

【前情提要】

公司有很多 IT 系统,例如:企业邮箱,github,jenkins,grafana,zabbix,vpn,HR 系统,用友,金蝶,文件系统,aws,aliyun,cmdb,jira,confluence....等等。

在新员工入职时,要做的事情。

- 要根据员工的职位,确认开通 IT 系统的权限。
- 在对应的 IT 系统中添加账户,设置密码。
- 各种渠道通知到新员工,IT 系统权限和 IT 系统访问地址。

在老员工离职时,上面的事又要做一遍。

在正常工作时,很多员工因各种奇葩原因忘记密码,来找你重置,修改。

在员工升职,调换岗位。又是一通修改和删除。

有木有崩溃?这还不够,一个员工需要手动操作 N 次,每天会有 0-N 个员工,如果出现误操作,导致数据泄露。这口锅直接背起。有木有感觉不会再爱了。

【解决方案】

说了那么多痛点,其实解决方案很简单,有个认证管理中心就可以解决了。那就是

LDAP,LDAP 是什么,干什么用?

LDAP 是 Lightweight Directory Access Protocol 的缩写,中文意思是目录服务的协议,并且以树状结构来存储数据。

主要用来存储企业人员信息和组织架构,进行统一认证管理。

同时可以与第三方应用集成,实现针对企业内部的人员或部门访问权限管理。

【实例讲解】

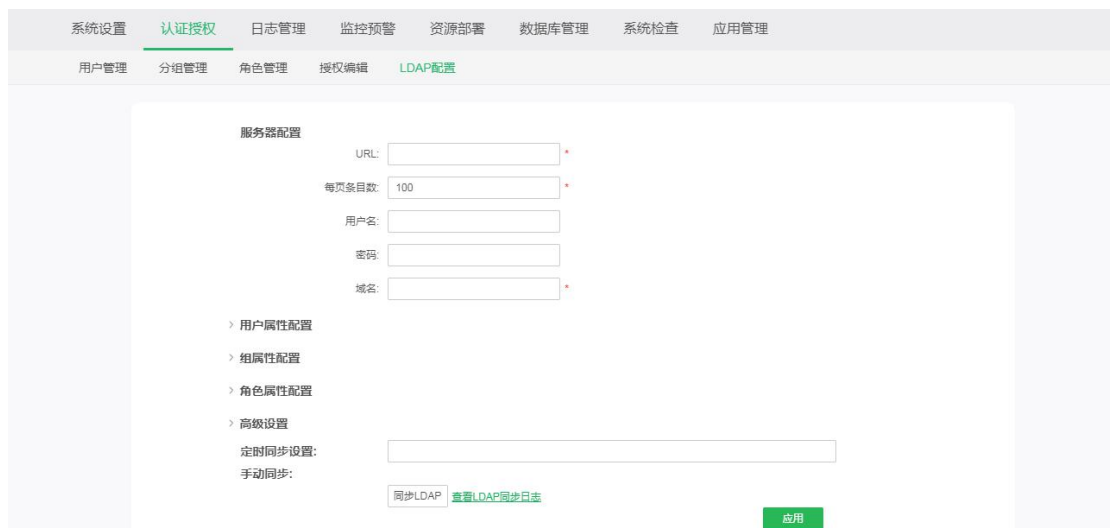
那咱们就来看一下 LDAP 在永洪 BI 中的使用，如何方便快捷进行永洪用户同步，以下实例中的 ldap 连接相关信息，都是以 ldapadmin 连接 ldap 服务器为例。

1. 权限设置

进入 管理系统->系统设置->权限管理系统配置中进行设置。将权限管理系统修改为 LDAP 同步&文件权限管理系统。如下图所示：



当用户选择 LDAP 同步&文件权限管理系统时，可以通过配置 LDAP 服务器与权限系统的对应关系，对接用户的 LDAP 服务器。可通过这一类型将 LDAP 中的用户同步进系统，并赋予资源和操作的权限，如下图所示：



