Itop 集成 AD 域控和导入帐号

（作者：shandyli）

1、配置

系统环境：CentOS+apache+php+mysql+itop

AD：windows2008

修改配置文件：/web/conf/production/config-itop.php

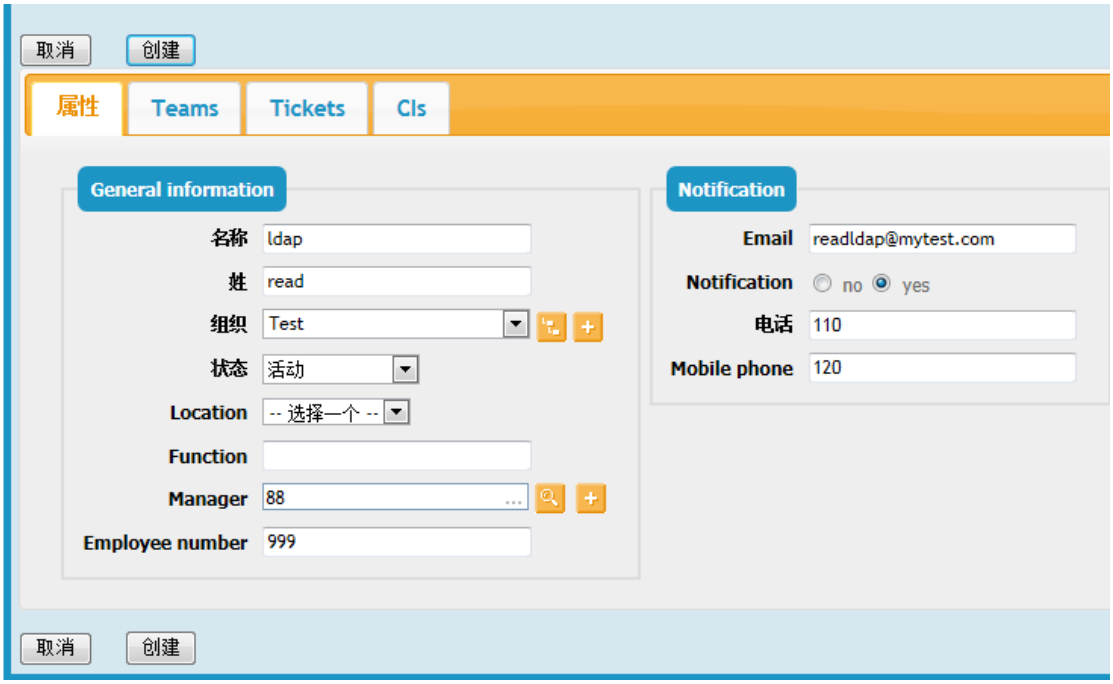
```
167 $MyModuleSettings = array(
168     'authent-ldap' => array (
169         'host' => 'ADIP or 域名',
170         'port' => 389,
171         'default_user' => 'readldap@mytest.com',
172         'default_pwd' => 'test',
173         'base_dn' => 'DC=test,DC=com',
174         'user_query' => '(&(samaccountname=%1$s))',
175         'options' => array (
176             17 => 3,
177             8 => 0,
178         ),
179     ),
```

修改地方是 169~174 行，当然这里要注意 user_query 这行。因为是 windows 的 AD 域控。其他方式本人没尝试成功。如果有大侠知道，欢迎指点。

