sambaAD+samba+winbind

1. 环境概述：
2. 需要一台linux机子，作为AD域服务器，在其上安装samba-AD所需的包，以及对相关文件进行配置。具体安装配置，请参照以下“samba-AD安装”部分。
3. 需要一台linux机子，作为文件共享服务器，需要加入AD域，并在其上安装samba-classic所需的包，以及对相关文件进行配置。具体安装配置，请参照以下“文件共享服务器安装”部分。
4. 其他普通linux机子，需要加入AD域，在其上安装samba-winbind所需的包，以获取在共享文件服务器上共享的文件。具体安装配置，请参照以下“普通linux加域”部分。
5. Appform、jhsecurity相关文件需要配置。具体配置，请参照以下“配置文件的修改”
6. Windows要挂载用户家目录，需要修改Jhdam中的文件，请参照以下“普通windows加域”
7. samba-AD安装
8. 使用命令rpm -qa|grep samba以及rpm –qa|grep libsmbclient查看系统已经安装的samba相关包，使用yum remove samba\*将samba相关安装包全部卸载。卸载完成后，使用命令rpm –qa|grep samba以及rpm –qa|grep libsmbclient查看应该没有任何相关的安装包。

注：使用yum卸载需要挂载系统盘，若无法挂载系统盘，使用rpm进行全部卸载。 rpm -e --nodeps <包的名字> 逐一进行卸载

1. 使用命令rpm -qa|grep pytalloc查看是否存在安装包，若存在，请进行卸载
2. 关闭图形化管理网络工具并设置开机不启动，执行如下命令：

service NetworkManager stop

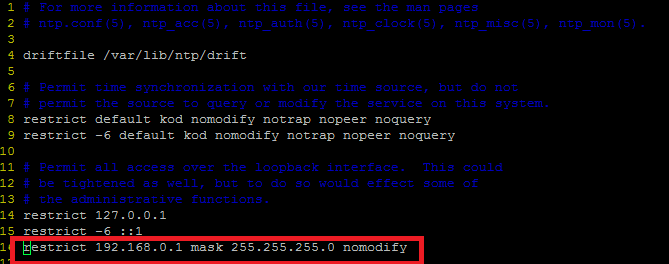
chkconfig NetworkManager off

1. 编辑文件/etc/selinux/config，配置SELINUX=disabled，重启机子
2. 配置ntp服务器:

(1) 在网卡上添加上可以访问外网的dns

(2)vim /etc/ntp.conf添加以下内容到指定行，如图:

restrict 192.168.0.1 mask 255.255.255.0 nomodify (配置192.168.0.1网段的客户端可以同步时间)



其他配置，默认配置

启动时间同步服务，执行命令service ntpd start

1. 将samba4.2.3安装包拷贝到本机，使用命令unzip samba4.2.3.zip进行解压，并进入解压后的samba4.2.3目录。按以下顺序进行安装：

rpm -ivh sernet-samba-common-4.2.3-18.el6.x86\_64.rpm

rpm -ivh sernet-samba-libs-4.2.3-18.el6.x86\_64.rpm

rpm -ivh sernet-samba-libsmbclient0-4.2.3-18.el6.x86\_64.rpm

rpm -ivh sernet-samba-libsmbclient-devel-4.2.3-18.el6.x86\_64.rpm

rpm -ivh sernet-samba-libwbclient-devel-4.2.3-18.el6.x86\_64.rpm

rpm -ivh sernet-samba-client-4.2.3-18.el6.x86\_64.rpm

rpm -ivh sernet-samba-ctdb-4.2.3-18.el6.x86\_64.rpm

rpm -ivh sernet-samba-ctdb-tests-4.2.3-18.el6.x86\_64.rpm

rpm -ivh sernet-samba-winbind-4.2.3-18.el6.x86\_64.rpm

rpm -ivh sernet-samba-4.2.3-18.el6.x86\_64.rpm

rpm -ivh sernet-samba-ad-4.2.3-18.el6.x86\_64.rpm

1. 配置AD域：
2. 编辑/etc/hosts添加本机IP与hostname映射，如下：

192.168.56.10 adserver.domain.com adserver

其中IP为本机IP，adserver为本机hostname，domain.com为准备启用的域名

1. 编辑网卡配置文件/etc/sysconfig/network-scripts/ifcfg-eth0，添加DNS为本机地址，如：DNS1 =192.168.56.10，其中192.168.56.10为本机IP
2. 配置AD域，执行如下命令：

samba-tool domain provision --use-rfc2307 --realm=domain.com --domain=domain --adminpass=JHadmin123456 --server-role=dc --dns-backend=SAMBA\_INTERNAL

