

AC结合云简与LDAP服务器配合进行Portal认证

Portal shawcccc 2023-08-14 发表

问题描述

Portal页面正常弹出，但是LDAP认证失败

Debugging ldp all报PAM_LDAP: Failed to perform binding operation as administrator 无法以管理员身份执行绑定操作

```
%WIFI[0]: Jul 31 15:18:56:076 2023 AC-Master PORTAL/6/PORTAL_PACKET_TO_AAA: -UserIP=172.18.100.223-UserMAC=F8-7D-76
          authentication request to AAA.
*Jul 31 15:18:56:079 2023 AC-Master LDAP/7/EVENT:
PAM_LDAP:Processing LDAP authentication.
*Jul 31 15:18:56:079 2023 AC-Master LDAP/7/EVENT:
PAM_LDAP:Data of authentication request successfully sent.
*Jul 31 15:18:56:080 2023 AC-Master LDAP/7/EVENT:
PAM_LDAP:Processing LDAP authentication data.
*Jul 31 15:18:56:080 2023 AC-Master LDAP/7/EVENT:
PAM_LDAP:LDAP server is: 172.29.29.51.
*Jul 31 15:18:56:080 2023 AC-Master LDAP/7/EVENT:
PAM LDAP:Created new connection.
*Jul 31 15:18:56:080 2023 AC-Master LDAP/7/EVENT:
PAM LDAP:Current bind state is 0.
*Jul 31 15:18:56:080 2023 AC-Master LDAP/7/EVENT:
PAM LDAP:State of State switch from init to binding admin.
*Jul 31 15:18:56:080 2023 AC-Master LDAP/7/EVENT:
PAM LDAP:Executing bind operation, DN is cn=dcadmin,ou=user,dc=necse,dc=china.
*Jul 31 15:18:56:089 2023 AC-Master LDAP/7/EVENT:
PAM LDAP:Performing binding operation as administrator.
*Jul 31 15:18:57:931 2023 AC-Master LDAP/7/EVENT:
PAM LDAP:Administrator's binding operation completed.
*Jul 31 15:18:57:931 2023 AC-Master LDAP/7/EVENT:
PAM LDAP:Response timeout timer successfully created.
*Jul 31 15:18:57:933 2023 AC-Master LDAP/7/EVENT:
PAM LDAP:Get Session Response, errno = 40.
*Jul 31 15:18:57:933 2023 AC-Master LDAP/7/EVENT:
PAM LDAP:Failed to perform binding operation as administrator.
*Jul 31 15:18:57:934 2023 AC-Master LDAP/7/EVENT:
PAM LDAP:Processing LDAP authentication.
*Jul 31 15:18:57:934 2023 AC-Master LDAP/7/EVENT:
PAM LDAP:Data of authentication reply successfully obtained, resultCode: 1.
```

过程分析

Base CN和管理员CN皆在云简上进行配置



检测AC上下发ldap server下发配置，存在以下错误

ldap server cloud_ldap

login-dn cn=blj_dcadmin, ou=user // 缺少dc，同时配置管理员权限的用户dn缺少上级目录

完整配置应为login-dn cn=domainwifi , ou=user,ou=网络设备同步账号, ou=sysadmins,[dc=necse,dc=china](#)

search-base-dn dc=necse,dc=china

ip 10.110.21.2

login-password cipher \$c\$3\$0Ks2uVlG0PipM2gsBlc4XinNf7+EbxgVlqPsFg+2

user-parameters user-name-attribute samaccountname

protocol-version v2 // 删除 Microsoft的LDAP服务器只支持LDAPv3，AC缺省配置为v3

解决方法

管理员权限的用户dn每一级目录都需配置，完成配置后认证成功

