安盟多因素身份认证系统
PAM6.0 认证代理客户端
应用 Linux 平台
管理员手册

安盟电子信息安全有限责任公司

2016 年 09 月

版本管理

版本	摘要	编者	日期
3.01	重新编写清理结点操作	陈俊	2020/09/02
3.02	增加例外组配置说明，增加清理节点密文概念	陈俊	2020/09/07

适用范围

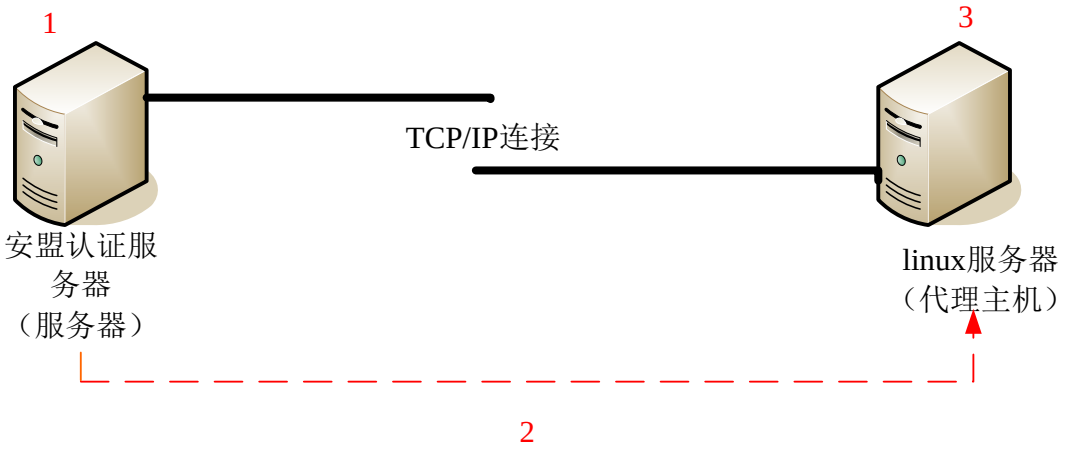
构建的安盟身双因素身份认证系统中，服务器为 Windows 操作系统，客户端为 Linux 操作系统。

适合人群

网络安全管理员

目　　录

安装的基本思路

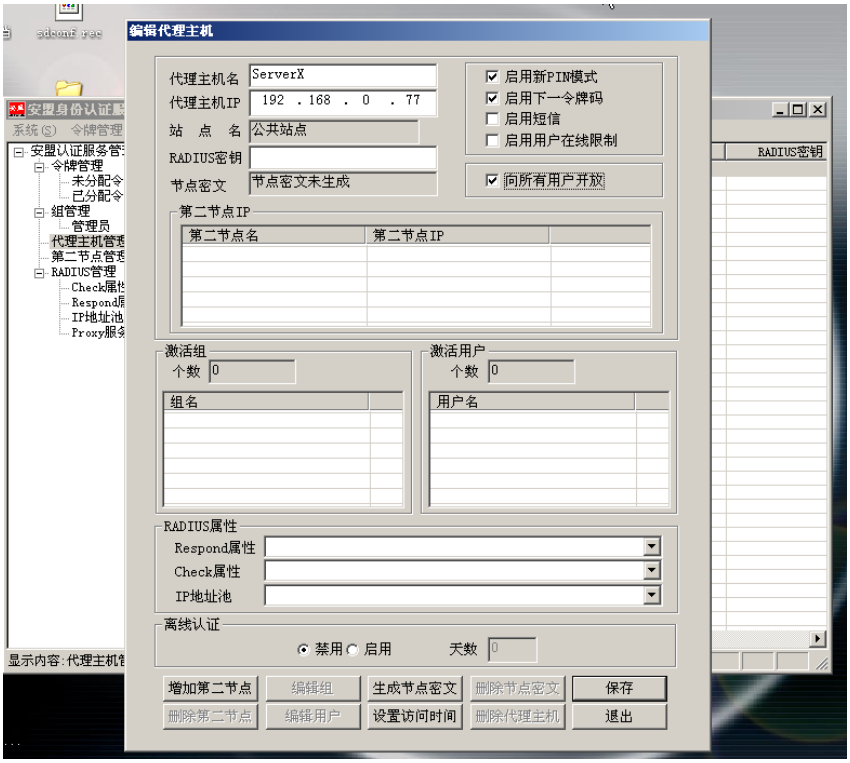


1， 在服务器端生成代理主机的配置文件 sdconf.rec 文件；
2， 从服务器端将文件复制到代理主机上；
3， 存放 sdconf.rec 文件，安装客户端软件；
4， 测试客户端；
5， 登录测试。