2、手动建测试帐号

管理员登录 itop

A、配置管理里建联系人



在这里填上你的信息→创建。

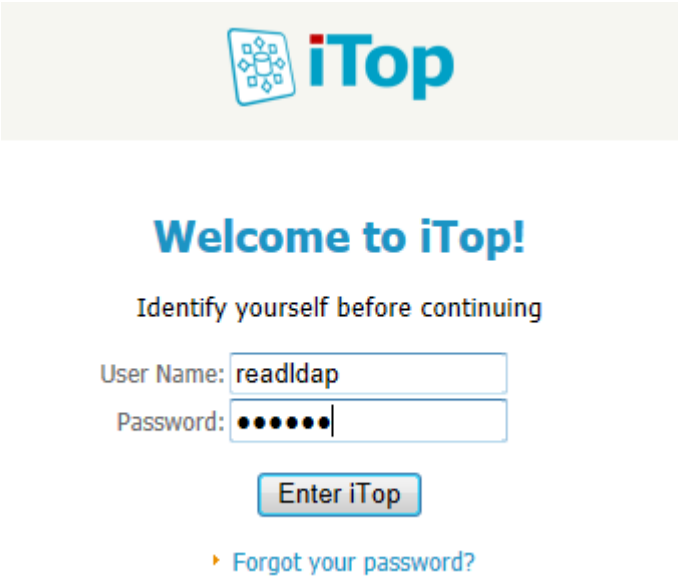
B、管理工具里建用户

这里填上登录名，当然语言这里，选上简体中文（官方原版也可以的）。接着在简档

栏添加简档（个人理解为权限），先添加成 portal user。

→创建。

C、测试登录



→走你。

呵呵→成了！

说明 itop 已经能访问域控，可以通过域控做认证了。接着就是把我们域控里的帐号导入到 itop 里了。

3、批量导入帐号

论坛下载导入脚本 AD_import_accounts.php

修改配置

```
$aConfig = array(
        // Configuration of the Active Directory connection
        'host'  => 'adip or domain', // IP or FQDN of your domain controller
        'port'  => '389', // LDAP port, 398=LDAP, 636= LDAPS
        'dn'        => 'DC=mytest,DC=com', // Domain DN
        'username'  => 'readldap@mytest.com', // username with read access
        'password'  => 'test', // password for above
        'ldap_query' => '(objectCategory=user)',
        'login' => 'samaccountname',
```

```
                // Since each iTop user must have at least one profile, ass
                // Below to users for which there was no match in the above
                'default_profile' => 'Portal user',

                'default_language' => 'ZH CN', // Default language for crea
```

这里和上面的配置文件一样，也是连域控的参数。为了登录进去就是中文界面，缺省语言(default_language)设置成”ZH CN”。当然还可以让导入就是管理员，修改 default_profile 的值即可。

另外为了导入的数据符合平常的习惯，还改了下面的地方。

```
                $oPerson = new Person();
                $oPerson->Set('name', $aData['sn']);
                $oPerson->Set('first_name', $aData['givenname']);
                $oPerson->Set('email', $aData['mail']);
```

把 name 和 first_name 的值调换一下。

```
                $oPerson = new Person();
                $oPerson->Set('name', $aData['givenname']);
                $oPerson->Set('first_name', $aData['sn']);
                $oPerson->Set('email', $aData['mail']);
```

现在通过浏览器来访问，有可能会提示有文件找不到。

继续修改配置文件，把下面的路径对应上自己的就 OK，不详说。

```php
if (file_exists('../approot.inc.php'))
{
    // iTop 1.0.2
    include('../approot.inc.php');
}
else // iTop 1.0 & 1.0.1
{
    define('APPROOT', '../');
}
require_once(APPROOT.'application/application.inc.php');
require_once(APPROOT.'application/webpage.class.inc.php');
require_once(APPROOT.'application/csvpage.class.inc.php');
require_once(APPROOT.'application/clipage.class.inc.php');
require_once(APPROOT.'application/startup.inc.php');

```

接着刷新浏览器，如果配置 ok，会出来登录框

Welcome to iTop!

Identify yourself before continuing

User Name:

Password:

Enter iTop

Forgot your password?

输入 admin 和密码，会出来结果

Simulation mode -- no action will be performed

Set the parameter simulation=0 to trigger the actual execution.

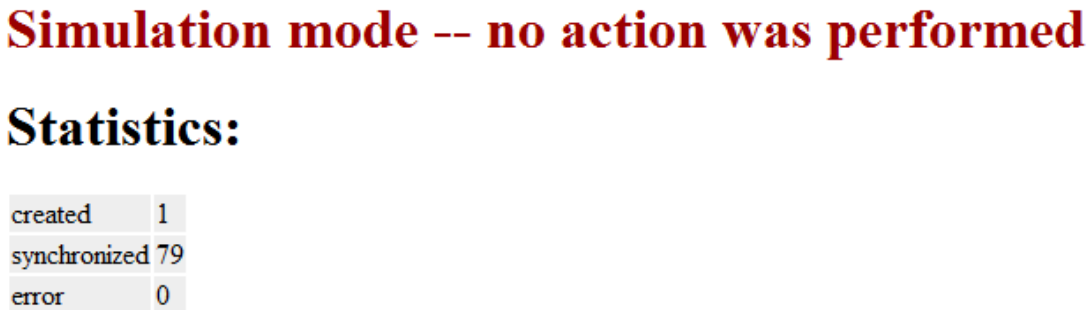
Connected to [redacted] on port 389

Identified as [redacted]

LDAP Query: '(&(objectCategory=user))'

80 user(s) found in Active Directory, 81 (includin

在页面的最后，有一个统计数。



Simulation mode -- no action was performed

Statistics:

created	1
synchronized	79
error	0

现在数据读出来了。但只是模拟更新了，实际并没有更新到我们的 itop 里。为了更新到 itop 里，还需要修改一个地方。

```
421  // By default, run in simulation mode (i.e do nothing)
422  $bSimulationMode = utils::ReadParam('simulation', 0, true);
423  $oMyChange = null;
```

把其中“0”改为“1”。保存刷新，执行完后再进 itop 里看，是不是数据都有了。

赶快拿其中一个导入进去的帐号测试一下吧。

4、后续

第一步导入帐号成功了。但帐号在 itop 里是同一层级的，并没有按 AD 里的分组。如果有实现了一次导入组织结构和帐号的。求共享了。