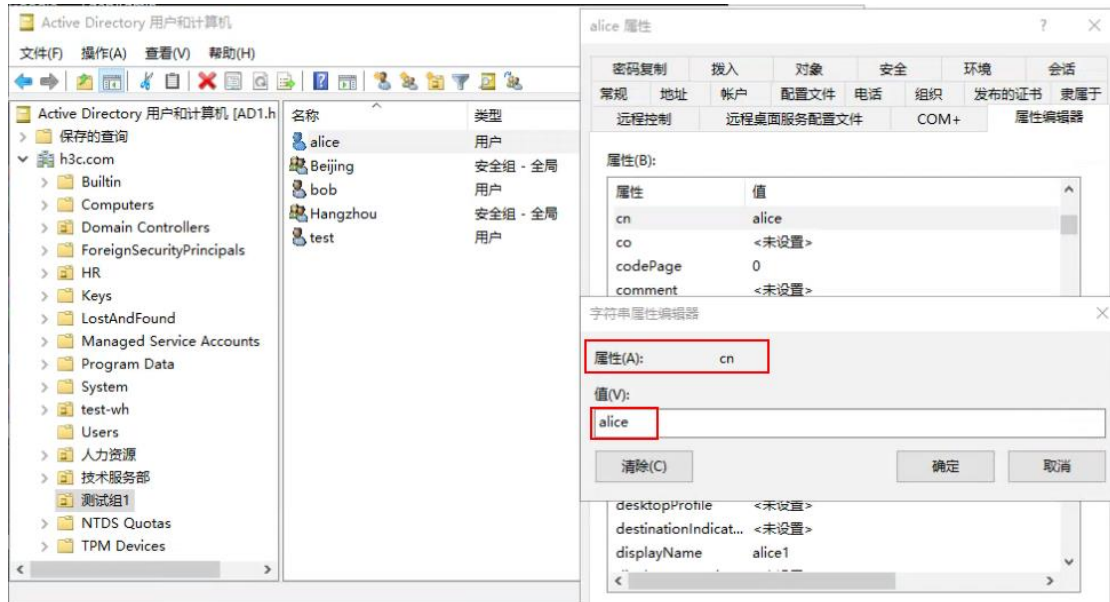
[H3C]ldap server ldapserver
[H3C-ldap-server-ldapserver] search-base-dn dc=h3c,dc=com

```

也可以在 Web 界面进行配置，如下在“对象->用户->认证管理->LDAP->LDAP 方案->编辑 LDAP 方案”中正确填写用户 DN 查询的起始节点，同时无特殊需求，保持用户 DN 查询的范围为默认查询所有子目录，然后点击确定。

9, 检查用户名是否配置正确

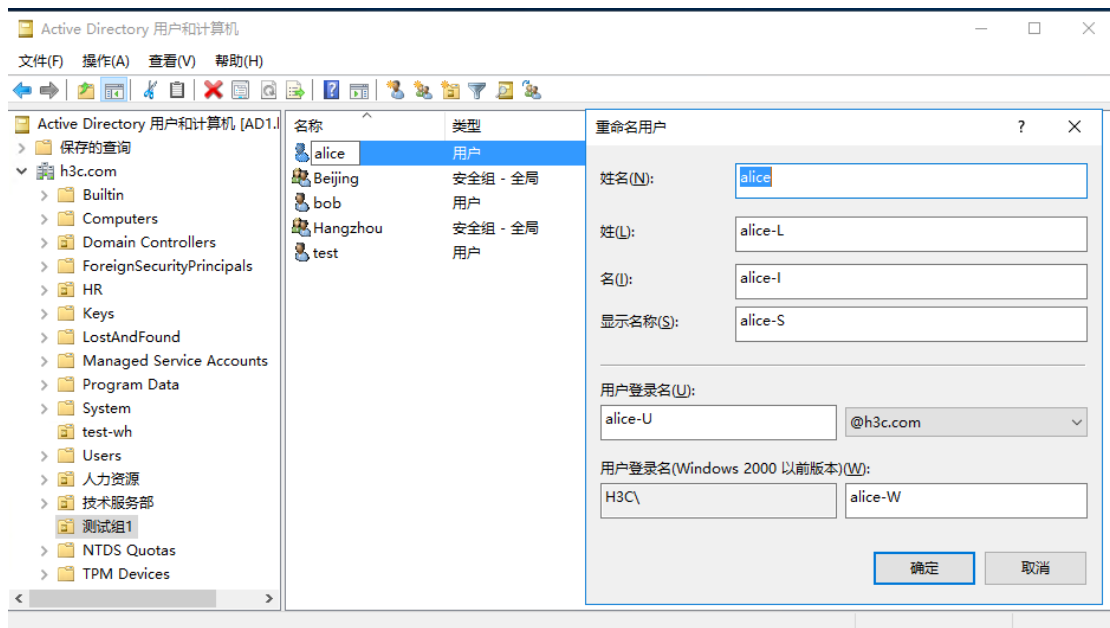
缺省情况下, 用户查询的用户名属性为 Common Name 即 CN。在 LDAP 服务器上如下查看 alice 的 CN 属性为 alice, 此 CN 属性和 CN (distinguishedName: CN=alice,OU=测试组1,DC=h3c,DC=com) 中的 CN 是一致的。



