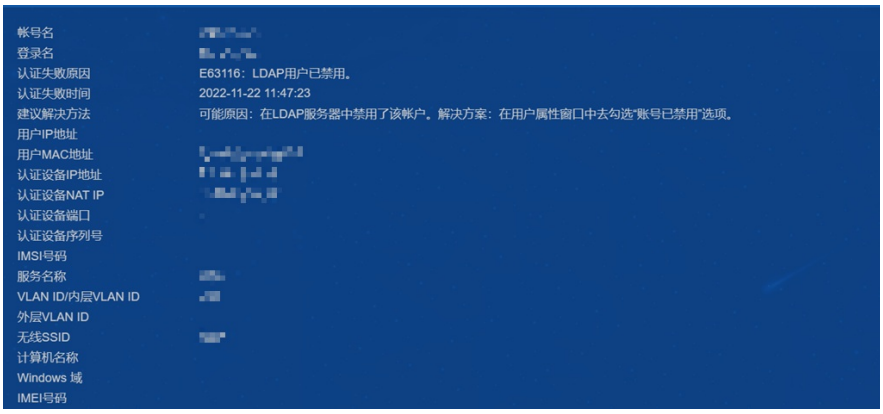
LDAP用户被禁用

LDAP 802.1X iMC UAM 陈启敏 2022-11-30 发表

问题描述

版本：imc 0706p12　eia 0623h01

无线802.1x结合ladp认证，之前业务正常，后整个机房异常掉电，再次上电后，发现ladp服务器同步过来的用户无法认证，提示ladp用户已被禁用



过程分析

1、检查ladp服务器上用户是否正常，新建用户没有问题
2、新建用户也无法认证，提示相同报错
3、异常断电导致，建议现场先在设备上逃生，然后重启imc和域控服务器测试，也无法恢复正常
4、查看认证失败原因，提出可能原因是ladp服务器禁用了该账户，需要在用户属性窗口中去勾选“账号已禁用”选项，操作后发现账户并未被禁用
5、查看imc的uam日志，报错与认证失败原因相同

```
%% 2022-11-22 08:47:55.875 ; [ERR] ; [14596] ; LDAP ; [encypt.parsePktLdap] gotHash:0, attrInvalid:0, usrMtched:1, err:10.
%% 2022-11-22 08:47:55.875 ; [HINT] ; [14596] ; EAP ; MsChapV2.authn: parsing-pkt from java-svr returned error [10, 63116].
%% 2022-11-22 08:47:55.875 ; [ERR] ; [14596] ; EAP ; EapProc.typeCall: eap module mschapv2 authen failed with err-no 2.
%% 2022-11-22 08:47:55.875 ; [ERR] ; [14596] ; EAP ; EapProc.typeSelect: fail to do typeCall for EAP/mschapv2.
%% 2022-11-22 08:47:55.875 ; [WARN] ; [14596] ; EAP ; eapProc.auth: typeSelect says reject with ErrCode 63116.
%% 2022-11-22 08:47:55.875 ; [ERR] ; [14596] ; EAP ; EapProc.wireFmt: peap auth by mschapv2 failend.
%% 2022-11-22 08:47:55.875 ; [ERR] ; [14596] ; EAP ; EapProc.compose: Reply_Message:E63116: The LDAP account is disabled..
%% 2022-11-22 08:47:55.875 ; [ERR] ; [14596] ; EAP ; peapProc: STATE invalid.
%% 2022-11-22 08:47:55.890 ; [ERR] ; [17112] ; EAP ; peapProc: Had sent TLV failure, rejecting.
%% 2022-11-22 08:47:55.890 ; [ERR] ; [17112] ; EAP ; EapProc.typeCall: eap module peap authen failed with err-no 2.
%% 2022-11-22 08:47:55.890 ; [ERR] ; [17112] ; EAP ; EapProc.typeSelect: fail to do typeCall for EAP/peap.
```

6、远程检查imc与域控服务器的配置，未发现异常
7、研发分析日志发现LDAP侧返回报错信息，协调LDAP侧运维人员协助分析，是否存在LDAP服务异常或其他原因

```
[2022年11月22日 下午2:29:00][Error]: The authentication error msg: Logon failure: account currently disabled., and error code: 10
[2022-11-22 14:29:00.833] [Error] [MSChapAuthProvider::authenticate]MSChap authentication unknown exception. The ifReload parameter is true <mscv2js.security.SecurityProviderException: Logon failure: account currently disabled.>
mscv2js.security.SecurityProviderException: Logon failure: account currently disabled.
        at mscv2js.mschap.MSChapAuth.connect(Unknown Source)
        at mscv2js.mschap.MSChapAuth.mschapv2Validate(Unknown Source)
        at mscv2js.mschap.MSChapAuthProvider.authenticate(Unknown Source)
        at mscv2js.server.MsChapAuthHandler.run(Unknown Source)
        at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1128)
        at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:628)
        at java.base/java.lang.Thread.run(Thread.java:829)
Caused by: jcifs.smb.SmbAuthException: Logon failure: account currently disabled.

[2022-11-21 18:02:01.264] [Error] [MSChapAuthProvider::authenticate]<pool-31-thread-1> authenticate Exception. <mscv2js.security.SecurityProviderException: Logon failure: account currently disabled.>
mscv2js.security.SecurityProviderException: Logon failure: account currently disabled.
        at mscv2js.mschap.MSChapAuth.connect(Unknown Source)
        at mscv2js.mschap.MSChapAuth.mschapv2Validate(Unknown Source)
        at mscv2js.mschap.MSChapAuthProvider.authenticate(Unknown Source)
        at mscv2js.server.MsChapAuthHandler.run(Unknown Source)
        at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1128)
```

at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:628)

at java.base/java.lang.Thread.run(Thread.java:829)

解决方法

Caused by: jcifs.smb.SmbAuthException: Logon failure: account currently disabled.

at jcifs/smb/SmbTransportImpl.checkStatus2(SmbTransportImpl.java:1410)

后发现域控重启，虚拟计算机被禁用，导致认证失败，在ldap服务器上解除禁用就可以了

如果是ad域控的话，可以在域控服务器上，看虚拟计算机账号的图标就可以看出来， 一般被禁用了账号图标上有个向下的粗箭头