结合LDAP服务器进行portal认证配置案例

LDAP 杨银波 2015-06-23 发表

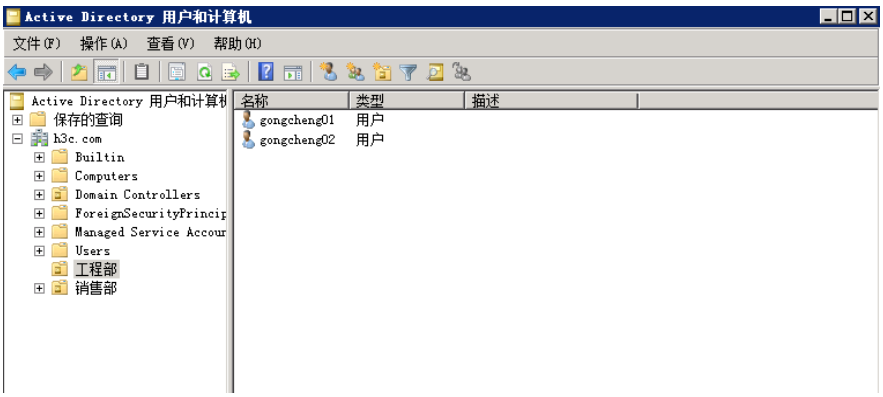
> LDAP服务器是一种以目录树结构存储用户信息的服务器。LDAP服务器中存储的用户称为LDAP用户。
>
> iMC EIA组件可以将iMC中的接入用户和LDAP用户相关联。当接入用户发起认证请求时，iMC确认存在此用户后，根据配置执行本地LDAP用户的验证或将验证工作转交给LDAP服务器。实现此功能后，在相对稳定的网络中引入iMC时，不需要重建用户信息数据库，节省了大量的维护成本。