但是用户在名字上还有其他属性, 这些属性名称设置可能不尽相同, 如下:

姓名	name	alice
姓	sn	alice-L
名	givenName	alice-I
显示名称	displayName	alice-S
用户登录名	userPrincipalName	alice-U@h3c.com
用户登录名	sAMAccountName	alice-W

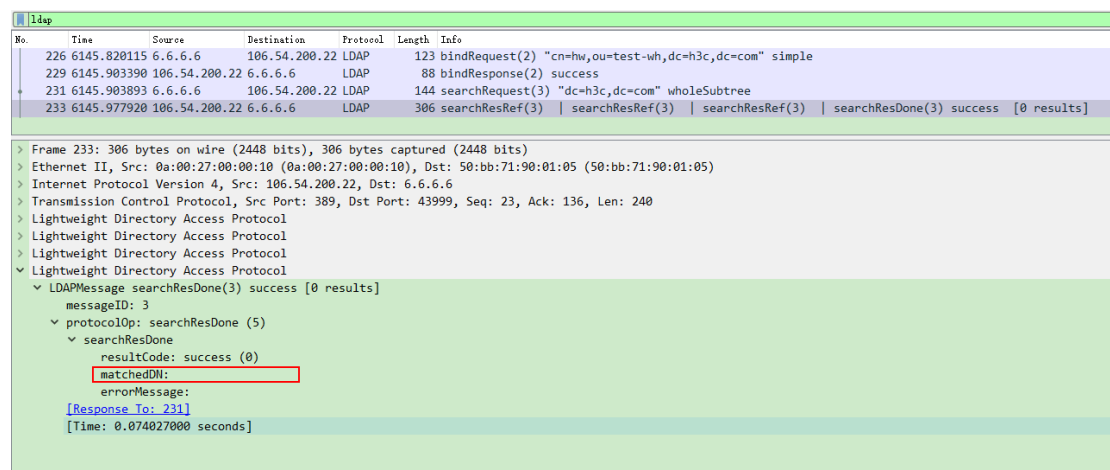
从 LDAP 服务器视图显示更通俗易懂, 如下:



LDAP 中的属性不区分大小写。name 与 cn 是一致的，当 name 进行修改时，cn 也同时被修改；name 可以通过 sn + givenName 来显示，也可以主动修改；userPrincipalName 需要携带 LDAP 服务器域名；sAMAccountName 与用户登录名（Windows 2000 以前版本）保持一致。

- (1) 如果 inode 用户名输入错误，比如将 alice 输错为 alice1，会有以下报错来提示该用户无法找到。

