

# 知 某局点EIA V9 LDAP认证错误密码也能正常通过

LDAP 范中鹏 2023-02-06 发表

## 问题描述

中南大学macportal+LDAP认证，使用错误密码也能正常通过。抓包中没有uam和ldap服务器的交互信息，ldap是openldap，使用bind请求认证，配置检测可以通过。

测试用户mac: 2A:62:4A:EB:EB:90 测试用户名: 32180287

用户在线记录如下图

NAS ID	帐号名	登录名	用户名	服务名	接入时间	接入时长	登录IP地址	用户IP地址	安全状态	客户端定制
	32180287				2022-12-26 15:45:34	00P			无密安全认证	

LDAP服务器信息，连通性为“是”

服务器地址: [redacted]  
服务器类型: 通用LDAP服务器  
管理员DN: [redacted]  
管理员密码: \*\*\*\*\*  
Base DN: [redacted]

高级信息

服务器版本:	3	服务同步方式:	手工触发
实时认证:	是	连接静默时长:	1分钟
端口:	389	同步超时时间(秒):	0
连接超时时间(秒):	30		
用户分组:	按OU同步		
父分组:			
业务分组:	未分组	启用SSL连接:	否
连接服务器:	是		
帐号名属性名称:	uid		
用户密码属性名称:	password		
支持Bind请求:	是		
帐号名形式:	保持原样		

## 过程分析

udm日志记录发送ldap请求消息时超时，用户认证是按照逃生处理

```
ldap ; simpleBndAuth: rcv message timeout while using primary server, return ok and update server  
_state to LDAP_SERVER_NOT_CONNECT.
```

第三方进程连不通LDAP server会回应81，LDAP服务器联通性会被修改为“否”

```
2022-12-26 15:18:40 [com.h3c.imf.105.100.MessageBroadcaster-43329] [INFO ] [com.h3c.imc.acm.a  
uthN.LdapAuthN:bindAuthn] resp is{ -- SEQUENCE --  
resultCode = 81  
}
```

经上述定位发现北向IP地址与域控不通

#### 解决方法

防火墙上放行北向IP后，认证正常。

