

# 知 某局点使用WX3520H-F结合LDAP做portal认证， portal认证用户登录失败问题排查案例

Portal 徐猛 2018-10-30 发表

## 组网及说明

现场一台无线控制器WX3520H-F旁挂在核心交换机上，并使用集中转发的方式进行终端业务数据的转发。同时该无线控制器能和LDAP服务器通信，并结合LDAP服务器进行终端的认证。

## 问题描述

现场使用我们的无线控制器结合LDAP服务器进行portal认证，目前portal页面正常弹出，但是输入用户名和密码后提示认证失败，使用的认证域非缺省认证域，认证的时候加上域信息依旧认证失败。加上域信息进行认证，依旧失败的报错情况截图如下：



## 过程分析

1. 初始第一次检查现场设备配置如下：

```
#  
wlan service-template 1  
description waibu  
ssid I-KEJI  
vlan 112  
portal enable method direct  
portal domain ldap  
portal apply web-server newpt  
service-template enable  
  
#  
ldap server ldap  
login-dn uid=wlan,ou=manager,dc=scst,dc=edu,dc=cn  
search-base-dn ou=jzg,ou=people,dc=scst,dc=edu,dc=cn  
ip 10.1.2.25  
login-password cipher $c$3$mXkuOQSeD/QLK0w1b+ZmKbyHmkI4nYodD7gN8OO9hVs=  
  
#  
ldap scheme ldap  
authentication-server ldap  
  
#  
domain ldap  
authorization-attribute idle-cut 15 1024  
authentication portal ldap-scheme ldap  
authorization portal none  
accounting portal none  
  
#  
portal web-server newpt  
url http://172.19.255.100:8080/portal  
server-type cmcc  
#
```

```

portal local-web-server http
default-logon-page defaultfile.zip
tcp-port 8080
#
ip http enable
#
检查配置暂未发现存在异常。

```

2.进行debug分析如下：

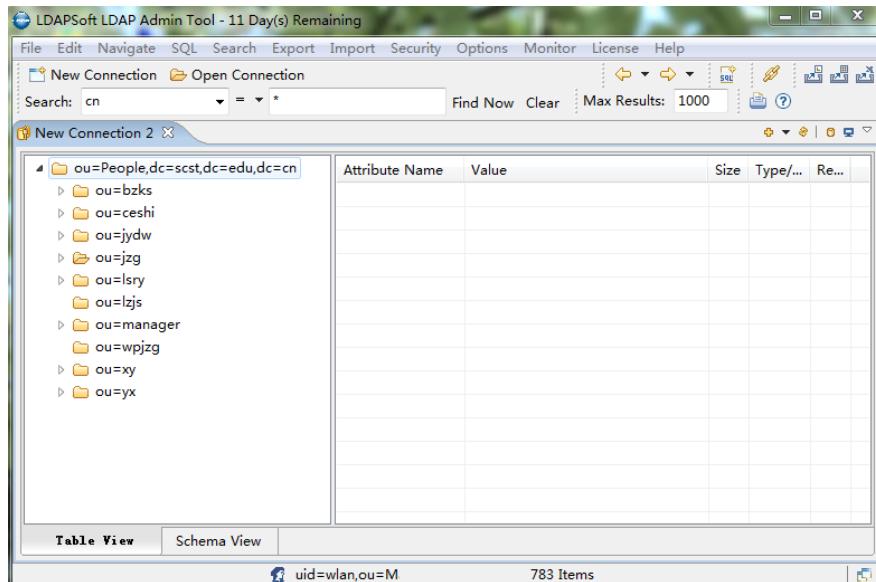
```

*Oct 9 12:09:41:083 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP:Administrator's binding operation completed.
*Oct 9 12:09:41:083 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP:Response timeout timer successfully created.
*Oct 9 12:09:41:085 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP:Get result message errno = 0
*Oct 9 12:09:41:085 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP[State]:State switch from binding admin to authentication searching.
*Oct 9 12:09:41:085 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP:Search user when authentication.
*Oct 9 12:09:41:085 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP:Username is 31013.
*Oct 9 12:09:41:085 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP[Authen]:Search filter is (&(objectClass=person)(cn=31013)).
*Oct 9 12:09:41:085 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP[Authen]:Search base DN is ou=people,dc=scst,dc=edu,dc=cn.
*Oct 9 12:09:41:086 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP:Get result message errno = 0
*Oct 9 12:09:41:087 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP:User 31013 search done.
*Oct 9 12:09:41:087 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP[State]:State switch from authentication searching to binding user.
*Oct 9 12:09:41:087 2018 WX3520H-F LDAP/7/ERROR:
PAM_LDAP:Failed to bind user 31013 for the result of searching DN is NULL. /查找DN是空的
*Oct 9 12:09:41:087 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP:Processing LDAP authentication.
*Oct 9 12:09:41:087 2018 WX3520H-F LDAP/7/EVENT:
PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.
*Oct 9 12:09:41:087 2018 WX3520H-F PORTAL/7/EVENT: User-SM[172.19.255.192]: Received authentication response, RespCode=26.