```
*Dec 19 11:05:17:327 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Get result message errno = 0
*Dec 19 11:05:17:327 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:User alicel search done.
*Dec 19 11:05:17:327 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP[State]:State switch from authentication searching to binding user.
*Dec 19 11:05:17:327 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Failed to bind user alicel for the result of searching DN is NULL.
*Dec 19 11:05:17:327 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Processing LDAP authentication.
*Dec 19 11:05:17:327 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.
```



- (2) 如果用户名输入正确，但是用户的密码出现错误，LDAP 服务器会返回错误码为 invalidCredentials (49)，这和 LDAP 管理员账号密码输入错误是一直的，都是身份存在问题。

```

*Dec 19 11:10:29:693 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Get result message errno = 0
*Dec 19 11:10:29:693 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:User alice search done.
*Dec 19 11:10:29:693 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP[State]:State switch from authentication searching to binding user.
*Dec 19 11:10:29:693 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Performing binding operation as user.
*Dec 19 11:10:31:168 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Finish bind as user.
*Dec 19 11:10:31:615 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Get result message errno = 49
*Dec 19 11:10:31:615 2019 H3C LDAP/7/ERROR: -Context=1;
  PAM_LDAP:Failed to perform binding operation as user.
*Dec 19 11:10:31:615 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Processing LDAP authentication.
*Dec 19 11:10:31:615 2019 H3C LDAP/7/EVENT: -Context=1;
  PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.

```

No.	Time	Source	Destination	Protocol	Length	Info
55	6645.685120	6.6.6.6	106.54.200.22	LDAP	123	bindRequest(2) "cn=hw,ou=test-wh,dc=h3c,dc=com" simple
59	6645.766482	106.54.200.22	6.6.6.6	LDAP	88	bindResponse(2) success
61	6645.767098	6.6.6.6	106.54.200.22	LDAP	143	searchRequest(3) "dc=h3c,dc=com" wholeSubtree
79	6651.684031	6.6.6.6	106.54.200.22	LDAP	130	bindRequest(2) "CN=alice,OU=\346\265\213\350\257\225\347\273\2041,DC=h3c,DC=com" simple
80	6651.738610	106.54.200.22	6.6.6.6	LDAP	176	bindResponse(2) invalidCredentials (80090308: LdapErr: DSID-0C09042A, comment: AcceptSec

> Frame 80: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)

> Ethernet II, Src: 0a:00:27:00:00:10 (0a:00:27:00:00:10), Dst: 50:bb:71:90:01:05 (50:bb:71:90:01:05)

> Internet Protocol Version 4, Src: 106.54.200.22, Dst: 6.6.6.6

> Transmission Control Protocol, Src Port: 389, Dst Port: 44007, Seq: 1, Ack: 65, Len: 110

Lightweight Directory Access Protocol

- LDAPMessage bindResponse(2) invalidCredentials (80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext error, data 52e, v3839)
 - messageID: 2
 - protocolOp: bindResponse (1)
 - bindResponse
 - resultCode: invalidCredentials (49)
 - matchedDN:
 - errorMessage: 80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext error, data 52e, v3839
 - [Response To: 79]
 - [Time: 0.054579000 seconds]

(3) 除了用户的 cn 属性,还常用到用户的“sAMAccountName”属性值和 “userPrincipalName” 属性值,

- sAMAccountName 属性

设备上 ldap server 配置用户名称属性填写为 sAMAccountName, 以用户 alice 为例, 则用户查询条件以 alice 的该属性进行过滤:

```
*Dec 19 11:33:27:715 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Username is alice-W.
*Dec 19 11:33:27:715 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP[Author]:Search filter is (&(objectClass=person)(samaccountname=alice-W)).
```

```
> Frame 41: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits)
> Ethernet II, Src: 50:bb:71:90:01:05 (50:bb:71:90:01:05), Dst: 0a:00:27:00:00:10 (0a:00:27:00:00:10)
> Internet Protocol Version 4, Src: 6.6.6.6, Dst: 106.54.200.22
> Transmission Control Protocol, Src Port: 15809, Dst Port: 389, Seq: 1, Ack: 1, Len: 91
< Lightweight Directory Access Protocol
  LDAPMessage searchRequest(9) "dc=h3c,dc=com" wholeSubtree
    messageID: 9
    protocolOp: searchRequest (3)
      searchRequest
        baseObject: dc=h3c,dc=com
        scope: wholeSubtree (2)
        derefAliases: neverDerefAliases (0)
        sizeLimit: 0
        timeLimit: 0
        typesOnly: False
      Filter: (&(objectClass=person)(samaccountname=alice-W))
        filter: and (0)
          and: (&(objectClass=person)(samaccountname=alice-W))
            and: 2 items
              Filter: (objectClass=person)
                and item: equalityMatch (3)
                  equalityMatch
                    attributeDesc: objectClass
                    assertionValue: person
              Filter: (samaccountname=alice-W)
                and item: equalityMatch (3)
                  equalityMatch
                    attributeDesc: samaccountname
                    assertionValue: alice-W
            attributes: 0 items
          [Response In: 42]
```

如果该属性用户名或者密码输入错误，排错过程和 CN 属性一致。

● userPrincipalName 属性

由于用户的 userPrincipalName 属性是携带 LDAP 服务器域名的，防火墙设备上需要设置为登录用户添加域名进行配合使用。user-name-format 表示发送给服务器的用户名格式，携带 with-domain 表示发送给服务器的用户名带 ISP 域名；默认参数为 without-domain 表示发送给服务器的用户名不带 ISP 域名。值得注意的是，当没有配置 user-name-format with-domain（即使用默认 without-domain）时，即使 iNode 用户使用携带其他域名也没有影响，比如使用 alice@666，防火墙设备和 LDAP 服务器交互时，会把@666 域名去除，使用 alice 用户进行授权和认证。设备配置了 user-name-format with-domain，会将登录用户后再加上使用 SSL VPN 访问实例下 ISP 认证域，提交给 LDAP 服务器进行认证和授权，所以必须保证设备上的 ISP 命名和 LDAP 服务器的域名一致，否则无法进行认证。

a) 配置了 userPrincipalName 但是没有配置 with-domain 调试和抓包信息会有以下报错来提示该用户无法找到。

