

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。

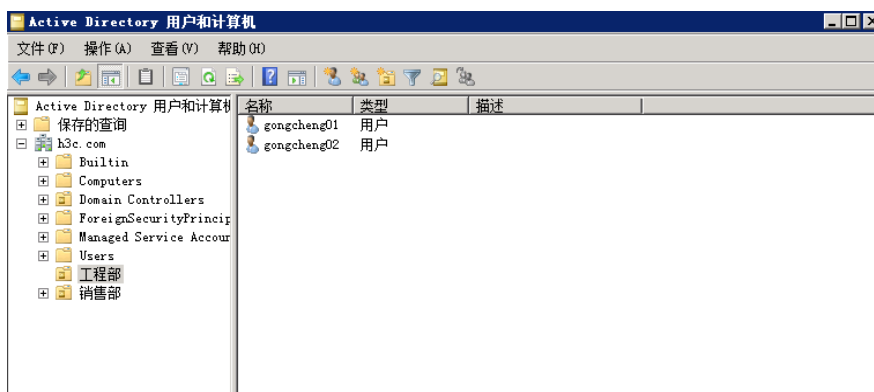
iMC EIA组件可以将iMC中的接入用户和LDAP用户相关联。当接入用户发起认证请求时，iMC确认存在此用户后，根据配置执行本地LDAP用户的验证或将验证工作转交给LDAP服务器。实现此功能后，在相对稳定的网络中引入iMC时，不需要重建用户信息数据库，节省了大量的维护成本。

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。

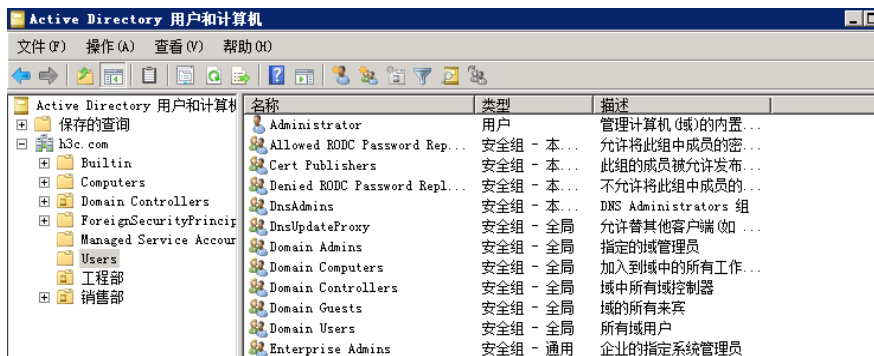
网络中存在LDAP服务器，并使用iMC进行接入认证管理。

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：

用户 > 接入策略管理 > 接入服务管理 > 修改接入服务

基本信息

服务名 *	server_01	服务后缀	
业务分组 *	未分组	缺省接入策略 *	policy01
缺省安全策略 *	不使用	缺省内网外连策略 *	不使用
缺省私有属性下发策略 *	不使用	缺省单帐号在线数量限制 *	0
缺省单帐号最大绑定终端数 *	0		

服务描述

可申请 Portal无感知认证

配置LDAP服务器

首先在iMC中添加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：

用户 > 接入策略管理 > LDAP业务管理 > 服务器配置 > 增加LDAP服务器

LDAP服务器信息

基本信息

服务器名称 *	LDAPserver	服务器版本	3
服务器地址 *	10.1.1.1	端口 *	389
服务器类型	微软活动目录	服务同步方式	手工指定
实时认证	是	连接静默时长 *	1分钟
连接超时时间(秒) *	30	同步超时时间(秒) *	0
用户分组 *	手工指定		
业务分组 *	未分组	<input type="checkbox"/> 启用SSL连接	

