

知 LDAP用户认证时，输入了正确的用户名和密码，但是认证失败，提示密码错误。

iMC EIA LDAP 潘榕略 2019-03-06 发表

组网及说明

不涉及

问题描述

LDAP用户认证时，输入了正确的用户名和密码，但是认证失败，提示密码错误。

过程分析

原因分析：

LDAP用户认证时，输入了正确的用户名和密码。UAM收到认证请求后将认证请求转发给LDAP服务器。如果LDAP用户密码已经过期，或LDAP用户为新建用户且要求下次登录修改密码，则LDAP服务器会返回认证结果给UAM。LDAP服务器类型、认证方式和认证结果的关系如下表所述。

表1 认证结果

LDAP服务器类型	LDAP用户认证方式	认证结果
微软Active Directory	EAP-PEAP/EAP-MSCHAPv2	认证失败，通知用户密码错误。
	CHAP	Windows AD类型的LDAP服务器不支持CHAP认证。
	除EAP-PEAP/EAP-MSCHAPv2和CHAP外的其他认证方式	认证成功。
通用LDAP服务器	任意认证方式	认证失败，通知用户密码错误。

由上表可知，LDAP用户认证失败并收到密码错误的提示是由于用户的密码已经过期，或该用户是新建用户且设置了下次登录时需修改密码。而仅当LDAP服务器为微软AD，且并没有采用EAP-PEAP/EAP-MSCHAPv2方式认证时，密码过期和新用户下次登录需修改密码的问题才会被忽略。

解决方法

解决方法如下：

解决方法

LDAP服务器类型	LDAP用户认证方式	解决方法
微软Active Directory	EAP-PEAP/EAP-MSCHAPv2	1. 修改LDAP用户所使用接入策略中的首选EAP类型。 2. 到AD上重置用户密码的过期时间，或取消下次登录需修改密码的配置。
	除EAP-PEAP/EAP-MSCHAPv2和CHAP外的其他认证方式	无需解决。
通用LDAP服务器	任意认证方式	到LDAP服务器上重置用户密码的过期时间，或取消下次登录需修改密码的配置。