2. LDAP 配置

在 LDAP 配置页面需要配置以下属性，具体介绍如下所示。

2.1 服务器配置

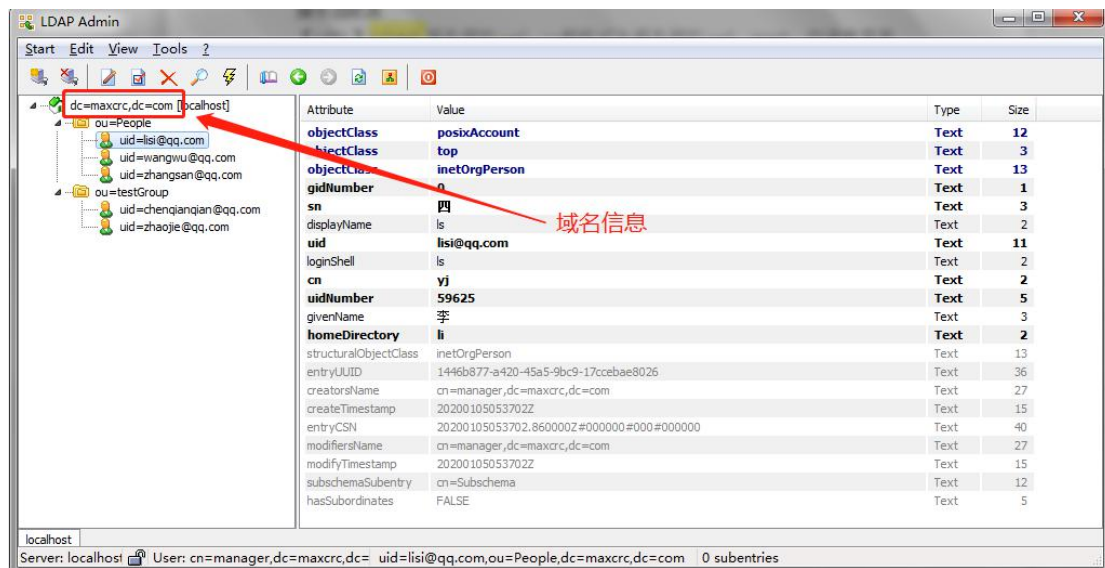
URL: LDAP 服务器的 url，一般格式为服务器的 url: port，但通常需要带上 ldap 协议头，如: ldap://192.168.0.181:389;

每页条目数: 每页可以导入的条目数，这个值是根据 LDAP 的用户总数由用户自行设定的，如设置为 500 或者 1000;

用户名: 登录 LDAP 的用户名称;

密码: 登录 LDAP 的密码;

域名: LDAP 服务器的域名，比如: dc=maxcrc,dc=com。域名可以在连接页面查询，如下图:



服务器配置页面如下所示:

服务器配置

URL:	<input type="text" value="ldap://192.168.0.181:389"/>	*
每页条目数:	<input type="text" value="100"/>	*
用户名:	<input type="text"/>	
密码:	<input type="password"/>	
域名:	<input type="text" value="dc=maxcrc,dc=com"/>	*