```
*Dec 19 14:20:24:700 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Search user when authentication.
*Dec 19 14:20:24:700 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Username is alice-U.
*Dec 19 14:20:24:700 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP[Authen]:Search filter is (&(objectClass=person)(userprincipalname=alice-U)).
. . . . .
*Dec 19 14:20:24:983 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Get result message errno = 0
*Dec 19 14:20:24:983 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP>User alice-U search done.
*Dec 19 14:20:24:983 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP[State]:State switch from authentication searching to binding user.
*Dec 19 14:20:24:983 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Failed to bind user alice-U for the result of searching DN is NULL.
*Dec 19 14:20:24:983 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Processing LDAP authentication.
*Dec 19 14:20:24:983 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.
```

```
> Frame 293: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits)
> Ethernet II, Src: 50:bb:71:90:01:05 (50:bb:71:90:01:05), Dst: 0a:00:27:00:00:10 (0a:00:27:00:00:10)
> Internet Protocol Version 4, Src: 6.6.6.6, Dst: 106.54.200.22
> Transmission Control Protocol, Src Port: 15809, Dst Port: 389, Seq: 216, Ack: 1756, Len: 94
< Lightweight Directory Access Protocol
  < LDAPMessage searchRequest(15) "dc=h3c,dc=com" wholeSubtree
    messageID: 15
    < protocolOp: searchRequest (3)
      < searchRequest
        baseObject: dc=h3c,dc=com
        scope: wholeSubtree (2)
        derefAliases: neverDerefAliases (0)
        sizeLimit: 0
        timeLimit: 0
        typesOnly: False
      < Filter: (&(objectClass=person)(userprincipalname=alice-U))
        < filter: and (0)
          < and: (&(objectClass=person)(userprincipalname=alice-U))
            < and: 2 items
              < Filter: (objectClass=person)
                < and item: equalityMatch (3)
                  < equalityMatch
                    attributeDesc: objectClass
                    assertionValue: person
              < Filter: (userprincipalname=alice-U)
                < and item: equalityMatch (3)
                  < equalityMatch
                    attributeDesc: userprincipalname
                    assertionValue: alice-U
            attributes: 0 items
          [Response In: 294]
```

b) 配置了 userPrincipalName 也配置了 with-domain，但是 SSL VPN 访问实例中调用的不一致，如下 LDAP 域名为 h3c.com，但是引用的 ISP 认证域为 111。

编辑访问实例

基本配置 | Web业务 | TCP业务 | IP业务 | BYOD业务 | 资源组 | 页面配置

访问实例 ? * (1-31字符)

关联网关 + 新建 ✎ 编辑 ✕ 删除 *

网关	访问方式	域	主机名称	编辑
<input type="checkbox"/> gw	直接访问网关			✎

VRF

ISP认证域

开启验证码验证 ?

开启证书认证 ?

开启IMC短信认证 ?

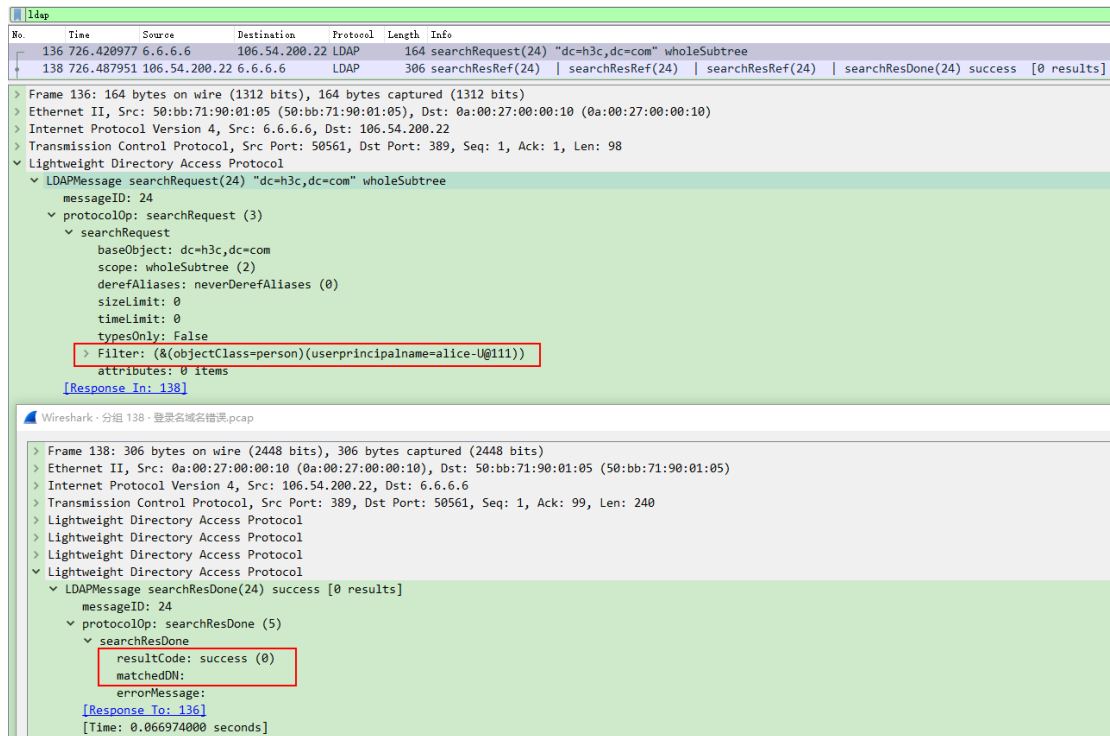
最大用户数 (1-1048575)

每用户在线控制 ? 最大会话数 (0-1048575)

完成 取消

此时调试和抓包信息也会有以下报错来提示该用户无法找到。