1 PAM 安装

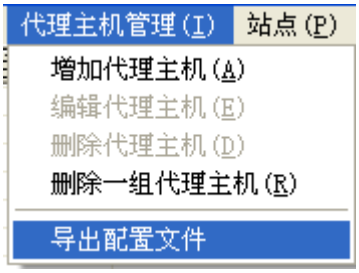
1.1 安装软件前准备

添加受保护的目标机器为代理主机。以安盟认证服务器 7.0 版本为例，在认证服务器端的 hosts 文件里，添加代理主机的 IP 地址和计算机名称。



1.2 生成代理主机配置文件

在服务器端生成代理主机文件，在安盟认证服务管理器→代理主机管理→导出配置文件。



单击“导出配置文件”得到 sdconf.rec 配置文件。

1.3 上传配置文件和 Agent60pam.tar 程序

在代理主机上备份以下文件

/etc/pam.d/sshd

/etc/ssh/sshd_config

然后在目录/var 下建立 ace 目录，将生成的配置文件 sdconf.rec 放置其中。

在根目录下建立一个文件夹 Agent60pam，将 Agent60pam.tar 程序解压到其中

[root@anhost~]mkdir Agent60pam

[root@anhost~]cd Agent60pam

[root@anhost Agent60pam] tar –vxf Agent60pam.tar

1.4 安装客户端

然后进入到 Agent60pam

```
[root@anhost ~]# cd Agent60pam
[root@anhost Agent60pam]# ls
aix          hp11           license2.txt   license.txt~  solsparc
AMLog.txt    hpitan         license2.txt~  lnx32         solx86
AMLog.txt~   install_pam.sh  license.txt    lnx64         uninstall_pam.sh
[root@anhost Agent60pam]#
```

键入./install_pam.sh 回车。

```
[root@anhost Agent60pam]# ./install_pam.sh

ARE YOU A CUSTOMER ORDERING THIS AM PRODUCT FROM AM SECURITY INC., FROM EITHER NORTH AM
ERICA, SOUTH AMERICA OR THE PEOPLE'S REPUBLIC OF CHINA (EXCLUDING HONG KONG): (y/n) [y]
```

键入“y”回车继续。

```
LICENSE AGREEMENT

***    IMPORTANT    ***
PLEASE READ CAREFULLY BEFORE CONTINUING WITH THIS INSTALLATION.  AT THE END OF THE LICE
NSE TERMS AND CONDITIONS STATED BELOW, CUSTOMER WILL BE ASKED TO ACCEPT OR REJECT SUCH
TERMS.  BY INDICATING ITS ACCEPTANCE, CUSTOMER AGREES TO BE BOUND BY THE TERMS OF THIS
LICENSE AGREEMENT.

This is a legal agreement ("the Agreement") between the end user ("Customer") and AM Se
curity Inc. ( "AM"). This Agreement may be superseded by any written agreement signed b
y both Customer and AM.  This Agreement is part of a package (the "Package") that also
includes a sealed CD-ROM disk or sealed diskettes (collectively, the "Disk") and certai
n Documentation.

1.       DEFINITIONS:

"Documentation" means all user documentation whether in hard copy or soft copy form inc
luding manuals, handbooks, and other written materials relating to the AM Products prov
ided by AM.

"Licensed Product(s)" means one or more of the Customer's products or product groups id
entified in a separately prepared "License/Product Schedule" that has been or will be d
--More--(5%)
```

按空格键翻页，直到出现

```
Do you accept the License Terms and Conditions stated above? (Accept/Decline) [D]a
```

键入“A”回车继续。

```
Enter Directory where sdconf.rec is located [/var/ace]
```

按回车键，这个就是先前在/var/ace 目录下导入的 sdconf.rec 文件。

```
Please enter the root path for the AM Authentication Agent for PAM directory [/opt]
```