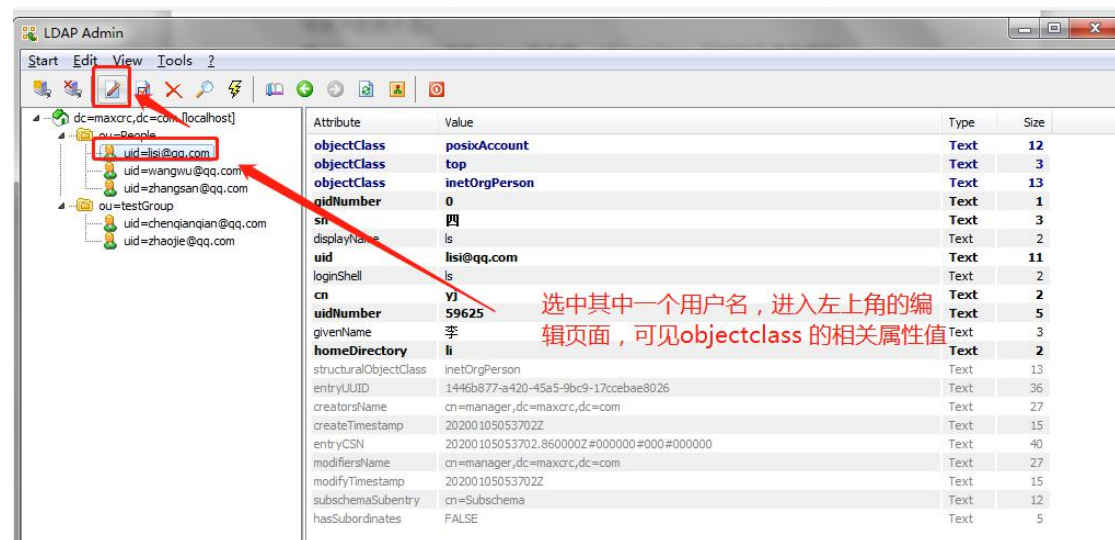
注：若无特定设置用户名以及密码，可不填写该两项。

2.2 用户属性配置

ObjectClass：LDAP 对象类，是 LDAP 内置的数据模型，比如 inetOrgPerson 对象类。每种 objectClass 有自己的数据结构，比如“用户”的 objectClass，会内置很多属性(attributes)，如用户名(name)，密码(password)，电话(mobile)等；所有拥有此对象类的数据将会被当做一个用户条目来解析；

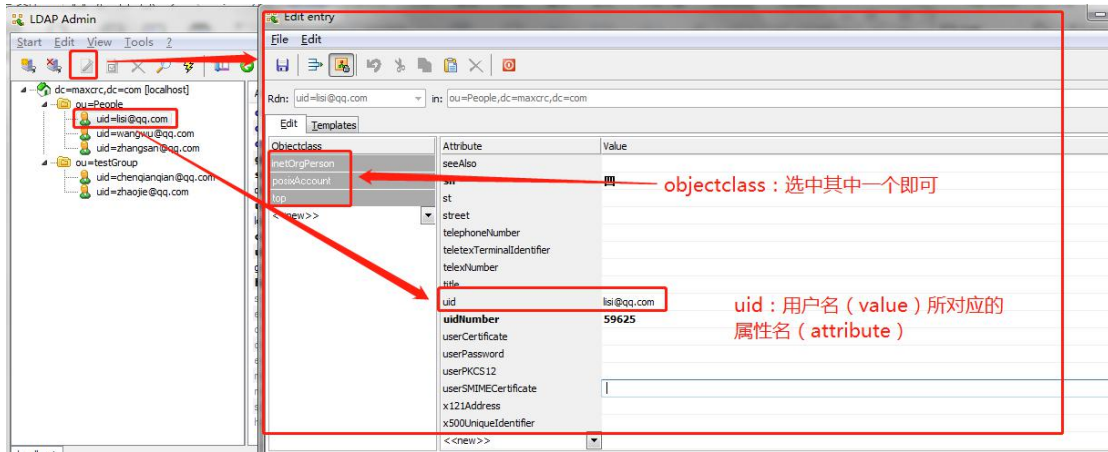
UID：用户的 uid 对应 item 中的 file 的名称的映射。比如：将 LDAP 条目中的“name”属性作为 UID 时，同步进系统后，“name”属性的值将对应系统中用户的用户名；

