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

安盟电子信息安全有限责任公司

2019 年 06 月

版本管理

版本	摘要	作者	日期
2.7	增加高级管理	陈俊	2019/06/12
2.70	增加卸载 PAM 操作	陈俊	2020/09/02
2.71	标题中增加版本，重新编写适用范围	陈俊	2020/09/07

目录

1 前言

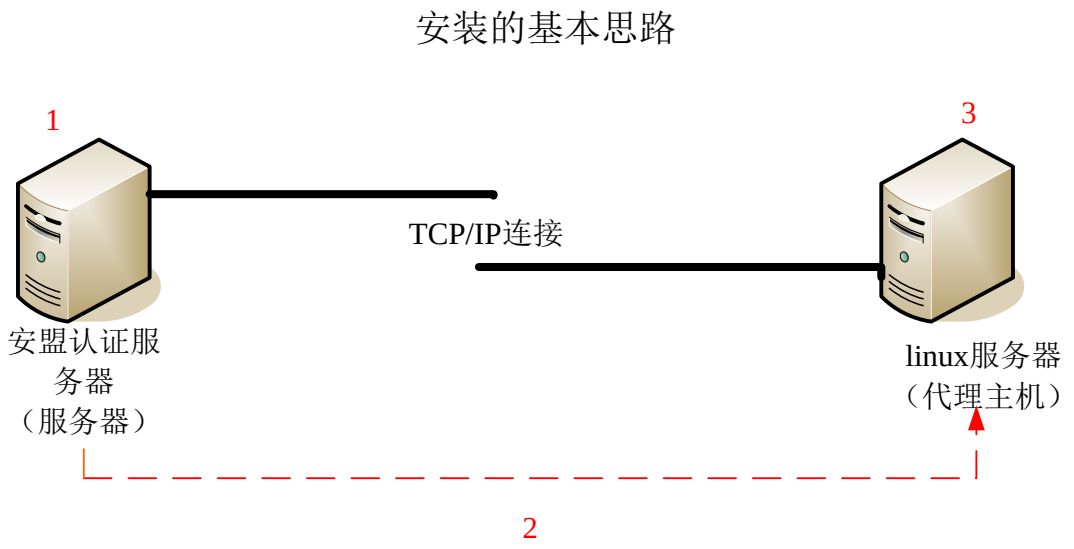
适用范围

构建的安盟身份认证系统中，认证服务器为 window 系统，代理端为 Solaris 系统。

适用人群

网络安全管理员

安装思路



1，在认证服务器上添加目标机
2，在代理主机管理中导出配置文件 sdconf.rec
3，向目标机上传 sdconf.rec 文件和 PAM6.0.tar 安装包
4，解压安装并测试
5，设置登录保护
6，登录验证

2 PAM安装

2.1 安装步骤

1， 以管理员身份，创建文件夹ampam和ace

#mkdir ampam
#mkdir /var/ace

2， 将Aget6.0Pam.tar和sdconf.res配置文件放到目标机ampam中

ftp 目标机 IP
使用 root 用户登录
ftp > cd ampam
ftp > put sdconf.rec
ftp> bin #需要用 2 进制方式上传安装包
ftp > put Agent6.0Pam.tar

3， 对目标机的/etc/ssh/sshd_config 文件备份
#cd /etc/ssh
#cp ssd_config ssd_config00

4， 进入ampam目录，复制sdconf.rec 到 /var/ace目录

#cd ampam
#cp sdconf.rec /var/ace

5， 解压AgentPam60.tar安装包

#tar -xvf AgentPam60.tar

7，.运行安装PAM安装脚本.

#./install_pam.sh

.根据提示信息，键入字母A，直到出现

```
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
************************************************************
```

到此安装完成

2.2 测试客户端

以 root 用户 cd /opt/pam/bin 目录

#./acestatus　　可以查看认证服务器信息

执行测试 acetest

#./acetest　　可以作为测试客户端

Username : ctest

Passcode:　1111

如果提示认证成功，证明客户端与认证服务器通信正常，测试完全无误后，就可以对具体的服务进行登录保护。

3　登录保护设置

3.1 ssh登录保护

3.1.1　方法一：添加 SSHD 服务进程（推荐）

添加 SSHD 服务进程，可以对 ssh，sftp 启动验证保护。

1， 以管理员身份打开/etc/pam.conf 文件

2， 增加 sshd 服务控制栈协议。默认状态下是没有该进程，需要手工写入。

sshd-none	**auth required pam_securid.so**	**reserve**
sshd-password	**auth required pam_securid.so**	**reserve**
sshd-kbdint	**auth required pam_securid.so**	**reserve**
sshd-pubkey	**auth required pam_securid.so**	**reserve**
sshd-hostbased	**auth required pam_securid.so**	**reserve**