```
*Dec 19 14:29:13:686 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Search user when authentication.
*Dec 19 14:29:13:686 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Username is alice-U@111.
*Dec 19 14:29:13:686 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP[Authen]:Search filter is (&(objectClass=person)(userprincipalname=alice-U@111)).
.....
*Dec 19 14:29:13:754 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Failed to bind user alice-U@111 for the result of searching DN is NULL.
*Dec 19 14:29:13:754 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Processing LDAP authentication.
*Dec 19 14:29:13:754 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.
```



10. 修改用户名

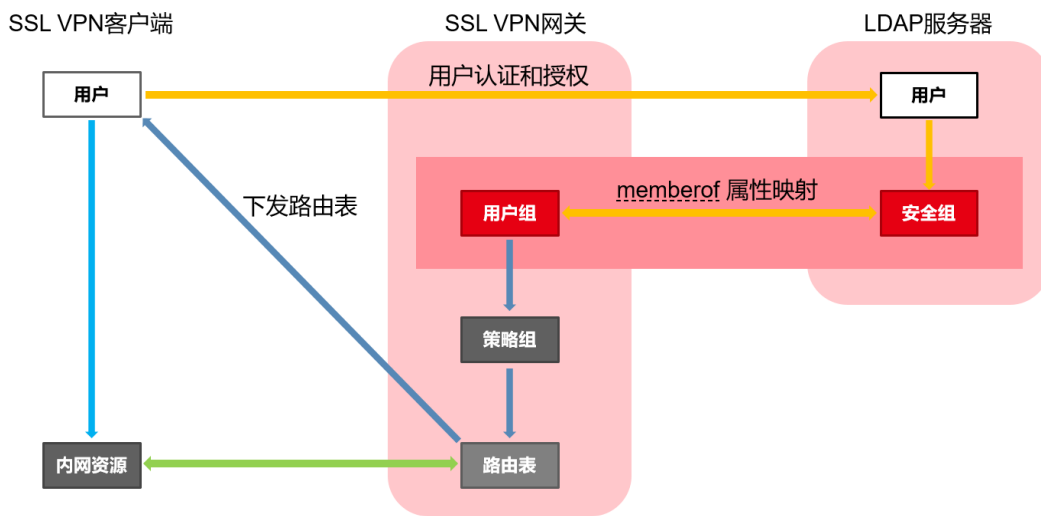
针对不同的用户过滤条件，在 iNode 客户端上输入对应的用户名和密码即可。



11, 检查 LDAP 属性映射是否正确

在用户的 LDAP 授权过程中，设备会通过查询操作得到用户的授权信息，该授权信息由 LDAP 服务器通过若干 LDAP 属性下发给设备。若设备从 LDAP 服务器查询得到某 LDAP 属性，则该属性只有在被设备的 AAA 模块解析之后才能实际生效。如果某 LDAP 服务器下发给用户的属性不能被 AAA 模块解析，则该属性将被忽略。因此，需要通过配置 LDAP 属性映射表来指定要获取哪些 LDAP 属性，以及 LDAP 服务器下发的这些属性将被 AAA 模块解析为什么类型的 AAA 属性，具体映射为哪种类型的 AAA 属性由实际应用需求决定。每一个 LDAP 属性映射表项定义了一个 LDAP 属性与一个 AAA 属性的对应关系。将一个 LDAP 属性表在指定的 LDAP 方案视图中引用后，该映射关系将在 LDAP 授权过程中生效。

通常情况下，我们将授权特定安全组(即 memberof 属性)的用户显示特定资源，将 LDAP 上对应的用户所在的安全组与设备上到用户组 (user-group) 进行映射，用户组下绑定对应 SSL VPN 资源，从而为接入用户达到授权的目的。SSL VPN 结合 LDAP 授权流程图如下：



如果上图任何操作存在问题，则无法实现通过 LDAP 服务器对 SSL VPN 用户进行授权的操作了，我们按照各种情况一一说起。

(1) LDAP 方案中没有调用 LDAP 属性映射表，显示授权成功，但不会返回任何信息。