ObjectClass 以及 UID 可在如下界面看到：

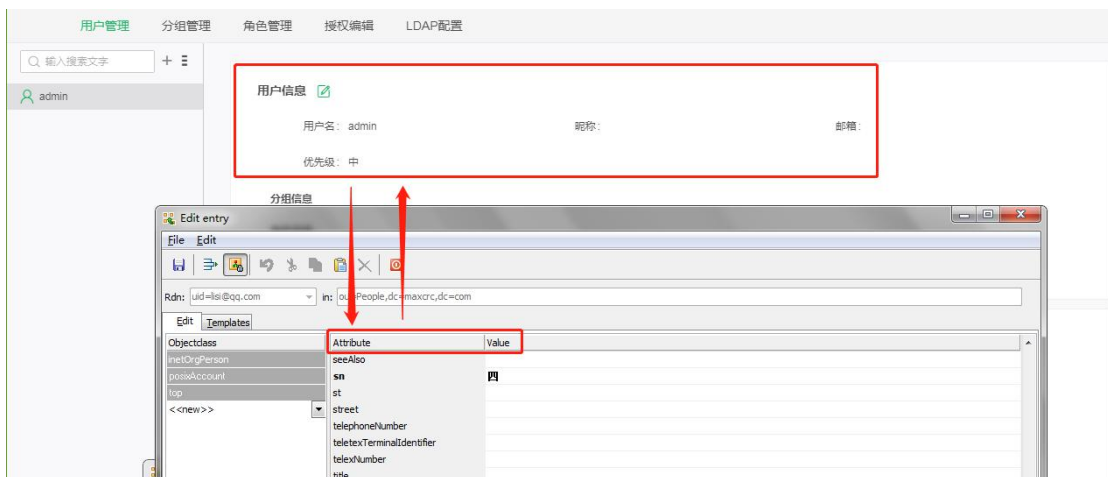


The screenshot shows the LDAP Admin interface. On the left, a tree view shows the directory structure with 'uid=lisi@qq.com' selected. On the right, a table displays the attributes and values for this entry. A red box highlights the 'uid=lisi@qq.com' entry in the tree, and a red arrow points from it to the 'objectClass' attribute in the table. A red text box with an arrow points to the 'objectClass' attribute, stating: '选中其中一个用户名，进入左上角的编辑页面，可见objectclass的相关属性值'.

Attribute	Value	Type	Size
objectClass	posixAccount	Text	12
objectClass	top	Text	3
objectClass	inetOrgPerson	Text	13
gidNumber	0	Text	1
sn	四	Text	3
displayName	ls	Text	2
uid	lisi@qq.com	Text	11
loginShell	ls	Text	2
cn	yl	Text	2
uidNumber	59625	Text	5
givenName	李	Text	3
homeDirectory	li	Text	2
structuralObjectClass	inetOrgPerson	Text	13
entryUUID	1446b877-a420-45a5-9bc9-17cceb8e8026	Text	36
creatorsName	cn=manager,dc=maxcrc,dc=com	Text	27
createTimestamp	20200105053702Z	Text	15
entryCSN	20200105053702.860000Z#000000#000#000000	Text	40
modifiersName	cn=manager,dc=maxcrc,dc=com	Text	27
modifyTimestamp	20200105053702Z	Text	15
subschemaSubentry	cn=Subschema	Text	12
hasSubordinates	FALSE	Text	5



属性配置：系统属性和 LDAP 属性的对应关系，如下图所示。



LDAP 配置中的组属性以及角色属性配置同用户属性配置。

2.3 高级设置

高级设置

自定义转换器:

自定义同步器:

自定义认证器:

自定义转化器：给定制转化器预留的接口；

自定义同步器：给定制同步器预留的接口；

自定义认证器：有 2 种方式，即：`g5.secure.fs.LDAP.impl.LDAPAuthenor` 和 `g5.secure.fs.LDAP.impl.DefAuthenor`。

`g5.secure.fs.LDAP.impl.LDAPAuthenor` 表示同步后，产品将使用 LDAP 服务器的密码进行认证登录；

`g5.secure.fs.LDAP.impl.DefAuthenor` 表示同步后，产品将使用 LDAP 与产品的匹配字段作为密码进行认证登录；

V8.5.1 之前默认为：`g5.secure.fs.LDAP.impl.DefAuthenor`，V8.5.1 之后默认为：`g5.secure.fs.LDAP.impl.LDAPAuthenor`。

注：该配置为特定认证需求预留接口，基本配置中该配置一般不填写。

2.4 定时同步设置

组属性配置

角色属性配置

高级设置

定时同步设置:

00:00
02:00
04:00
06:00
08:00
10:00

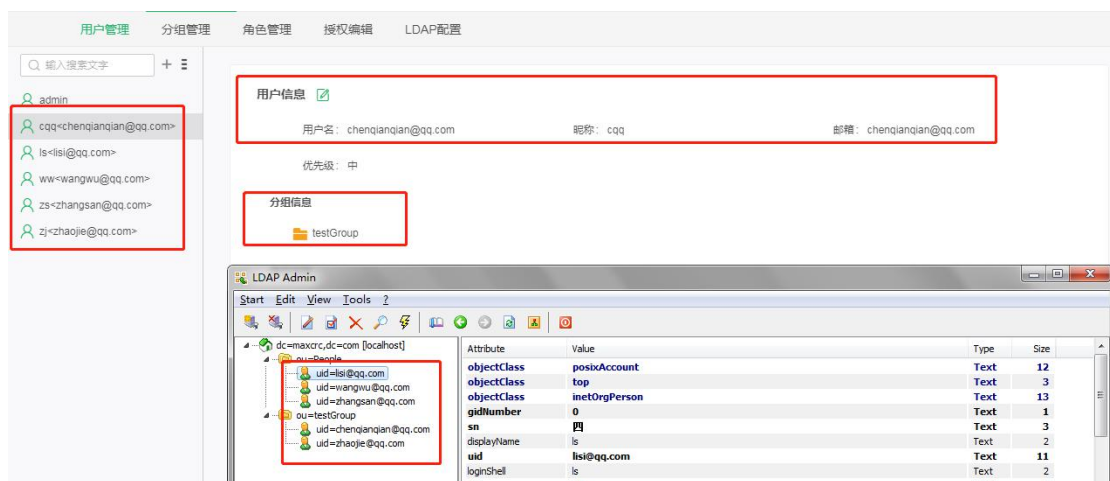
点击定时同步的输入框可在下拉列表中选择定时同步的时间，选择后，每天的这个时间系统都会自动与 LDAP 服务器进行同步。