按回车键，这个是指定安盟身份认证的安装路径，默认在/opt 下

```
PAM Agent is already installed in the /opt/pam

Would you like to overwrite it? (y/n) [y]
```

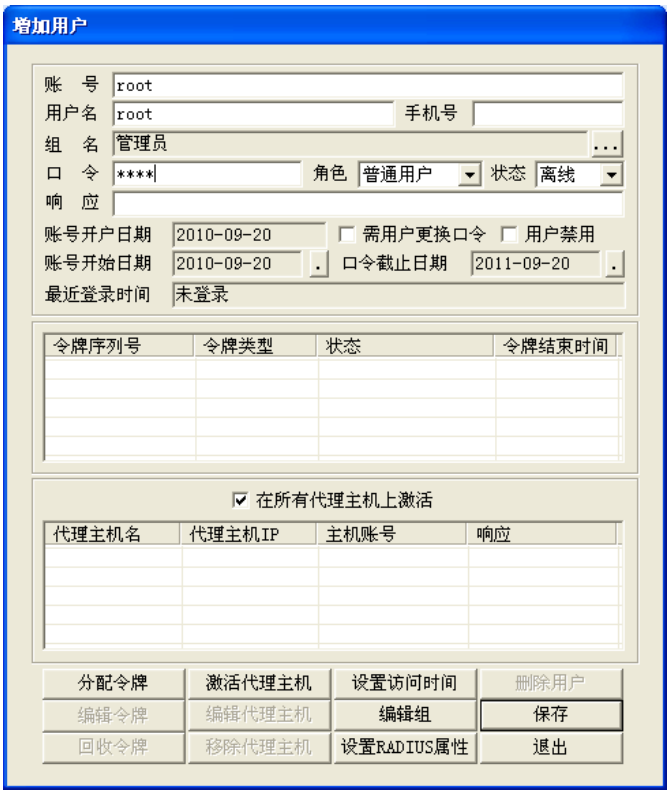
按回车键，直接安装

```
Checking /etc/sd_pam.conf:

VAR_ACE exists - entry will not be updated
ENABLE_GROUP_SUPPORT exists - entry will not be updated
INCL_EXCL_GROUPS exists - entry will not be updated
LIST_OF_GROUPS exists - entry will not be updated
PAM_IGNORE_SUPPORT exists - entry will not be updated
AUTH_CHALLENGE_USERNAME_STR exists - entry will not be updated
AUTH_CHALLENGE_RESERVE_REQUEST_STR exists - entry will not be updated
AUTH_CHALLENGE_PASSCODE_STR exists - entry will not be updated
AUTH_CHALLENGE_PASSWORD_STR exists - entry will not be updated

*****************************************************************
* You have successfully installed AM Authentication Agent 6.0 for PAM
*****************************************************************
```

安盟身份认证软件安装成功！

1.5 添加用户账户

在安盟认证服务器上，添加用户账户，并在这个代理主机上，并在代理主机上激活



同时，在代理主机上同样添加相同用户账户，并设置密码。

#passwd root

Changing password for user root

New UNIX password:

Retype new UNIX password:

Passwd: all authentication tokens updated successfully

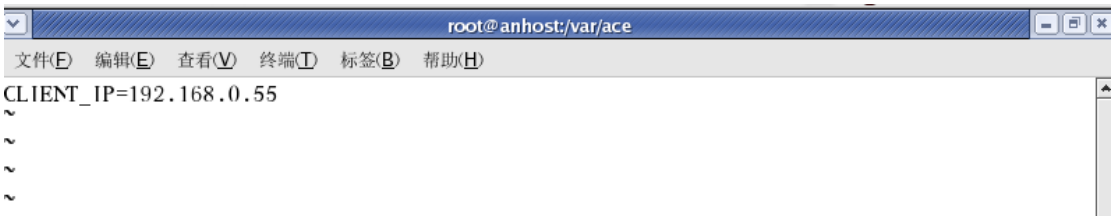
```
[root@anhost ~]# passwd root
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

1.6 配置客户端

在/var/ace 目录下创建一个 sdopts.rec 文件

键入 CLIENT_IP=代理主机的 IP 地址

注意：要大写并且主机名称和 IP，要和安盟认证服务器上添加的信息相同。



保存退出。

1.7 测试客户端

测试客户端，回到根目录下，进入到/opt/pam/bin 目录中。

键入 ./acetest