本案例需求为公司LDAP服务器上已经保存了所有员工信息，工程部的所有员工可以直接在iMC中进行认证，而不需要在iMC中手工创建这些用户。

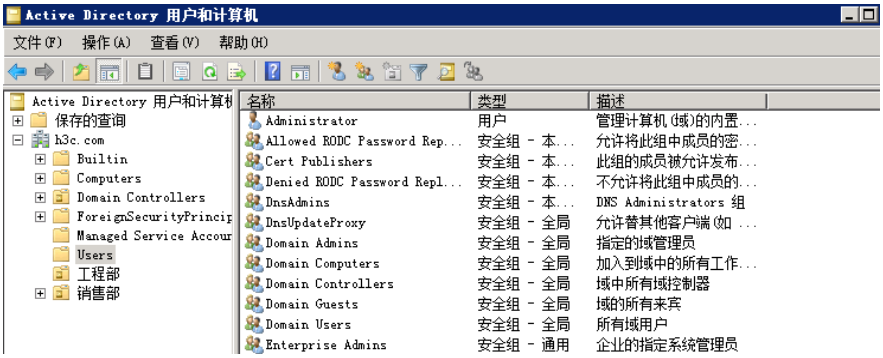
网络中存在LDAP服务器，并使用IMC进行接入认证管理。

查看LDAP服务器

首先登录LDAP服务器，可以看到h3c.com下有一个组织单元"工程部"，其下有两个用户"gongcheng01"和"gongcheng02"。如下图：



并且管理员administrator位于h3c.com下的Users下，如下图：



按照此结构，接下来配置IMC。

配置接入服务

首先登录iMC页面，进入【用户-接入策略管理-接入策略配置】中创建接入策略"policy01"，如下图所示：

然后在【用户-接入策略管理-接入服务】中创建接入服务，引用之前的接入策略。如下图所示：

配置LDAP服务器

首先在iMC中增加LDAP服务器，进入【用户-接入策略管理-LDAP业务管理-服务器配置】点击“增加”，在参数配置中填入LDAP服务器相关信息，如下图所示：

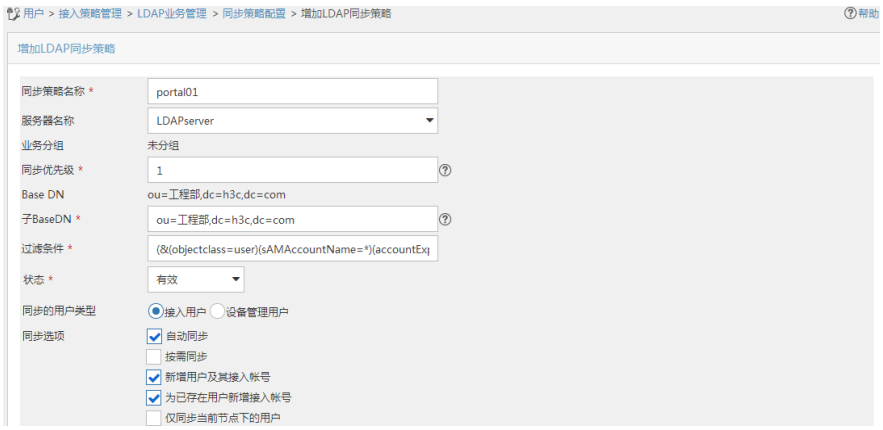
注：基本信息中如实填写服务器IP地址，其他保持默认即可。

Base DN就是iMC同步LDAP账号的路径，只有Base DN中的账号才会被同步到iMC来。

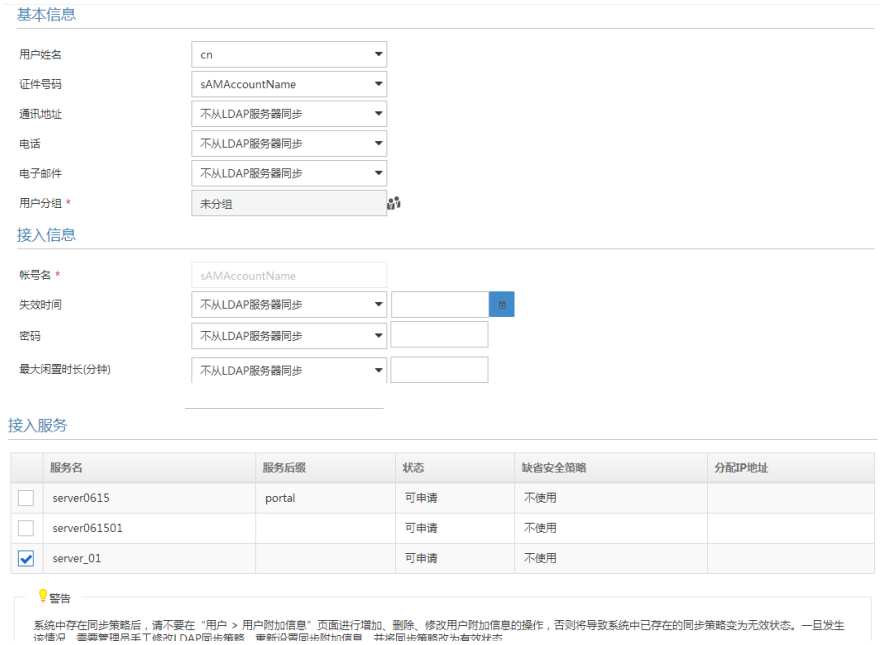
每个参数具体含义可以参考当页联机帮助查询。

配置完成后请点击“检测”来检查一下和LDAP服务器连通是否正常。

接下来配置LDAP同步策略，进入【用户-接入策略管理-LDAP业务管理-同步策略配置】，点击“增加”，填入同步策略参数，如下图所示：

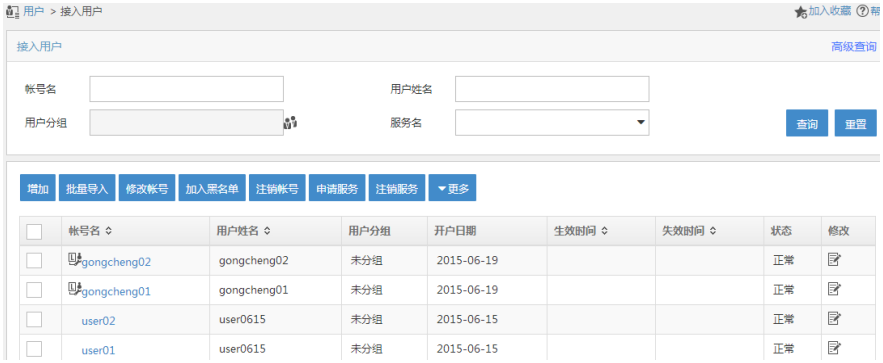


下一步进入账号参数同步配置界面，根据需求填写一下。如下图所示：



注：由于添加LDAP服务器时选择的服务同步方式是“手工指定”，所以这里我们需要手工勾选一下要为用户绑定哪个接入服务，完成后本同步策略同步过来的用户都会绑定这个接入服务。