2.5 手动同步

配置好属性后，手动点击同步 LDAP，系统则会按照配置好的对应关系进行同步。同步时，下方会自动显示 LDAP 同步的日志。

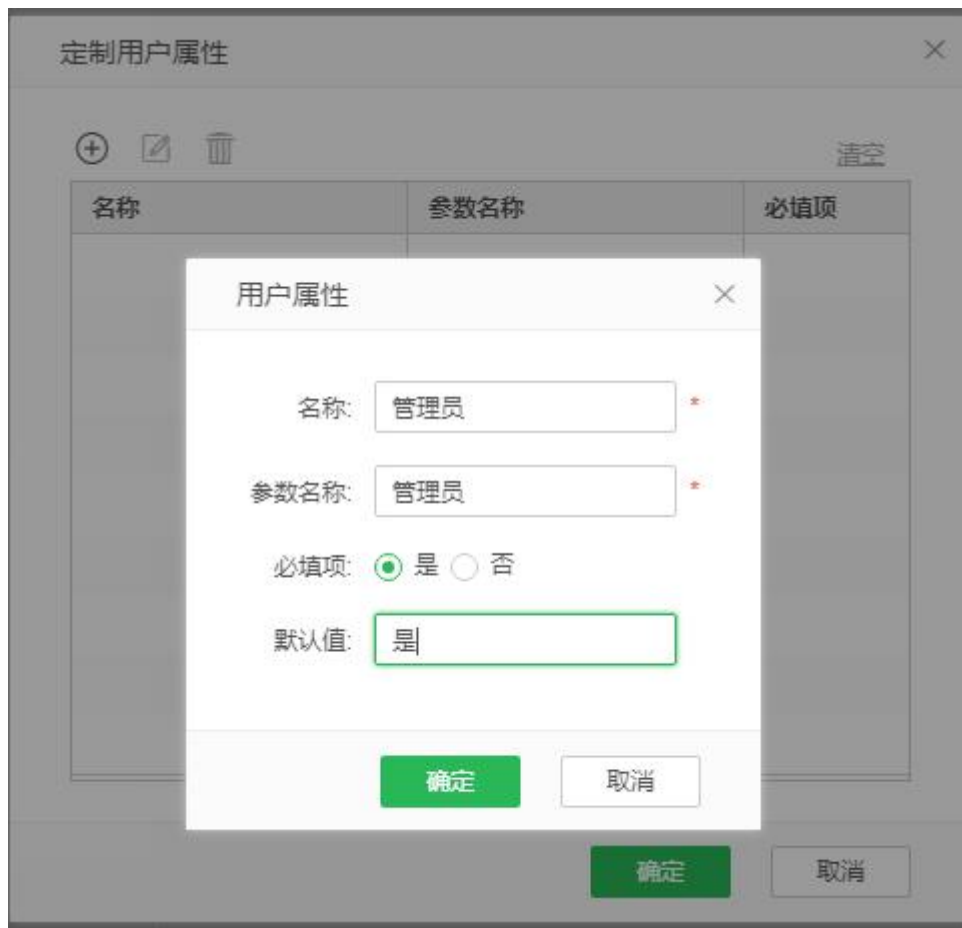
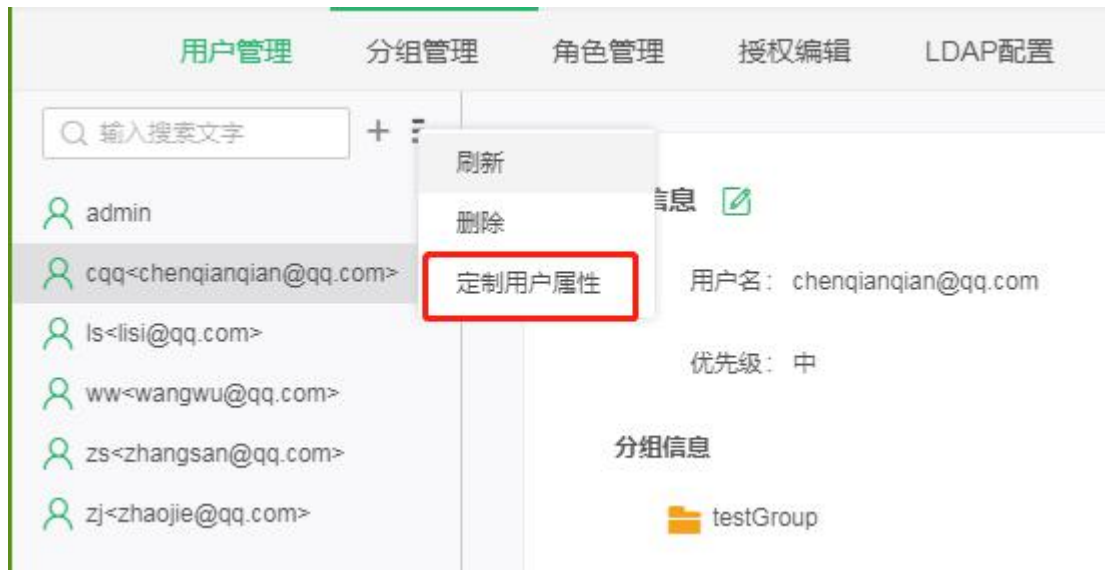