```

报错显示查找DN是空的。

3.让现场反馈用户的LDAP服务器上查看的用户信息如下：



Search Results (1)					
	Attribute Name	Value	Size	Type/Editor	Required
1	objectClass	top	3	ObjectClass	Y
2	objectClass	person	5	ObjectClass	Y
3	objectClass	organizationalPerson	20	ObjectClass	Y
4	objectClass	user	13	ObjectClass	Y
5	objectClass	inetOrgPerson	16	ObjectClass	Y
6	cn	刘强东	9	Text	Y
7	sn	刘强东	9	Text	Y
8	addFrom	是	18	Text	N
9	birthday	1970-03-30	10	Text	N
10	createTimestamp	20100006Z (*****)	15	Operational	N
11	createUserName	root	20	Operational	N
12	entryType	directory manager	47	Operational	N
13	gender	男	1	Text	N
14	inetUserStatus	Active	6	Text	N
15	iplanet-am-user-alias-list	刘强东	18	Text	N
16	memberOf	cn=Groups,dc=scst,dc=edu,dc=cn	37	DN	N
17	pwdLastSet	ctory manager	20	Operational	N
18	pwdLastSetTime	28012852Z (***** ***** 28 2016 09:28:52 GMT+0800)	15	Operational	N
19	privacyProtected	0	1	Text	N
20	pwdPolicy	1	1	Integer	N
21	pwdPolicyAnswer	李彦宏	9	Text	N
22	pwdPolicyQuestion	你的运动委员是谁?	33	Text	N
23	securityEmail	183@qq.com	16	Text	N
24	sambaHomeDirEntry	cn=ema	9	Operational	N
25	uid	31013	5	Text	N

经查看现场用户目录，发现LDAP服务器侧查询的用户属性类型为UID类型的，而我们无线设备侧在配置LDAP服务器时，缺省查看的用户属性类型为CN类型的。

解决方法

查看官网资料，可配置的LDAP用户属性参数列表如下：

操作	命令	说明
进入系统视图	system-view	-
进入LDAP服务器视图	ldap server server-name	-
配置用户查询的起始DN	search-base-dn base-dn	缺省情况下，未指定用户查询的起始DN
(可选) 配置用户查询的范围	search-scope { all-level   single-level }	缺省情况下，用户查询的范围为all-level
(可选) 配置用户查询的用户名属性	user-parameters user-name-attribute { name-attribute   cn   uid }	缺省情况下，用户查询的用户名属性为cn
(可选) 配置用户查询的用户名格式	user-parameters user-name-format { with-domain   without-domain }	缺省情况下，用户查询的用户名格式为without-domain
(可选) 配置用户查询的自定义用户对象类型	user-parameters user-object-class object-class-name	缺省情况下，未指定自定义用户对象类型，根据使用的LDAP服务器的类型使用各服务器缺省的用户对象类型

后续现场添加配置 user-parameters user-name-attribute uid 后正常。

```
#  
ldap server ldap  
login-dn uid=wlan,ou=manager,dc=scst,dc=edu,dc=cn  
user-parameters user-name-attribute uid  
search-base-dn ou=jzg,ou=people,dc=scst,dc=edu,dc=cn  
ip 10.1.2.25  
login-password cipher $c$3$mXkuOQSeD/QLKOW1b+ZmKbyHmkI4nYodD7gN8OO9hVs=  
#
```