**samba-tool domain provision --use-rfc2307 --realm=racher.com --domain=racher --adminpass=ZR123.com --server-role=dc --dns-backend=SAMBA\_INTERNAL**

其中--realm后配置的是将要启用的域名，--domain后配置的是短域名，--adminpass后配置的是admin的密码，密码要求有大小写字母、数字，这儿配置的域名、密码在随后的加域过程中会用到。

1. 执行以下几个命令，修改AD密码策略：

samba-tool domain passwordsettings set --complexity=off

samba-tool domain passwordsettings set --history-length=0

samba-tool domain passwordsettings set --min-pwd-age=0

samba-tool domain passwordsettings set --max-pwd-age=0

1. 更改samba的启动模式，编辑配置文件/etc/default/sernet-samba，修改SAMBA\_START\_MODE="ad"
2. 启动samba-ad，执行命令service sernet-samba-ad start
3. 使用smbpasswd –a命令可以添加AD用户，使用pdbedit –L命令可以查看命令
4. 文件共享服务器安装
5. 安装samba
6. 将samba4.2.3安装包拷贝到本机，使用命令unzip samba4.2.3.zip进行解压，并进入解压后的samba4.2.3目录。按以下顺序进行安装：

rpm -ivh sernet-samba-common-4.2.3-18.el6.x86\_64.rpm;

rpm -ivh sernet-samba-libs-4.2.3-18.el6.x86\_64.rpm;

rpm -ivh sernet-samba-libsmbclient0-4.2.3-18.el6.x86\_64.rpm;

rpm -ivh sernet-samba-libsmbclient-devel-4.2.3-18.el6.x86\_64.rpm;

rpm -ivh sernet-samba-client-4.2.3-18.el6.x86\_64.rpm;

rpm -ivh sernet-samba-winbind-4.2.3-18.el6.x86\_64.rpm;

rpm -ivh sernet-samba-4.2.3-18.el6.x86\_64.rpm

1. 修改DNS
2. 编辑网卡配置文件/etc/sysconfig/network-scripts/ifcfg-eth0，添加DNS为AD域服务器地址，如：DNS1=192.168.56.10，其中192.168.56.10是AD域服务器IP。
3. 编辑/etc/sysconfig/network更改主机名:

更改为长主机名，主机名加域名：例如域：domian.com,更改后的主机名host.domian.com.

1. 执行service network restart，重启网络。
2. 以上操作完成后，在命令行执行ping domain.com应该可以ping通，其中domain.com是AD域的域名。如果ping不通，请检查防火墙以及DNS的配置。
3. 禁用SELinux, 编辑文件/etc/selinux/config，设置

SELINUX=disabled

然后重启机器。

1. 关闭防火墙

chkconfig iptables off

service iptables stop

1. 时间同步
2. 执行crontab -e，加入如下内容，实现每小时与AD服务器同步一次时间

00 \* \* \* \* root /usr/sbin/ntpdate IP;/usr/sbin/hwclock –w (ip为ntp服务器的ip地址)

1. crond服务加入开机启动，并立即重启crond服务

chkconfig crond on

service crond restart

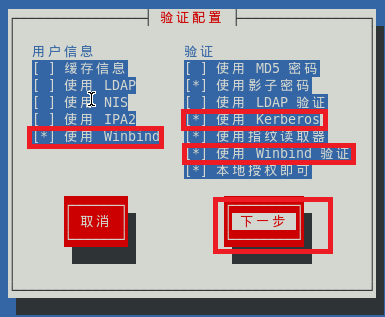
1. 在命令行执行/usr/sbin/ntpdate ip;/usr/sbin/hwclock –w (ip为ntp服务器的ip地址)
2. 加域

cd /etc/init.d

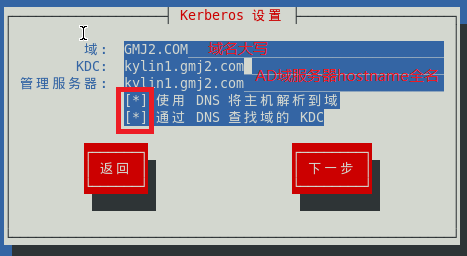
cp sernet-samba-winbindd winbind

service winbind restart

（1）在命令行执行authconfig-tui，出现下图，在图中选择“use winbind”“use kerberos”“use winbind authertication”三项



