

关于iMC UAM&EIA开启LDAP按需同步实时认证功能会导致UAM&EIA处理性能异常的技术公告

舒中华 2015-12-15 发表

iMC UAM&EIA (iMC UAM/EIA V5-V7版本) 支持和LDAP服务器对接实现LDAP域账号准入认证。iMC和LDAP服务器同步的方式分为：按需同步和自动同步。而按需同步认证模式又分为“实时认证”和“本地备份”两种。按需认证模式为“实时认证”的优势是：在LDAP服务器侧创建了新的域账号后，终端可以立即上线，无需等待临时表同步时间。但同时会有性能风险，特别是客户业务环境中存在如下**三个条件**（满足任何一个条件都有可能导致问题），会偶发性导致UAM&EIA处理性能异常而认证失败。

- 1、按需认证模式为“实时认证”时，按需同步策略较多，当前出现问题局点的同步策略为15个，具体多少个同步策略会导致问题无法评估。
- 2、按需认证模式为“实时认证”时，LDAP服务器响应UAM&EIA检索速度慢，主要表现在组网环境复杂、LDAP服务器性能不佳的场景。
- 3、按需认证模式为“实时认证”时，网络中存在大量iMC中并不存在的用户接入请求报文。主要表现在接入设备启用了MAC认证，存在大量终端接入请求，而iMC中并没有该MAC地址的用户。

UAM&EIA按需同步实时认证模式的检索查询机制是：当收到一个账号请求后，先查询iMC本地有没有从LDAP服务器同步过来的账号，如果有则取出userDn属性内容，然后通过LDAP协议到LDAP服务器上绑定操作（即认证）；

如果iMC本地没有该账号，则逐个检索所有按需同步策略，一旦搜索到账号再到LDAP服务器上绑定操作（即认证），如果检索不到，则认证失败。在当前这种机制下，如果客户业务满足：“存在多个按需同步策略”、“LDAP服务器检索响应速度慢”、“网络中存在大量iMC中并不存在的账号的接入请求报文”这三个条件，很容易导致UAM&EIA处理性能问题。同时iMC前台和后台会打印输出如下队列满日志。

- 1、iMC前台“用户>用户接入日志>认证失败日志”会打印输出“E63700：接入用户认证队列满”日志，如下图所示。

		E63700::接入用户认证队列满。	2015-12-08 16:56:22			
		E63700::接入用户认证队列满。	2015-12-08 16:56:22			

- 2、UAM&EIA后台LOG会出现大量的“Message queue is full[256]”日志，如下图所示。

```
3307275 % 2015-12-08 16:31:28.437; [WARNING (2)]; [16392]; UAM; $SYS$; (NULL); (NULL); (NULL); rcv: [cmn2] Message queue is full[256]
3307624 % 2015-12-08 16:31:29.530; [WARNING (2)]; [16392]; UAM; $SYS$; (NULL); (NULL); (NULL); rcv: [cmn2] Message queue is full[256]
3307740 % 2015-12-08 16:31:30.201; [WARNING (2)]; [16392]; UAM; $SYS$; (NULL); (NULL); (NULL); rcv: [cmn2] Message queue is full[256]
3307898 % 2015-12-08 16:31:30.443; [WARNING (2)]; [16176]; UAM; $SYS$; (NULL); (NULL); (NULL); rcv: [cmn2] Message queue is full[256]
3307933 % 2015-12-08 16:31:30.612; [WARNING (2)]; [16392]; UAM; $SYS$; (NULL); (NULL); (NULL); rcv: [cmn2] Message queue is full[256]
3307958 % 2015-12-08 16:31:30.700; [WARNING (2)]; [16176]; UAM; $SYS$; (NULL); (NULL); (NULL); rcv: [cmn2] Message queue is full[256]
3307983 % 2015-12-08 16:31:31.012; [WARNING (2)]; [16176]; UAM; $SYS$; (NULL); (NULL); (NULL); rcv: [cmn2] Message queue is full[256]
3308008 % 2015-12-08 16:31:31.232; [WARNING (2)]; [16176]; UAM; $SYS$; (NULL); (NULL); (NULL); rcv: [cmn2] Message queue is full[256]
3308044 % 2015-12-08 16:31:31.242; [WARNING (2)]; [16392]; UAM; $SYS$; (NULL); (NULL); (NULL); rcv: [cmn2] Message queue is full[256]
3308069 % 2015-12-08 16:31:31.243; [WARNING (2)]; [16176]; UAM; $SYS$; (NULL); (NULL); (NULL); rcv: [cmn2] Message queue is full[256]
3308094 % 2015-12-08 16:31:31.267; [WARNING (2)]; [16176]; UAM; $SYS$; (NULL); (NULL); (NULL); rcv: [cmn2] Message queue is full[256]
```

UAM&EIA后台LOG目录：\\iMC\\uam\\log\\yyyyymmdd.log。

- 1、将LDAP按需认证模式修改为“本地备份”，如下图所示。

用户 > 接入策略管理 > LDAP业务管理 > 参数配置

LDAP功能参数

LDAP用户在同步策略间转移 允许

☒ LDAP分页(条) 1000

☒ LDAP同步/备份任务 每1天3点

日志级别 告警

LDAP按需认证模式 本地备份

LDAP同步/备份任务下一次执行时间: 2015-12-10 03:00:00

本地服务器端口 * 9812

UAM V5版本实时认证开关见“用户接入管理>业务参数配置>系统配置”菜单。

当在LDAP服务器上新增域账号后，可以等待如下图4“LDAP同步/备份任务”触发时间或点击下图5“按需同步生效”按钮，满足新增账号能立即认证上线的需求。

用户 > 接入策略管理 > LDAP业务管理 > 参数配置

LDAP功能参数

LDAP用户在同步策略间转移 允许

☒ LDAP分页(条) 1000

☒ LDAP同步/备份任务 每1天3点

日志级别 告警

LDAP同步策略查询

同步策略名称

服务器名称

用户分组

同步的用户类型

业务分组

增加

按需同步生效

同步策略名称	服务器名称	同步的用户类型	业务分组	状态	同步优先级	按需同步	LDAP用户
anxu	yrldap	接入用户	未分组	有效	1	是	
测试账号转移1	yrldap	接入用户	未分组	有效	1	否	

2、研发后续版本针对按需同步认证检索机制会进一步优化。