```
Enter USERNAME: root
Enter PASSCODE:
You must select a new PIN.
Do you want the system to generate
your new PIN? (y/n) [n]
Enter a new PIN between 4 and 8 digits:
Re-enter new PIN to confirm:
New PIN accepted.
Enter USERNAME: root
Enter PASSCODE:
Authentication successful.
```

身份认证通过，证明客户端认证成功。这个里边 root 用户是首次使用身份认证，所以要创建 PIN 码。

2 配置

2.1 登录启用身份认证设置

SSH 登录代理主机是日常操作，启用安盟认证主要是对 SSH 登录更换指向认证模块。客户端在登录时，不在“走向”本地认证，而是先转入到安盟认证，然后在回归到本地其它策略。

2.1.1 Readhat 5.X+

回到根目录下，进到文件目录/etc/pam.d 中，编辑文件 sshd

注释掉原有的 Auth 验证

#auth required pam_stack.so service=system_auth

#auth required pam_nologin.so

增加 PAM 模式验证

auth required pam_securid.so reserve

保存退出。

注意：部分 PAM 经上述设置无效时，可参考使用下述配置：

auth required pam_securid.so service=system-auth

2.1.2 CentOS7.X

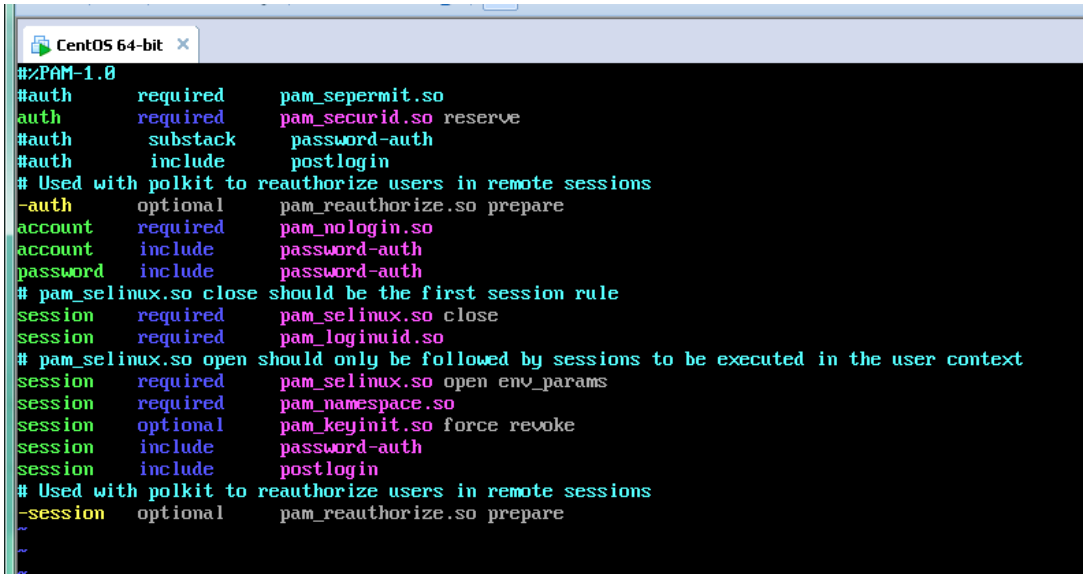
编辑