```
PAM_LDAP:Keep state authorization searching for incomplete searching.
*Dec 17 15:51:13:929 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Get result message errno = 0
*Dec 17 15:51:13:929 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:User alice search done.
*Dec 17 15:51:13:930 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP: Processing LDAP authorization.
*Dec 17 15:51:13:930 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authorization reply successfully obtained, resultCode: 0.
*Dec 17 15:51:13:930 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP: LDAP authorization succeeded.
```

(2) LDAP 方案中调用的 LDAP 属性映射表名称错误，比如将 map 调用成 map1，此时认证阶段调试信息中会提示无法获取属性信息报错：Failed to get search attributes。

```
PAM_LDAP:Search user when authorization.
*Dec 17 15:54:02:509 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Username is alice.
*Dec 17 15:54:02:509 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP[Author]:Failed to get search attributes.
*Dec 17 15:54:02:509 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Failed to search user.
*Dec 17 15:54:02:509 2019 H3C LDAP/7/ERROR: -Context=1;
PAM_LDAP:Failed to start state machine.
*Dec 17 15:54:02:509 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP: Processing LDAP authorization.
*Dec 17 15:54:02:509 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authorization reply successfully obtained, resultCode: 2.
```

(3) LDAP 属性映射表中的属性名称配置错误，比如 memberof 写成了 membeof，和(1)一样显示授权成功，但不会返回任何信息。

```
*Dec 17 14:29:11:267 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Get result message errno = 0
*Dec 17 14:29:11:267 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:User alice search done.
*Dec 17 14:29:11:267 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP: Processing LDAP authorization.
*Dec 17 14:29:11:267 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authorization reply successfully obtained, resultCode: 0.
*Dec 17 14:29:11:267 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP: LDAP authorization succeeded.
```

(4) LDAP 属性映射表中的属性前缀和分割符配置错误，比如我们将 `prefix CN= delimiter ,` 配置成 `prefix CN delimiter ,`，那么对于 `CN=Beijing,OU=测试组 1,DC=h3c,DC=com`，我们获取的用户组为=Beijing，但是设备不存在此用户组，将导致用户授权失败，调试信息如下：

