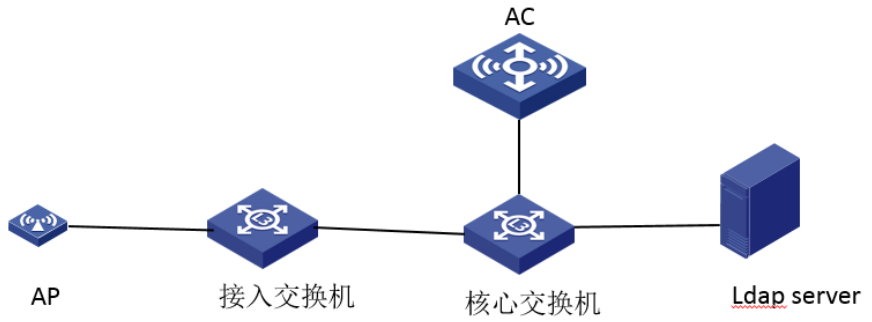
AC结合ldap做portal认证输入用户名密码提示登陆失败，请重试

Portal wlan接入 king666 2019-10-12 发表

组网及说明

组网方式：



问题描述

AC结合第三方ldap服务器做portal认证,之前使用正常，之后突然出现终端连上无线在portal页面输入用户名密码后提示“登陆失败，请重试”。

过程分析

1、检查AC的配置如下，未发现错误配置，确认配置也没有修改过。

```
wlan service-template inside
description LDAP
ssid AMSC
vlan 511
user-isolation enable
portal enable method direct
portal domain ldap
portal bas-ip 10.127.0.4
portal apply web-server newpt
service-template enable

ldap server ldap
login-dn cn=administrator,cn=users,dc=amscdomain,dc=com
search-base-dn dc=amscdomain,dc=com
ip 10.8.0.1
login-password cipher $c$3$q3ygeh60lD20k8iteb5aRW+680+D4lpodd1sLVw2uSjd14Q=
user-parameters user-name-attribute samaccountname
```

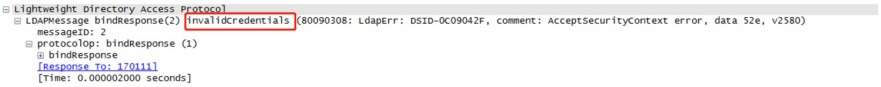
2、通过在AC上抓ldap server侧的报文发现AC发出了bindrequest报文，之后ldap server回复的bindresponse报文中显示凭证无效“invalidcredentials”。怀疑是用户名和密码配置不一致或者用户权限有问题。

```
172.255.0.14    10.8.0.1        LDAP    142 bindRequest(2) "cn=administrator,cn=users,dc=amscdomain,dc=com" simple
10.8.0.1        172.255.0.14    LDAP    176 bindResponse(2) invalidCredentials (80090308: LdapErr: DSID-0C09042F, comment: Acce
```

请求报文

```
⊟ Lightweight Directory Access Protocol
  ⊟ LDAPMessage bindRequest(2) "cn=administrator,cn=users,dc=amscdomain,dc=com" simple
      messageID: 2
    ⊟ protocolOp: bindRequest (0)
      ⊟ bindRequest
          version: 3
          name: cn=administrator,cn=users,dc=amscdomain,dc=com
        ⊟ authentication: simple (0)
            simple: 42664259622a30256c5354706574514f
      [Response In: 170114]
```

回复报文



3、通过debug信息发现以一条报错如下，含义是ldap上面的用户没有管理员权限。

PAM_LDAP:Failed to perform binding operation as administrator.
跟客户再三确认故障前后ldap服务器有没有变更或者改动，经排查发现是管理员将用户移除了，重新添加后问题解决。

解决方法

在ldap的服务器上重新添加用户后问题解决。