

知 某局点v7 portal结合ldap认证失败问题

Portal 陆启隆 2021-08-04 发表

组网及说明

普通无线组网，使用v7 ac，终端的网关和dhcp server在核心交换机。

问题描述

终端可以接入无线服务，并获取到地址，可以弹出portal页面，但是提示认证失败。

过程分析

可以弹出portal页面，输入用户名和密码点击提交报出认证失败，表明portal认证没有问题，应该着重分析ldap过程。

现场在ac上开启ldap的debug。

Debug中存在error报错，

```
*Apr 20 10:18:43:277 2021 无线控制器 LDAP/7/EVENT:
```

```
PAM_LDAP:Get result message errno = 49
```

```
*Apr 20 10:18:43:277 2021 无线控制器 LDAP/7/ERROR:
```

```
PAM_LDAP:Failed to perform binding operation as user.
```

服务器回复bindresponse中报错原因代码49，认证失败，但是具体的失败信息，需要从抓包中查看详细原因代码。

在ac于ldap之间进行抓包，查看报错代码为52e，密码或凭据无效，因此建议现场去检查用户名和密码配置。

```
130481 533.420.172.21.233. 10.10.104. LDAP 115 bindRequest(9) "CN=...OU=VMware,DC=ncvcct,DC=
130482 533.423.10.10.104. 172.21.233. LDAP 164 bindResponse(9) invalidCredentials (80090308: L
131064 536.582.10.10.208. 10.10.104. LDAP 405 searchRequest(2818) "<ROOT>" baseObject
131066 536.583.10.10.104. 10.10.208. LDAP 1265 searchResEntry(2818) "<ROOT>" | searchResDone(-
131085 536.618.10.10.208. 10.10.104. LDAP 66 unbindRequest(2820)

Transmission Control Protocol, Src Port: 389, Dst Port: 34409, Seq: 221, Ack: 425, Len: 110
 Lightweight Directory Access Protocol
 LDAPMessage bindResponse(9) invalidCredentials (80090308: LdapErr: DSID-0C090436, comment: AcceptSecurityContext
 messageID: 9
  protocolOp: bindResponse (1)
  bindResponse
    resultCode: invalidCredentials (49)
    matchedDN:
      errorMessage: 80090308: LdapErr: DSID-0C090436, comment: AcceptSecurityContext error, data 52e, v4563
      [Response To: 130481]
```

常见的错误代码解释如下：

525—用户不存在

52e—密码或凭据无效

530—此时不允许登录

531—在此工作站上不允许登录

532—密码过期

533—账户禁用

701—账户过期

773—用户必须重置密码

775—用户账户锁定

解决方法

检查ldap服务器上配置的用户名和密码，再次检查输入用户名和密码后故障解除。