```
*Dec 17 14:32:55:360 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Map user group name array =Beijing.
*Dec 17 14:32:55:360 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP: Processing LDAP authorization.
*Dec 17 14:32:55:360 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP:Data of authorization reply successfully obtained, resultCode: 0.
*Dec 17 14:32:55:360 2019 H3C LDAP/7/EVENT: -Context=1;
PAM_LDAP: LDAP authorization succeeded.
```

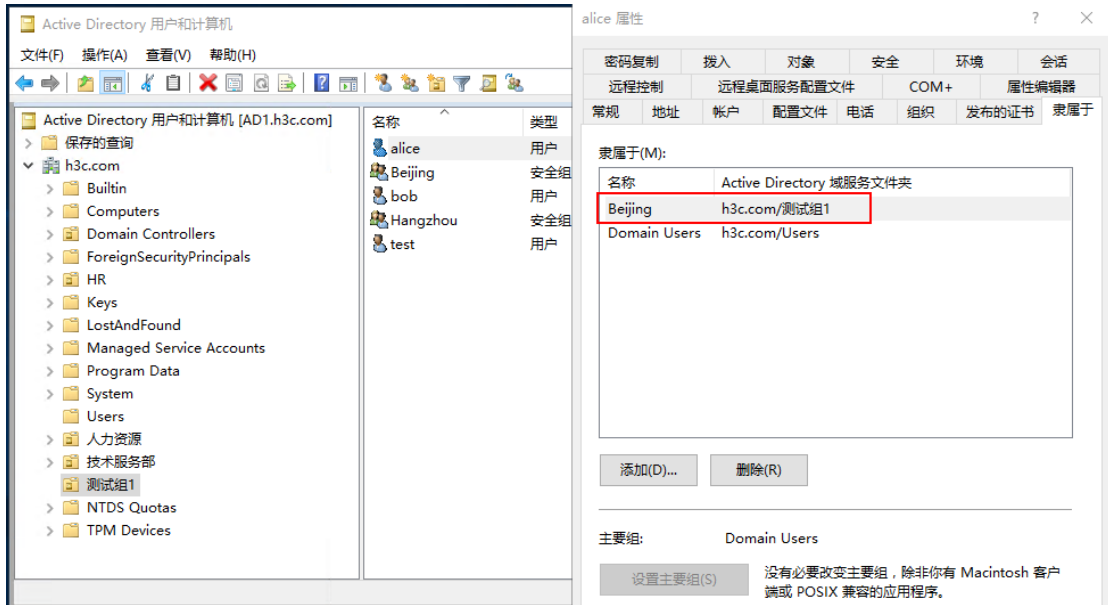
(5) 无用户组或者用户组不正确或者用户组下没有绑定 SSL VPN 绑定资源或者绑定资源名称错误，此时和 LDAP 认证过程已经没有关系，和 SSL VPN 模块有关，此时 LDAP 的调试一切正常，SSL VPN 调试会报以下错误：

```
*Dec 17 15:21:29:698 2019 H3C SSLVPNK/7/SSLVPN_ERROR: -Context=1; IPAC: Failed to get IP
resources. ContextID=0x1, onlineID=0x1a.
```

这时候请仔细检查设备上用户组的配置是否正确。

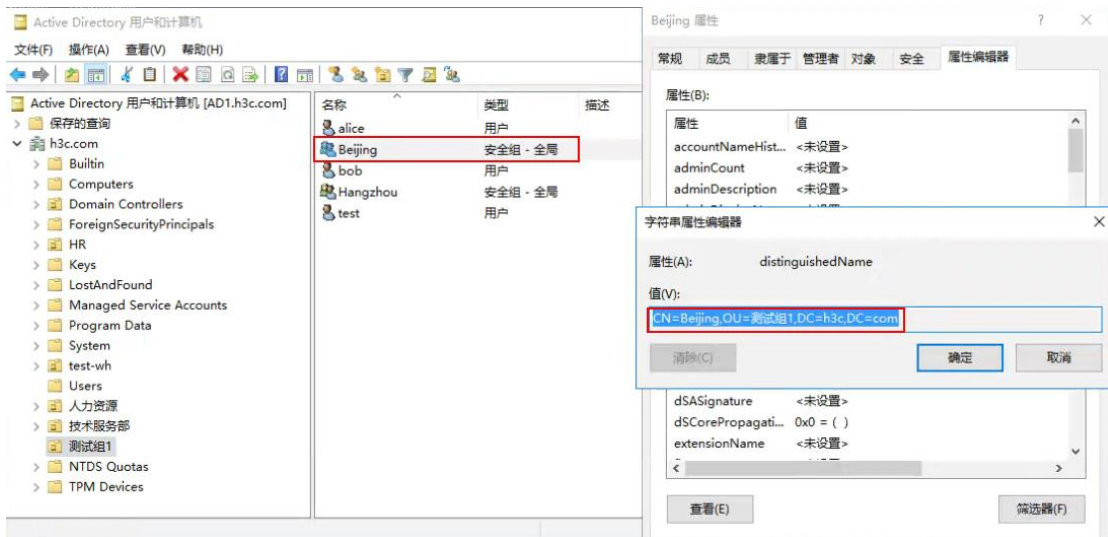
12. 修改 LDAP 属性映射

以用户 `alice` 为例，可以看到 LDAP 服务器上该用户隶属于 `Beijing` 这个安全组，LDAP 服务器上每一个创建的用户自动隶属于 `Domain Users`，且此用户组为主要组，且没有必要修改主要组。



通过查看 Beijing 这个安全组的属性，查询到其 DN 为：

CN=Beijing,OU=测试组 1,DC=h3c,DC=com



设备上通过映射的方式来提前对应的关键字，命令行下完整的操作为