#vi /etc/pam.d/sshd

注销所有 auth 开头的参数列表

添加

auth required pam_sercurid.so reserve



注意：为了能正常认证关闭系统自带的 SElinux

打开 selinux 配置文件

vim /etc/selinux/config

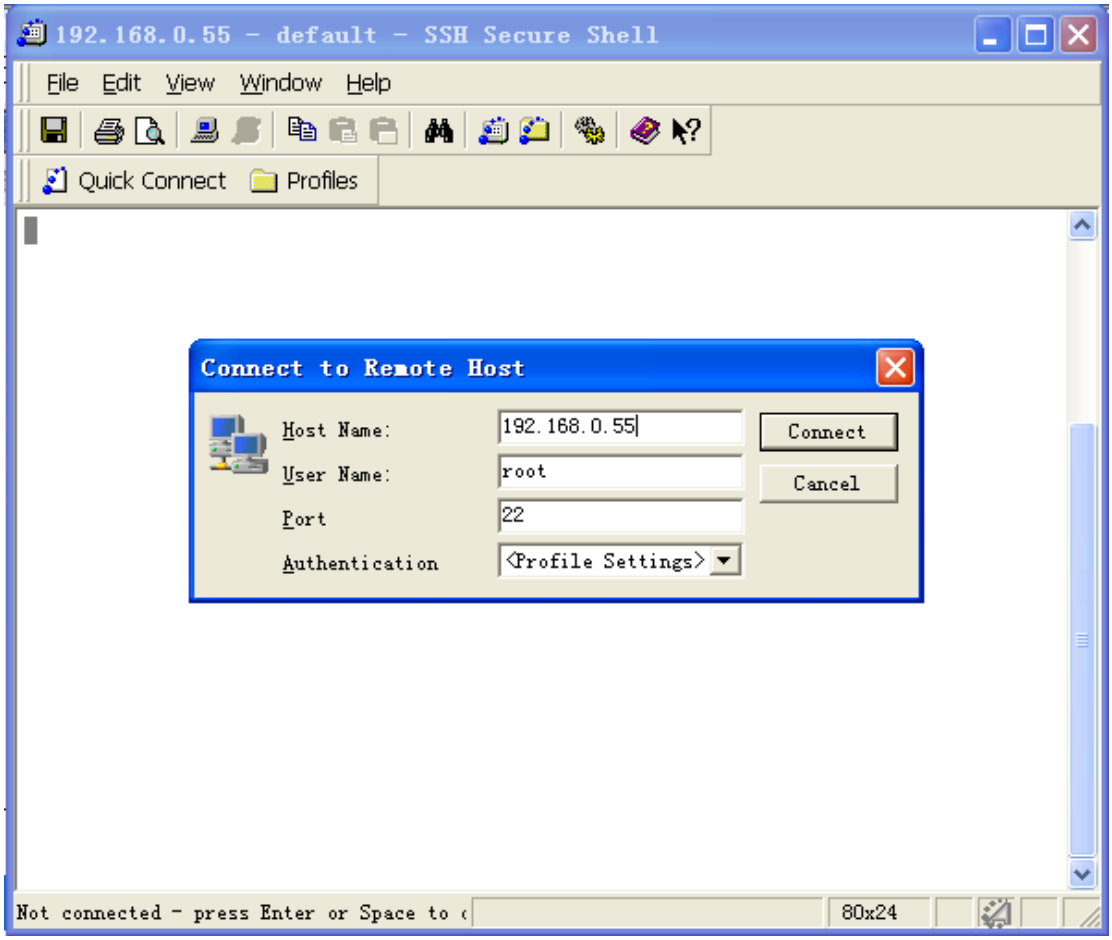
修改 selinux 配置文件

将 SELINUX=enforcing 改为 SELINUX=disabled，保存后退出。

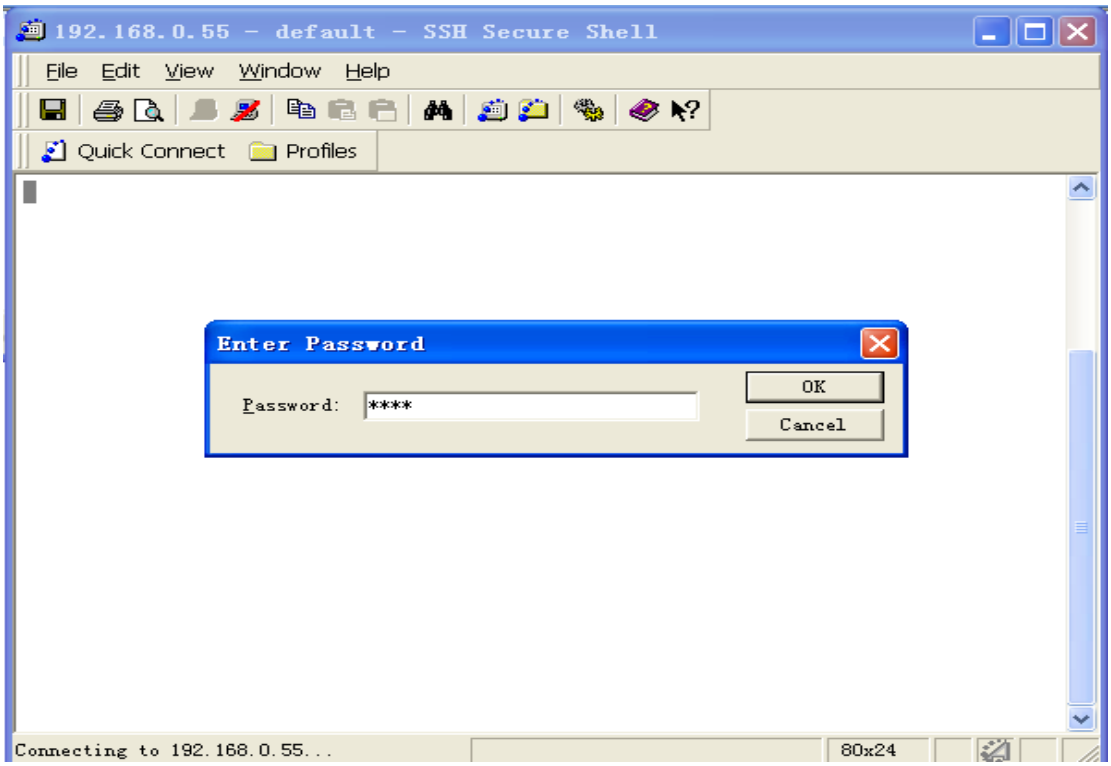
具体操作可以参照说明最后部分关闭 SElinux 操作。

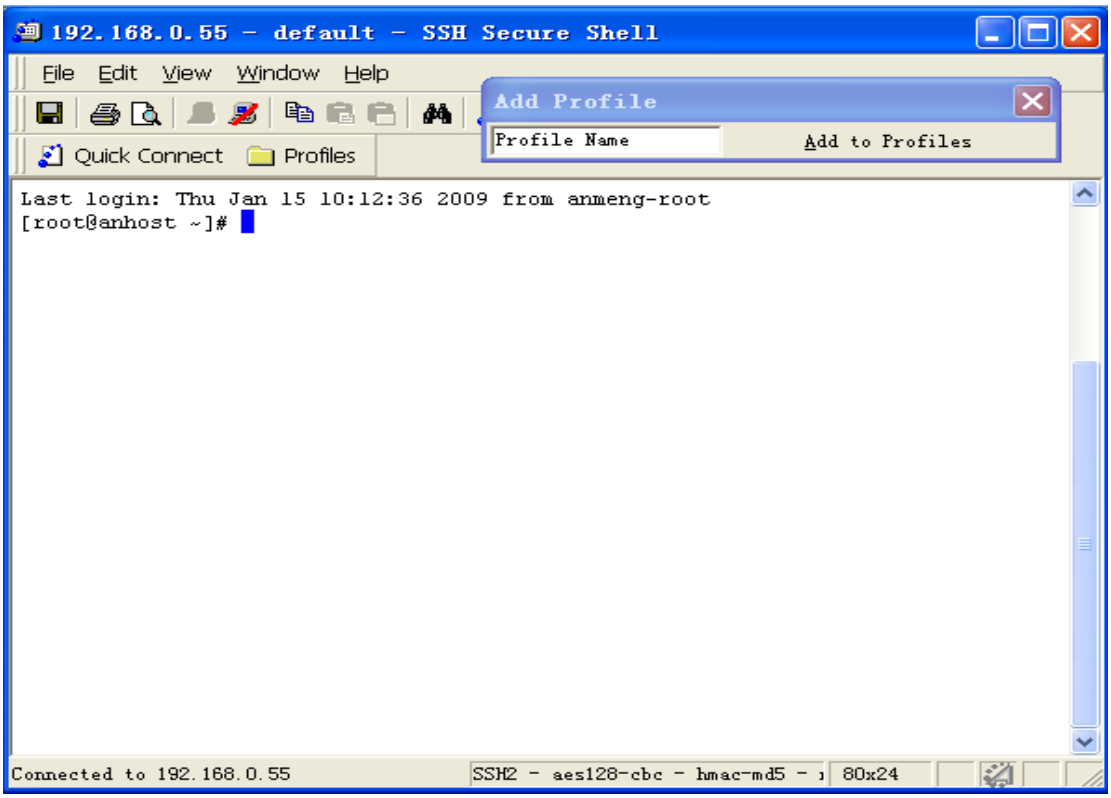
2.2 登录测试

这里我们用软件 Secure Shell Client 登录测试一下

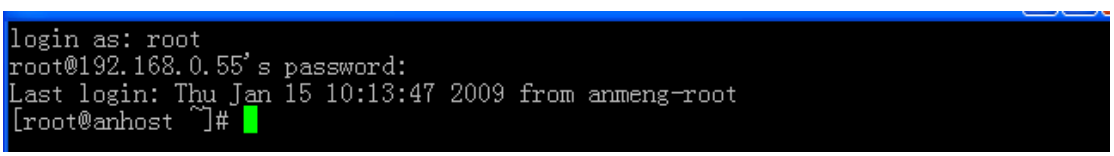


填入主机名和用户名，单击连接





成功，以后每次登录都需要进行身份认证。



其它登录方式同理。

配置 SSH 登录

在使用 ssh 协议连接代理主机的时候，ssh 默认配置是支持 PAM 模块应用，但是为了能和客户端正常配合使用需要检查文件 sshd_config 文件中的参数状态

确保/etc/ssh/sshd_configz 文件中：

UsePAM yes
UsePrivilegeSeparation no
PasswordAuthentication no

注意，参数值都为小写字母

如果修改过上面这个文件(/etc/ssh/sshd_config)，需要重新启动一次 sshd 服务

/etc/rc.d/init.d/sshd restart

该操作最好是在本地操作。重启完成后，新配置生效。