LDAP自动同步策略会每天凌晨自动执行同步，把LDAP上的用户同步到iMC来，当然也可以手工点击一下策略名中的”同步“来手工触发立即同步。
同步完成后即可看到接入用户列表中已经有了“gongcheng01“和”gongcheng02“这两个用户。
如下图所示：

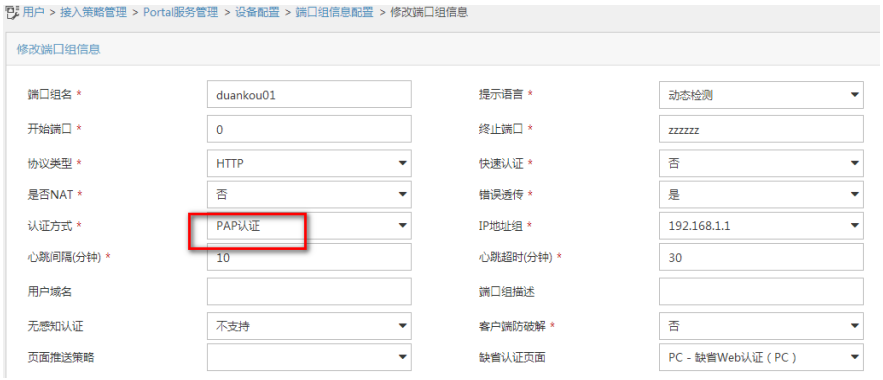


配置portal服务
首先进入【用户-接入策略管理-portal服务管理-IP地址组配置】中增加一个IP地址组，如下图所示：

完成后进入【用户-接入策略管理-portal服务管理-设备配置】中增加portal设备，如下图所示：

注：这里的IP地址要与BAS设备上配置的portal nas ip一致。

完成后点击设备后的"端口组信息管理"，添加一个端口组配置，如下图所示：



注：结合LDAP认证不支持CHAP方式。

配置接入设备

进入【用户-接入策略管理-接入设备管理-接入设备配置】增加一个接入设备，如下图所示：

注：这里的设备IP地址要与BAS设备上radius scheme中配置的nas ip一致（默认为设备上联iMC的接口地址）。

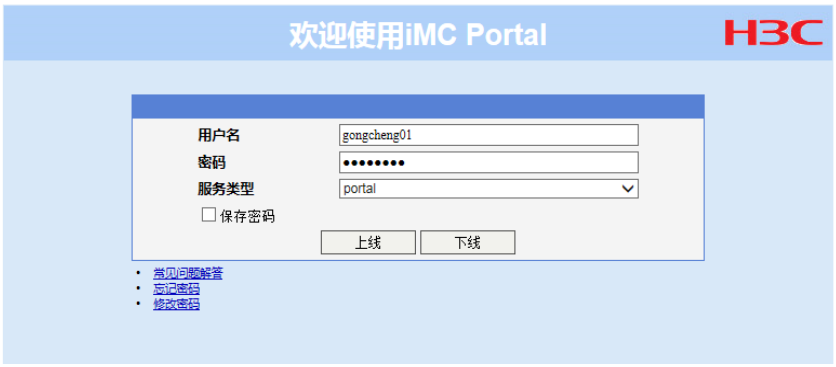
配置BAS设备

```
#
 portal server imc ip 10.1.1.1 key cipher $c$3$e/UXS659cp0VnmQbM0Hsrf/a04Nz9o8= url
http://10.1.1.1:8080/portal
#
radius scheme portal
 server-type extended
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1 1812
 key authentication cipher $c$3$zSYsmhRFj+EgRI0YN5NIuIWnATsPCCU=
 key accounting cipher $c$3$xckwfTBhuM1oBzxdm+zqU2az0aECFqc=
 user-name-format without-domain

domain portal
 authentication portal radius-scheme portal
 authorization portal radius-scheme portal
 accounting portal radius-scheme portal
 access-limit disable
 state active
 self-service-url disable

#
interface Vlan-interface2
 ip address 192.168.1.254 255.255.255.0
```

```
 portal server imc method direct
 portal domain portal
#
```



1. 只有Base DN中的用户才会被同步到iMC中来。
2. iMC会定期每天凌晨去同步LDAP上的用户，所以如果LDAP上新增加了用户，只有到第二天才能同步过来。可以手工点击同步或者配置“按需同步”来适应用户经常变化的场景。
3. 结合LDAP服务器进行portal认证，认证方式不能是CHAP。