【实例结果】



【定制属性】

若客户需要定制新的属性，比如是否管理员，用户地址等，都可以进行定制，定制方法如下：



注意：在定制用户属性时，新增用户属性的名称与参数名称需保持一致。新增定制属性后，可在 2.2 节属性配置-本地属性中查看。

【特别说明】

- 存量同步

如果 ldap 已经同步过一次，再次进行同步时，称为“存量同步”。通过属性：
`ldap.group.synchronize = true/false` 来决定 ldap 中的用户属性是否覆盖产品中的用户属性，默认值为 `true`。

`ldap.group.synchronize = true` 表示进行存量同步时，如果配置了产品与 ldap 的匹配属性时，ldap 中的该属性值会覆盖产品中对应的属性值。

例如：

- 1) 配置了产品中的“邮箱”和 ldap 中的属性“email”匹配，再进行存量同步时，ldap 中的 email 属性值会覆盖产品中的邮箱配置。
- 2) ldap 中存在用户 user1，为 People 组下成员。首次同步时，将 user1 同步到产品中，其父组为 People。在产品中将 user1 的父组调整为 group1，再进行存量同步，user1 的父组又变为了 People。

`ldap.group.synchronize = false` 表示进行存量同步时，如果配置了产品与 ldap 的匹配属性时，ldap 中的该属性值不会覆盖产品中对应的属性值，即：保留产品中的属性值。

例如：

- 1) 配置了产品中的“邮箱”和 ldap 中的属性“email”匹配，再进行存量同步时，ldap 中的 email 属性值不会覆盖产品中的邮箱配置。
- 2) ldap 中存在用户 user1，为 People 组下成员。首次同步时，将 user1 同步到产品中，其父组为 People。在产品中将 user1 的父组调整为 group1，再进行存量同步，user1 的父组仍然为 group1。

➤ 注意事项

ldap 同步时不会校验邮箱和密码的合法性，即：即使邮箱和密码不填或不合法也可以同步成功。

ldap 用户的名称不可以修改。例如：将 ldap 用户“user1”的名称改为“user2”，点击保存，会提示：LDAP 用户不能修改用户名。



属性 ldap.group.synchronize = true/false 为版本 V9.0 及以后版本新增，V851 之前版本产品逻辑为 ldap.group.synchronize =false 逻辑，V851-V88 版本产品逻辑为 ldap.group.synchronize =true 逻辑，如果是做产品升级，且用户是通过 ldap 同步的，一定要注意了！！

以上为永洪 BI 中使用 ldap 的实例说明，若有其他问题，可在永洪服务平台或者社区进行咨询。