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

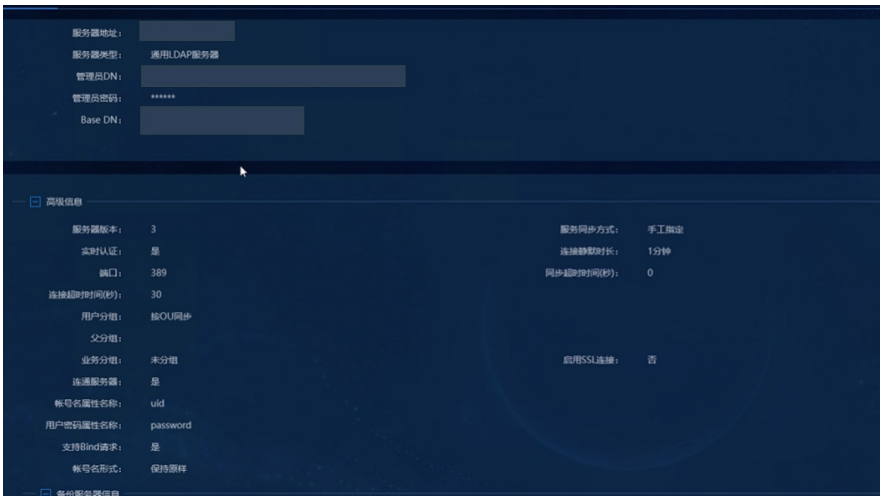
问题描述

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

LDAP服务器信息，连通性为“是”



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: recv 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.authN.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。