服务器信息

Base DN *

管理员DN

管理员密码

用户名属性名称 *

用户密码属性名称

密码策略

帐号名形式 保持原样 去除前缀 去除后缀 增加前缀

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：

用户 > 接入策略管理 > LDAP业务管理 > 同步策略配置 > 增加LDAP同步策略

增加LDAP同步策略

同步策略名称 *	portal01
服务器名称	LDAPserver
业务分组	未分组
同步优先级 *	1
Base DN	ou=工程部,dc=h3c,dc=com
子BaseDN *	ou=工程部,dc=h3c,dc=com
过滤条件 *	(&(objectclass=user)(sAMAccountName=*) accountExi
状态 *	有效
同步的用户类型	<input checked="" type="radio"/> 接入用户 <input type="radio"/> 设备管理用户
同步选项	<input checked="" type="checkbox"/> 自动同步 <input type="checkbox"/> 按需同步 <input checked="" type="checkbox"/> 新增用户及其接入帐号 <input checked="" type="checkbox"/> 为已存在用户新增接入帐号 <input type="checkbox"/> 仅同步当前节点下的用户

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：

基本信息

用户姓名	cn
证件号码	sAMAccountName
通讯地址	不从LDAP服务器同步
电话	不从LDAP服务器同步
电子邮件	不从LDAP服务器同步
用户分组 *	未分组

接入信息

帐号名 *	sAMAccountName
失效时间	不从LDAP服务器同步
密码	不从LDAP服务器同步
最大闲置时长(分钟)	不从LDAP服务器同步

接入服务

服务名	服务后缀	状态	缺省安全策略	分配IP地址
<input type="checkbox"/> server0615	portal	可申请	不使用	
<input type="checkbox"/> server061501		可申请	不使用	
<input checked="" type="checkbox"/> server_01		可申请	不使用	

警告

系统中存在同步策略后，请不要在“用户 > 用户附加信息”页面进行增加、删除、修改用户附加信息的操作，否则将导致系统中已存在的同步策略变为无效状态。一旦发生故障，请重新设置同步策略并重新同步。

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：

用户 > 接入用户 加入收藏 帮助

接入用户 高级查询

帐号名	用户姓名	用户分组	服务名	查询	重置
-----	------	------	-----	----	----

增加 批量导入 修改帐号 加入黑名单 注销帐号 申请服务 注销服务 更多

<input type="checkbox"/>	帐号名	用户姓名	用户分组	开户日期	生效时间	失效时间	状态	修改
<input type="checkbox"/>	gongcheng02	gongcheng02	未分组	2015-06-19			正常	修改
<input type="checkbox"/>	gongcheng01	gongcheng01	未分组	2015-06-19			正常	修改
<input type="checkbox"/>	user02	user0615	未分组	2015-06-15			正常	修改
<input type="checkbox"/>	user01	user0615	未分组	2015-06-15			正常	修改

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：

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 修改IP地址组

修改IP地址组

IP地址组名 *	192.168.1.1
起始地址 *	192.168.1.1
终止地址 *	192.168.1.254
业务分组	未分组
类型 *	普通

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：

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 修改设备信息

修改设备信息

设备信息

设备名 *	dev01	业务分组 *	未分组
版本 *	Portal 2.0	IP地址 *	192.168.1.254
监听端口 *	2000	本地Challenge *	否
认证重发次数 *	0	下线重发次数 *	1
支持逃生心跳 *	否	支持用户心跳 *	否
密钥 *	****	确认密钥 *	****
组网方式 *	直连		

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：

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 端口组信息配置 > 修改端口组信息

修改端口组信息

端口组名 *	duankou01	提示语言 *	动态检测
开始端口 *	0	终止端口 *	zzzzzz
协议类型 *	HTTP	快速认证 *	否
是否NAT *	否	错误透传 *	是
认证方式 *	PAP认证	IP地址组 *	192.168.1.1
心跳间隔(分钟) *	10	心跳超时(分钟) *	30
用户名		端口组描述	
无感知认证	不支持	客户端防破解 *	否
页面推送策略		缺省认证页面	PC - 缺省Web认证 (PC)

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：

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 修改接入设备

接入配置

认证端口 *	1812	计费端口 *	1813
组网方式	不启用混合组网	业务类型	LAN接入业务
接入设备类型	H3C(General)	接入设备分组	无
共享密钥 *	****	确认共享密钥 *	****

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+EgRI0YN5NluWnATsPCCU=
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。