

知 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”。

用户名	操作名称	错误信息	错误时间	源IP地址	目标IP地址	源端口	目标端口	认证结果
yangmai@china	ES3124	帐号未生效。	2021-12-13 10:18:18	10.243.36.99	E4B318.2F.99.55			失败
yangmai@china	ES3124	帐号未生效。	2021-12-13 10:18:15	10.243.36.99	E4B318.2F.99.55			失败
yangmai@china	ES3040	LDAP服务器BASE DN配置错误，请确认。	2021-12-13 10:15:25	10.243.36.99	E4B318.2F.99.55			失败
yangmai@china	ES3040	LDAP服务器BASE DN配置错误，请确认。	2021-12-13 10:15:20	10.243.36.99	E4B318.2F.99.55			失败
023456789@yazhongguan	ES3036	LDAP服务器上不存在用户名。	2021-12-13 10:13:07	0.0.0.0	02.34.56.4C.C9.48			失败
01090c1488e1b4ad80ad0a	ES3036	LDAP服务器上不存在用户名。	2021-12-13 10:12:49	0.0.0.0	F2.D3.99.C9.48.9E			失败
yangmai@china	ES3040	LDAP服务器BASE DN配置错误，请确认。	2021-12-13 10:12:48	10.243.36.99	E4B318.2F.99.55			失败
yangmai@china	ES3040	LDAP服务器BASE DN配置错误，请确认。	2021-12-13 10:11:30	10.243.36.99	E4B318.2F.99.55			失败
yangmai@china	ES3040	LDAP服务器BASE DN配置错误，请确认。	2021-12-13 10:10:41	10.243.36.99	E4B318.2F.99.55			失败
2252155a160@yazhongguan	ES3039	LDAP服务器上不存在用户名。	2021-12-13 10:10:04	0.0.0.0	22.52.15.5A.7E.9C			失败
yangmai@china	ES3040	LDAP服务器BASE DN配置错误，请确认。	2021-12-13 10:09:17	10.243.36.99	E4B318.2F.99.55			失败
yangmai@china	ES3040	LDAP服务器BASE DN配置错误，请确认。	2021-12-13 10:09:11	10.243.36.99	E4B318.2F.99.55			失败

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。

The screenshot displays the H3C Management Center interface for LDAP configuration. The left sidebar shows a navigation menu with 'LDAP业务管理' (LDAP Business Management) expanded, and '同步策略配置' (Synchronization Policy Configuration) selected. The main content area is titled 'LDAP功能参数' (LDAP Function Parameters) and is divided into two sections: '基本参数' (Basic Parameters) and '同步配置参数' (Synchronization Configuration Parameters).

基本参数 (Basic Parameters):

LDAP按需认证模式	本地备份
LDAP服务器故障时逃生	启用
LDAP服务器异常发送告警	禁止
MSCHAPv2 Server日志级别	警告
MSCHAPv2 认证未知异常重建通道	允许
MSCHAPv2 Server进程重启	修改计算机密码脚本

同步配置参数 (Synchronization Configuration Parameters):

LDAP同步时自动删除已经不存在的用户	启用
LDAP用户在同步策略间转移	允许
相同优先级的同步策略间用户转移	禁止
同步转移接入服务(手工指定)	禁止
同步转移接入服务(基于AD组)	允许
同步转移用户分组	禁止
同步策略间相同平台用户的用户分组转移	允许
LDAP同步处理成值	100
LDAP分页(条)	1000

The 'LDAP同步时自动删除已经不存在的用户' parameter is highlighted with a red box in the original image. A '确定' (Confirm) button is visible at the bottom right of the configuration area.

