各位朋友大家好！经过几天的纠结，终于能够顺利将AD中用户导入iTop，可以成功创建联系人及LDAP用户账号。现在把期间遇到的问题和解决方法和大家进行一下分享如下，渣排班勿怪。

iTop导入ActiveDirectory用户不完全指南

1. 服务器环境
   1. 操作系统Windows 7，服务器组件及版本请按照iTop要求进行配置（至少HTTPD、PHP、MYSQL）
   2. iTop版本2.0.x
   3. iTop导入AD用户脚本AD\_import\_accounts.php，下载链接：<http://www.combodo.com/documentation/AD_import_accounts.txt>，下载后需该扩展名为php。
2. 必要配置
   1. 请启用PHP的LDAP扩展。默认该选项为关闭，开启方法为将php.ini中“;extension=php\_ldap.dll”中“;”删除，重启HTTPD即可
   2. 任何脚本的修改，保存的时候一定注意，格式一定要是“UTF-8”，否则会产生各种乱码问题。
3. AD\_import\_ccounts.php的配置

iTop官方文档有介绍（需要翻\*墙），链接：<https://wiki.openitop.org/doku.php?id=active_directory_integration>，我还是贴一遍。

* 1. 需要修改的内容
     1. 如果需使用AD服务器认证，请启用iTop的LDAP认证配置,如只是导入用户，则该段无需配置，配置存储于iTop配置文件config-itop.php，位于iTop\conf\production目录。查看$MyModuleSettings数组中的 'authent-ldap'部分，原始文档如下

$MyModuleSettings = array(

'authent-ldap' => array (

'host' => 'your\_ad\_server',

'port' => 389,

'default\_user' => 'default\_login',

'default\_pwd' => 'default\_pwd',

'base\_dn' => 'DC=yourcompany,DC=com',

'user\_query' => '(&(samaccountname=%1$s)(objectCategory=User))',

'options' => array (

17 => 3,

8 => 0,

),

* + - 1. ‘host’为AD服务器，’port’为提供AD服务的端口，这两项配置请咨询你的域管理员
      2. ‘default\_user’和’default\_pwd’是拥有’base\_dn’ OU下所有用户查询权限的用户名及密码（原文为：default\_user and default\_pwd indetify a generic user that has enough rights in the active directory to be able to retrieve the list of users as defined by the user\_query）
      3. ‘base\_dn’是要认证的用户的范围，确保所有用户均在此OU或此OU的子OU下
      4. ‘user\_query’和’options’默认无需配置
    1. AD连接配置，位于脚本的开始位置，原始内容如下：

////////////////////////////////////////////////////////////////////////////////

// Configuration parameters: adjust them to connect to your AD server

// And configure the mapping between AD groups and iTop profiles

$aConfig = array(

// Configuration of the Active Directory connection

'host' => 'localhost', // IP or FQDN of your domain controller

'port' => '389', // LDAP port, 398=LDAP, 636= LDAPS

'dn' => 'DC=combodo,DC=net', // Domain DN

'username' => 'ad\_user', // username with read access

'password' => 'ad\_password', // password for above

// Query to retrieve and filter the users from AD

// Example: retrieve all users from the AD Group \"iTop Users\"

'ldap\_query' => '(&(objectCategory=user)(memberOf=CN=iTop Users,CN=Users,DC=combodo,DC=net))',

// Example 2: retrieves ALL the users from AD

// 'ldap\_query' => '(&(objectCategory=user))', // Retrieve all users

// Which field to use as the iTop login samaccountname or userprincipalname ?

'login' => 'samaccountname',

//'login' => 'userprincipalname',

// Mapping between the AD groups and the iTop profiles

'profiles\_mapping' => array(

//AD Group Name => iTop Profile Name

'Administrators' => 'Administrator',

),

// Since each iTop user must have at least one profile, assign the profile

// Below to users for which there was no match in the above mapping

'default\_profile' => 'Portal user',

'default\_language' => 'EN US', // Default language for creating new users

'default\_organization' => 2, // ID of the default organization for creating new contacts

);

// End of configuration

////////////////////////////////////////////////////////////////////////////////

根据需要，对上述配置进行修改

* + - 1. ‘host’为AD服务器，’port’为提供AD服务的端口，这两项配置请咨询你的域管理员
      2. ‘default\_user’和’default\_pwd’是拥有’base\_dn’ OU下所有用户查询权限的用户名及密码
      3. ‘dn’是要认证的用户的范围，确保所有要导入的账号均在此OU或此OU的子OU下
      4. ‘ldap\_query’和’options’默认无需配置,或参照示例进行修改
      5. ‘login’为从AD中取出的用户属性，AD用户属性有多个均可代表该用户，请选用合适的属性，建议不要修改，使用’samaccountname’即可，可以参考的还有cn、employeeID、mail、name等，具体哪个合适，咨询AD管理员并结合使用需要设置
      6. ‘profile\_mapping’为创建账号时用户所属组对简档映射，可以根据AD中用户所属的不同安全组进行赋权。iTop简档的书写大小写敏感，而且必须和iTop中的名称完全一致
      7. ‘default\_profile’为向新添加的账号的默认简档。当用户所属组不属于’profile\_mapping’映射中的任何一个组时，将按照此项进行简档赋权。如果此项为空，而用户所属组又未正常配置简档映射，将会导致用户创建失败，因为iTop不允许导入的用户没有任何简档。所以为防万一，这一项一定不要为空，并且设置一个有效的简档名称
      8. ‘defaule\_language’为导入账户的默认语言设置，如果要实用简体中文，可以设置为’ZH CN’
      9. ‘default\_organization’为导入账户的默认所属组织，值为组织的id，可以在数据库中进行查询，表名是：organization
    1. 脚本的使用方法
       1. 访问该脚本前，请将文件上传至webservices目录,并进行相关访问控制赋权
       2. 浏览器请访问http://your\_itop\_server/webservices/AD\_import\_accounts.php
       3. 命令模式为：
          1. 切换到脚本所在目录：’cd \Inetpub\wwwroot\itop\webservices’
          2. 使用php执行脚本’php.exe -q AD\_import\_accounts.php --auth\_user=<iTop\_admin\_user> --auth\_pwd=<iTop\_admin\_pwd>’
       4. 默认执行脚本的时候为模拟模式，脚本里的模拟测试开关为开启状态。执行脚本的时候会测试设置参数的执行情况，但是不会像iTop中导入数据
       5. 在正式导入数据时，应该将模拟测试开关关闭
          1. URL加参数’simulation=0’：http://your\_itop\_server/itop/webservices/AD\_import\_accounts.php?simulation=0
          2. 命令行家参数：’--simulation=0’： php.exe -q AD\_import\_accounts.php --auth\_user=<iTop\_admin\_user> --auth\_pwd=<iTop\_admin\_pwd> --simulation=0