```
[H3C] ldap attribute-map map
[H3C-ldap-attr-map-map]map ldap-attribute memberof prefix CN= delimiter ,
aaa-attribute user-group
```

ldap-attribute 参数表示要映射的 LDAP 属性，这里我们使用用户的 memberof 属性。prefix 和 delimiter 参数表示按照一定的格式提取 LDAP 属性字符串中的内容映射为 AAA 属性。其中，prefix 表示 LDAP 属性字符串中的某内容前缀（例如 cn=），delimiter 表示 LDAP 属性字符串中的内容分隔符（例如逗号）。经过上述操作，可以将 CN=Beijing,OU=测试组 1,DC=h3c,DC=com 中的 Beijing 这一关键字顺利提取出来。若不指定这两个可选参

数，则表示要将一个完整的 LDAP 属性字符串映射为指定的 AAA 属性，之后在 LDAP 方案中调用此映射。

```
[H3C]ldap scheme ldapscheme
[H3C-ldap-ldapscheme]attribute-map map
```

也可以在 Web 界面进行配置，如下在“对象->用户->认证管理->LDAP->LDAP 方案->编辑 LDAP 属性映射表”中编辑对应的属性：

属性名称	前缀	分隔符	AAA属性	编辑
<input type="checkbox"/> memberof	CN=	,	user-group	

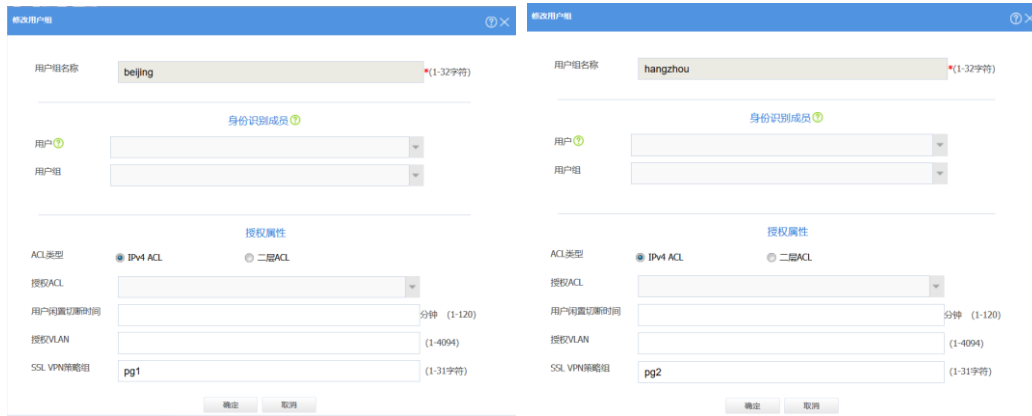
然后在“对象->用户->认证管理->LDAP->LDAP 方案->编辑 LDAP 方案”中选择创建的属性映射表 map，然后点击确定，如下：

名称: ldapscheme
属性映射表: map

完成上述操作后，创建 beijing 和 hangzhou 两个用户组，分别调用 pg1 和 pg2 的两个 SSL VPN 策略组，然后在 LDAP 方案中调用此 LDAP 属性映射表。

```
[H3C]user-group beijing
[H3C-ugroup-beijing]authorization-attribute sslvpn-policy-group pg1
[H3C]user-group hangzhou
[H3C-ugroup-hangzhou] authorization-attribute sslvpn-policy-group pg2
```

同样也可以在 web 界面创建相关用户组，如下：



13, 拨打热线 400-810-0504 寻求帮助

完成上述排查步骤后，就可以实现 LDAP 服务器对用户的认证和授权操作了，如果按照上述排查思路排查结果仍然存在异常，请收集完整的 debug 信息、设备的完整配置、LDAP 服务器上对应用户的属性和属性截图以及相关的抓包信息返回总部进行分析，技术支持热线为 400-810-0504。