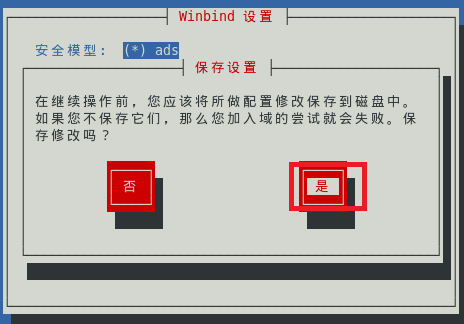
点击“下一步”



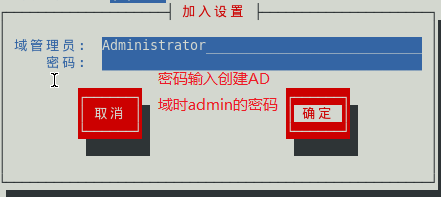
点击“下一步”，注意图中的域名、AD域服务器名与本文中的域名domain.com、AD域服务器名adserver.domain.com不同，请根据个人环境更改域名、AD域服务器名



点击“加入域”



点击“是”



点击“确定”



点击“确定”，退出setup

[/usr/bin/net join -w RACHER -S zhou.racher.com -U Administrator]

Enter Administrator's password:<...>

Using short domain name -- RACHER

Joined 'PBS' to dns domain 'racher.com'

No DNS domain configured for pbs. Unable to perform DNS Update.

DNS update failed: NT\_STATUS\_INVALID\_PARAMETER

Starting SAMBA winbindd : [确定]

正在启动 oddjobd： [确定]

1. 更改samba的启动模式，编辑配置文件/etc/default/sernet-samba，修改SAMBA\_START\_MODE="classic"
2. 编辑/etc/samba/smb.conf，修改如下一行，可以实现登录时不需要输入域名

winbind use default domain = true

1. 启动相关服务并设置开机自启动，执行如下命令：

service sernet-samba-winbindd start

Chkconfig sernet-samba-winbindd on

1. 测试加域是否成功

（1）# wbinfo –t ##测试RPC通讯，提示succeeded表示成功  
cheTEST the trust secret for domain DOMAIN via RPC calls succeeded

（2）# wbinfo -u ##查看域用户  
DOMAIN\guest  
DOMAIN\administrator  
DOMAIN\krbtgt  
DOMAIN\barlowliu  
……以下省略……

##如果如上，则读取正常

（3）# wbinfo -g ##查看域组  
DOMAIN\domain computers  
DOMAIN\cert publishers  
DOMAIN\domain users  
DOMAIN\domain guests  
DOMAIN\ras and ias servers  
DOMAIN\domain admins  
DOMAIN\schema admins  
DOMAIN\enterprise admins  
……以下省略……

上述两个命令执行后如果可以看到域中的用户和组则正常。如果提示如下，则表示与域控制器同步还未完成。

（4）测试ntlm组件

# ntlm\_auth --username=administrator  
password: ##输入用户密码  
NT\_STATUS\_OK: Success (0x0)   
（5）验证代域  
# net ads testjoin  
Join is OK

1. 创建共享目录，即用户家目录
2. 创建用户家目录，在此以/apps为例，具体目录可以自己规定，注意/etc/samba/smb.conf配置文件也要相应的改变，并要把家目录设为共享目录，共享目录设置请参考nfs文件共享

mkdir /apps

chmod 777 /apps

1. 编辑文件/etc/samba/smb.conf，在[global]添加如下几行：

template homedir = /apps/%D/%U

follow symlinks = yes

wide links = yes

unix extensions = no

在[homes]下添加如下几行：

[homes]

comment = Home Directories

read only = no

writeable = yes

1. 编辑/etc/pam.d/system-auth以及/etc/pam.d/sshd，两个文件中都加入如下一行：

session required pam\_mkhomedir.so skel=/etc/skel umask=0077

1. 启动相关服务，执行如下三个命令

service sernet-samba-smbd start

service sernet-samba-nmbd start

**service sernet-samba-winbindd restart**

1. 测试家目录是否可以成功创建，在命令行su成AD域用户jhadmin，在家目录/apps/domain下查看是否创建用户的家目录（与jhadmin同名的目录），如果成功创建，则相关配置正确。
2. 普通linux加域
3. 参照“文件共享服务器安装”部分的1、2、3、4、5，进行安装samba、加域、测试加域是否成功
4. 将“文件夹共享服务器安装”部分配置的用户家目录/apps/domain挂载到本地相同目录下，具体方法参考nfs的使用