3 高级设置

3.1 设置例外组

在日常维护中，需要一些特殊用户不使用口令认证，依然由服务器本地进行认证。假如特殊用户为 adminsys，特殊组为 super 组。

配置方法：

1， 以管理员身份创建特殊用户和特殊组

#groupadd adminsys
passwd adminsys
Changing password for user adminsys.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

#groupadd super
#usermod –g super adminsys

2, 配置例外组，编辑/etc/sd_pam.conf 文件
#vi /etc/sd_pam.conf

启用组管理
#ENABLE_GROUP_SUPPORT :: 1 to enable; 0 to disable group support
ENABLE_GROUP_SUPPORT=1

指定例外组
#LIST_OF_GROUPS :: a list of groups to include or exclude...Example

LIST_OF_GROUPS=other:wheel:eng:othergroupnames:**super**

注意：配置文件不要有空格，组和组之间用冒号：分隔。

保存配置文件。到此配置例外组到此完成。

4 日常维护

4.1 关闭 SElinux 操作

- 永久关闭

修改 selinux 的配置文件，重启后生效。

- 打开 selinux 配置文件

[root@localhost ~]# vim /etc/selinux/config

修改 selinux 配置文件
将 SELINUX=enforcing 改为 SELINUX=disabled，保存后退出
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
# enforcing - SELinux security policy is enforced.
# permissive - SELinux prints warnings instead of enforcing.
# disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of three two values:
# targeted - Targeted processes are protected,
# minimum - Modification of targeted policy. Only selected processes are protected.
# mls - Multi Level Security protection.
SELINUXTYPE=targeted
此时获取当前 selinux 防火墙的安全策略仍为 Enforcing，配置文件并未生效。
[root@localhost ~]# getenforce
Enforcing

- 重启

[root@localhost ~]# reboot

- 验证

[root@localhost ~]# /usr/sbin/sestatus
SELinux status: disabled

[root@localhost ~]# getenforce

Disabled

4.2 清除结点密文

保护机器与认证服务器建立正常通信后会生成结点密文，存放路径在/var/ace 目录
如果出现认证无响应的状态，请清除结点密文重新测试。

```
cd \var\ace
rm –rf secured
rm –rf sdstatus
```