

知

某局点ACG1000设备LDAP用户不同步问题处理经验案例

ACG1000

LDAP

冷L桔梗

2021-12-10 发表

组网及说明

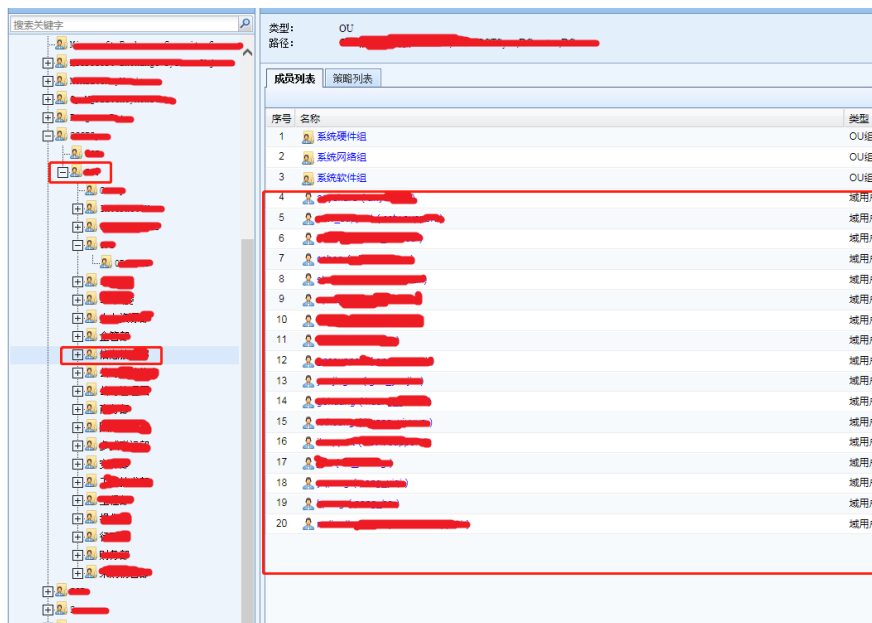
组网不涉及

问题描述

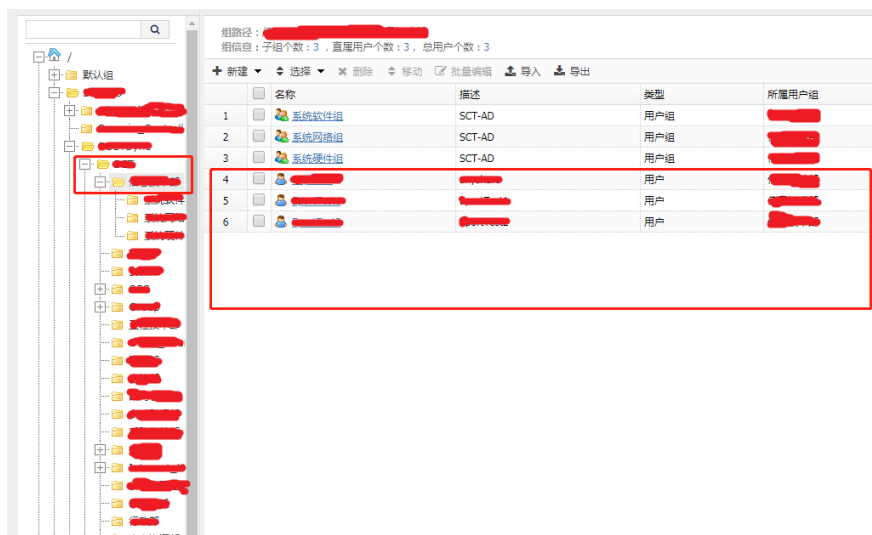
将LDAP服务器的用户同步到ACG1000设备上，结果发现同步信息不全

过程分析

查看LDAP服务器用户信息：



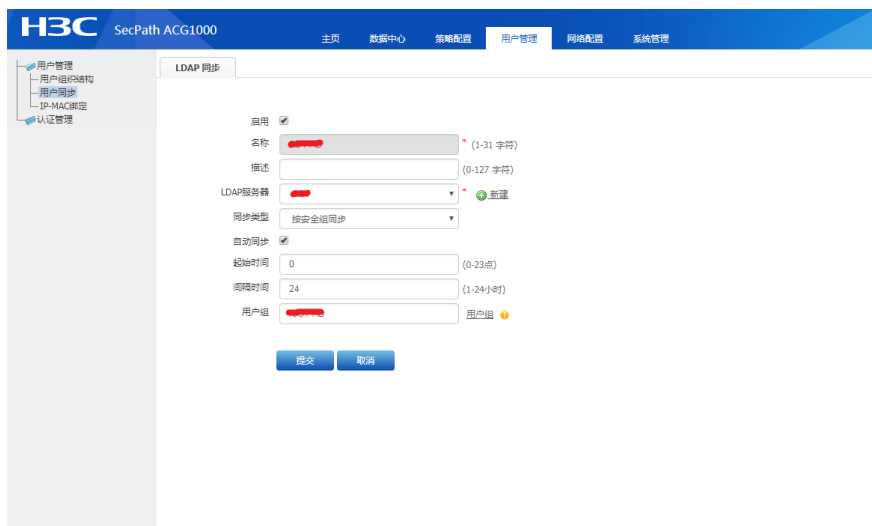
查看ACG上同步用户信息：



发现用户信息大部分丢失

查看同步配置，发现LDAP服务器类型为OU，同步配置也为OU，将类型修改为安全组同步，查看同步结果有增加，但是仍然未同步完全

同步配置：



同步结果（蓝框为OU类型同步，红框为安全组类型同步）：

解决方法

因为和LDAP的编码不匹配，导致编码发过来的报文带有和，这两个非法字符，设备无法识别

解决方法：更改LDAP的配置，修改用户名或者手工配置建立用户

同步结果

同步时间	同步结果
1	同步3216个用户，新增录入1383个用户
2	同步3360个用户，新增录入0个用户
3	同步失败（无此DN或DN下无同步对象）
4	同步失败（无此DN或DN下无同步对象）
5	同步3360个用户，新增录入0个用户
6	同步3360个用户，新增录入0个用户
7	同步3360个用户，新增录入0个用户
8	同步3360个用户，新增录入1个用户

查看报文发现LDAP服务器发给ACG设备的用户名有非法字符和，这两个非法字符导致ACG无法录入本地用户

3566 (13798)	18798 10.1.2.100	10.28.2.118	LDAP	searchResEntry(3695) "CN=chen,cheng,OU=,OU=SET,OU=SCCTSync,DC=sctcn,DC=com" searc
b0ed (45293)	18799 10.28.2.118	10.1.2.100	TCP	36941 → 389 [ACK] Seq=413750 Ack=11712500 Win=131392 Len=0
b0ee (45294)	18800 10.28.2.118	10.1.2.100	TCP	36941 → 389 [ACK] Seq=413750 Ack=11716769 Win=129024 Len=0
b0ef (45295)	18801 10.28.2.118	10.1.2.100	LDAP	searchRequest(3696) "CN=cheng,Bo,OU=,OU=SET,OU=SCCTSync,DC=sctcn,DC=com" baseObject

查看官网LDAP限制说明：

LDAP同步用户的限制？

AD服务器上用户名超长(大于63字符)，含有异常字符（汉字数字字母以及@_-0[]以外的特殊字符）可以同步，不能录入到本地用户结构，同步过程中会依次在本地用户结构添加用户、用户组，本地满规格时无法录入，同步规格和本地用户规格相同。