五．配置文件的修改

1. jhappform可以安装在任何一台机子上，按照“景行应用门户软件-用户手册”成功安装jhappform并进行配置

2. 安装配置完成后还需要进行文件配置

（1）编辑文件jhappform/conf/jhsecurity.conf，具体配置如下：

设置AD：ldap\_url=ldaps://192.168.56.10:636

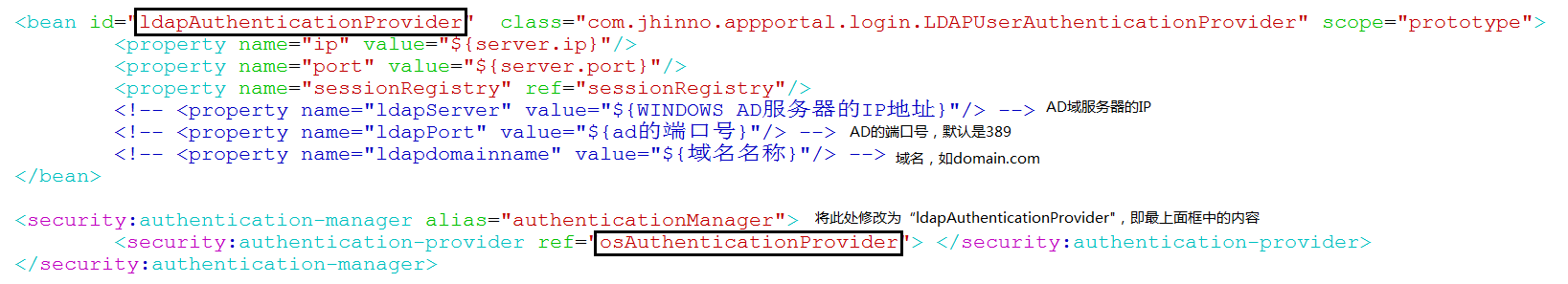
ldap\_userDn=CN=Administrator,CN=Users,DC=domain,DC=com

ldap\_password=#使用jhencry加密后的AD域admin密码#

ldap\_base=DC=domain,DC=com

其中domain、com是AD域的域名domain.com

(2)编辑文件jhappform/tomcat/jhinno/appform/WEB-INF/security.xml，如下图，去掉图中的注释，按黑字提示进行配置。如果使用openldap验证，该文件在此不需要配置，请参考“openldap安装手册”中对该文件的配置。



1. 导入证书

此处导入的是AD域证书，如果使用openldap验证，不需要做此处的操作，请参考“openldap安装手册”中的导入证书部分。

（1）在AD域服务器的/var/lib/samba/private/tls有默认的证书cert.pem

使用命令openssl pkcs12 -export -out jhinno.p12 -in cert.pem -inkey key.pem -name jhinno 导出一个pkcs12格式的证书，输入密码，如changeit

使用openssl pkcs12 -in jhinno.p12 -out test.cer导出证书test.cer，输入密码changeit

（2）将证书test.cer拷贝到安装jhappform的机子，进入目录jhappform/jre/lib/security

执行命令keytool -importcert -keystore cacerts -file test.cer -alias test，输入密码changeit，询问是否信任此证书，输入y。注意这里的test.cer要指定该文件的路径

（3）如果要删除证书，可使用命令keytool -delete -keystore cacerts -alias test

4. 配置完成后，启动jhappform

六．普通windows加域

1. 设置DNS为192.168.56.10（AD域服务器IP），加入AD域，加域时输入的用户名是administrator，密码是创建AD域时admin的密码，加域方式与以前一样

2. 在jhdam\bin\mountspooler.bat加入如下行：

net use H: \\192.168.56.11\%USERNAME%

其中192.168.56.11为samba文件共享服务器IP

七．解决uid不同问题

将以下内容拷贝到所有机子（安装ad服务器、文件共享服务器以及所有加域的linux机子）的/etc/samba/smb.conf的[global]中

idmap uid = 20000-29999

idmap gid = 20000-29999

idmap config domain:backend = rid

idmap config domain:range = 20000000-29999999 注意:domain(为短域名大写)

winbind enum users = yes

winbind enum groups = yes

winbind separator = +

server services = +smb -s3fs

dcerpc endpoint servers = +winreg +srvsvc