某局点EIA LDAP用户portal认证失败原因为“LDAP服务器BASE DN配置错误”

iMC 马永鸿 2021-12-29 发表

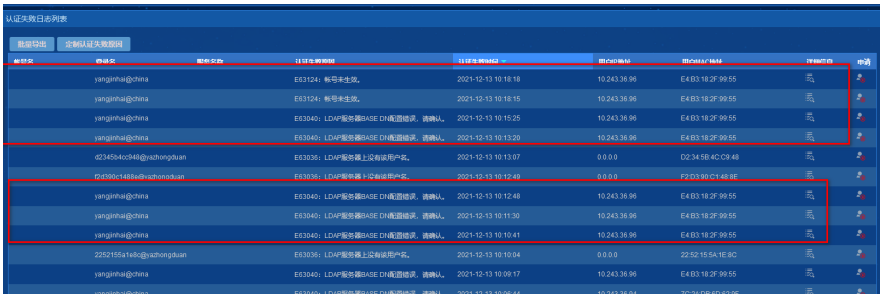
组网及说明

不涉及

问题描述

EIA版本7.3 E0611P09

现场EIA对接微软AD服务器，同步过来的用户进行portal认证，有部分用户认证失败。查看认证失败日志，失败原因为“LDAP服务器BASE DN配置错误”。



过程分析

分析uam debug日志：

%% 2021-12-13 10:20:57.298 ; [ERR] ; [3479168768] ; UsrMgr ; ldapUsr2Local: no free user matched with [cfgId=1,grpId=12954] for yangjinhai@china.

%% 2021-12-13 10:20:57.298 ; [ERR] ; [3479168768] ; ldap ; simpleLdapAuthProc: makeUsrComeReal failed: E63124: **The user account has not been generated**. Please retry 15 minutes later..

%% 2021-12-13 10:20:57.298 ; [ERR] ; [3479168768] ; LAN ; lanAuth.getUserSrvc: calling LdapAuthProc failed with err-msg : E63124: The user account has not been generated. Please retry 15 minutes later.

%% 2021-12-13 10:20:57.298 ; [ERR] ; [3479168768] ; LAN ; lanAuth.exec: fail to get user service, retCode: 63124.

%% 2021-12-13 10:20:57.298 ; [ERR] ; [3479168768] ; LAN ; lanAuthMsgProc.finsh: fail to authenticate the request message, retCode: 63124.

日志显示该用户没有被同步，结合认证失败原因，可能是现场ldap服务器的组织架构做了调整。
域控上修改组织架构后，EIA上同步用户还是以原来的组织架构去查询用户，发现查询不到用户，就会把用户置为不存在，后续这些用户上线时，还是用老的DN去查询用户，就会提示Base DN配置错误。

解决方法

现场可以尝试开启LDAP业务参数“ LDAP同步时自动删除已经不存在的用户 ”，然后重新同步用户即可。

同时也有“ 相同优先级的同步策略间用户转移 ”，也可以开启此参数，重新同步用户。