802.1x+LDAP认证失败，认证失败日志报错“没有接收到MSCHAPv2 SERVER的认证信息报文”

iMC 高洋 2022-07-01 发表

组网及说明

不涉及

告警信息

现场用户使用802.1x+LDAP认证失败，认证失败日志报错“没有接收到MSCHAPv2 SERVER的认证信息报文”。

问题描述

现场用户使用802.1x+LDAP认证失败，认证失败日志报错“没有接收到MSCHAPv2 SERVER的认证信息报文”；

现场有两套EIA各自独立运行，新的EIA数据是从旧的EIA上dbman备份恢复得来的，其中旧的EIA昨天晚上点出现以上报错，新EIA今天早上7时左右出现以上报错。两套环境对接了同一个LDAP服务器，使用了同一个虚拟机账户。

过程分析

对于现场的LDAP认证，登录账号的密码需要由EIA上报给LDAP服务器进行验证，当EIA（mschapv2server进程）与域控服务器通信时，需要借助一台虚拟计算机。同一个虚拟计算机账号只能创建一个认证通道，也就只能和一个EIA进行对接。当两套EIA与同一个虚拟计算机账号进行通信时，会相互挤占认证通道，导致域控接收不到mschapv2server进程发送的验证信息，进而出现“没有接收到MSCHAPv2 SERVER的认证信息报文”的报错。

同时mschapv2server日志中有“authenticator check failed”的认证报错，结合其他局点相似的故障表项，可以认为“没有接收到MSCHAPv2 SERVER的认证信息报文”的报错是因为两台EIA对接了同一个LDAP服务器的一个虚拟机账号引起的。

[2022-04-28 07:25:07.965] [Error] [MSChapAuthProvider::authenticate]MSChap authentication unknown exception. The ifReload parameter is true <mscv2js.security.SecurityProviderException: **NetrLogonSamLogon return authenticator check failed**>

```
mscv2js.security.SecurityProviderException: NetrLogonSamLogon return authenticator check failed
  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:834)
```

[2022年4月28日 上午7:25:07][Error]: **Exception or unkown exception, create new channel connect with error code=1**

[2022年4月28日 上午7:28:09][Error]: The authentication error msg: **NetrLogonSamLogon return authenticator check failed, and error code: 1**

解决方法

两套EIA对接同一个LDAP服务器时不要使用同一个虚拟机账号或者两套EIA分别对接两台LDAP服务器。