3.1.2　方法二：修改 other 服务进程

修改 other 服务进程，可以对 ssh，su，dtlogin 启动验证保护。

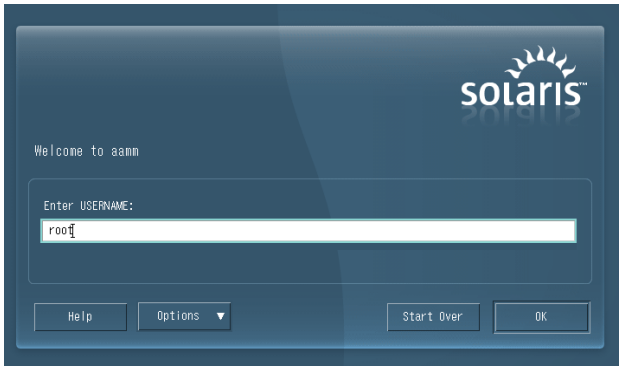
1， 以管理员身份打开/etc.pam.conf

2， 修改认证 Authentiction management other

```
#other   auth   requisite   pam_authtok_get.so.1
#other   auth   required    pam_dhkeys.so.1
#other   auth   required    pam_unix_cred.so.1
#other   auth   required    pam_unix_auth.so.1
other    auth   required    pam_securid.so reserve
```

可以让 x-windwos 进行身份认证

输入 root



输入密码，此处的密码是不显示的。

3.2 重启ssh服务

在服务器上所有配置与 SSH 服务有关的操作，最后都需要重新启动 ssh 服务，操作时候最好预先打开一个窗口（挂窗口），防止 ssh 启动失败。

sshd 重启

#svcadm restart ssh

sshd 启动

#svcadm enable svc:/network/ssh:default

sshd 停止

#svcadm disable svc:/network/ssh:default

查看 sshd

#svcs –a|grep ssh

3.3 rlogin登录保护设置

1. 进入/etc 目录, 打开 pam.conf 文件, 滚动到"认证管理"部分:
#vi /etc/pam.conf
2.找到 rlogin 部分,注释到一下这些行

```
#rlogin auth sufficient pam_rhosts_auth.so.1
#rlogin auth requisite pam_authtok_get.so.1
#rlogin auth required pam_dhkeys.so.1
#rlogin auth required pam_unix_cred.so.1
#rlogin auth required pam_unix_auth.so.1
rlogin auth required pam_securid.so reserve
```

3.4 除外用户和例外组

假设创建用户组 supper，除了这个组之外的组都要验证。

1， 以管理员身份修改 sd_pam.conf
#vi /etc/sd_pam.conf

2， 启动组验证功能，设置例外组 supper。

```
# 修改哪些组不需要验证
#ENABLE_GROUP_SUPPORT :: 1 to enable; 0 to disable group support
ENABLE_GROUP_SUPPORT=1

#INCL_EXCL_GROUPS :: 1 to always prompt the listed groups for securid authentication (include)
#                 :: 0 to never prompt the listed groups for securid authentication (exclude)
INCL_EXCL_GROUPS=0

#LIST_OF_GROUPS :: a list of groups to include or exclude...Example
#LIST_OF_GROUPS=other:wheel:eng:othergroupnames
LIST_OF_GROUPS=supper
```

4 日常基本维护

4.1 清除结点密文

日常维护中可能需要变动网络设备的路径，这样服务器上的节点密文可能会失效，需要重新生成一般的方法是，清除节点密文。

1，清除节点密文
以 root 用户 cd /var/ace 目录
2，删除 securid 文件
#rm –rf secured

3，再次生成节点密文
以 root 用户 cd /opt/pam/bin 目录
执行测试 acetest
#./acetest
Username : ctest
Passcode: 1111
提示验证成功，会重新生成节点密文

4.2 卸载PAM客户端

卸载 PAM 认证代理客户端，首先取消所有 pam 认证模块指向，恢复原本操作系统认证模块。

已 sshd 服务为例，只要注销即可。

```
#sshd-none          auth required pam_securid.so     reserve
#sshd-password      auth required pam_securid.so     reserve
#sshd-kbdint        auth required pam_securid.so     reserve
#sshd-pubkey        auth required pam_securid.so     reserve
#sshd-hostbased     auth required pam_securid.so     reserve
```

测试登录，是否恢复到操作系统原本认证。

最后，以管理员身份执行 uninstall.sh 脚本

```
cd /opt/pam/
./uninstall.sh
```

5 高级操作

5.1 负载均衡配置

安盟认证代理软件能通过向每个在域中的服务器发送一个时间请求来自动平衡认证的请求的负载，并根据每个服务器的回应时间生成一个优先值列表。

最快反应的服务器被列为最高权限并从代理主机收到最多的请求，而其他服务器获得较低的优先值和少量的请求。这种顺序一直持续直到代理软件重新发送请求。

如果轮回每个服务器的IP 地址（别名）是在代理主机配置文件(sdconf.rec)中指定，代理主机能通过防火墙连接到它的服务器。

安盟认证代理软件在使用别名发送它们的认证请求给服务器之前自动选中别名 IP 地址信息。

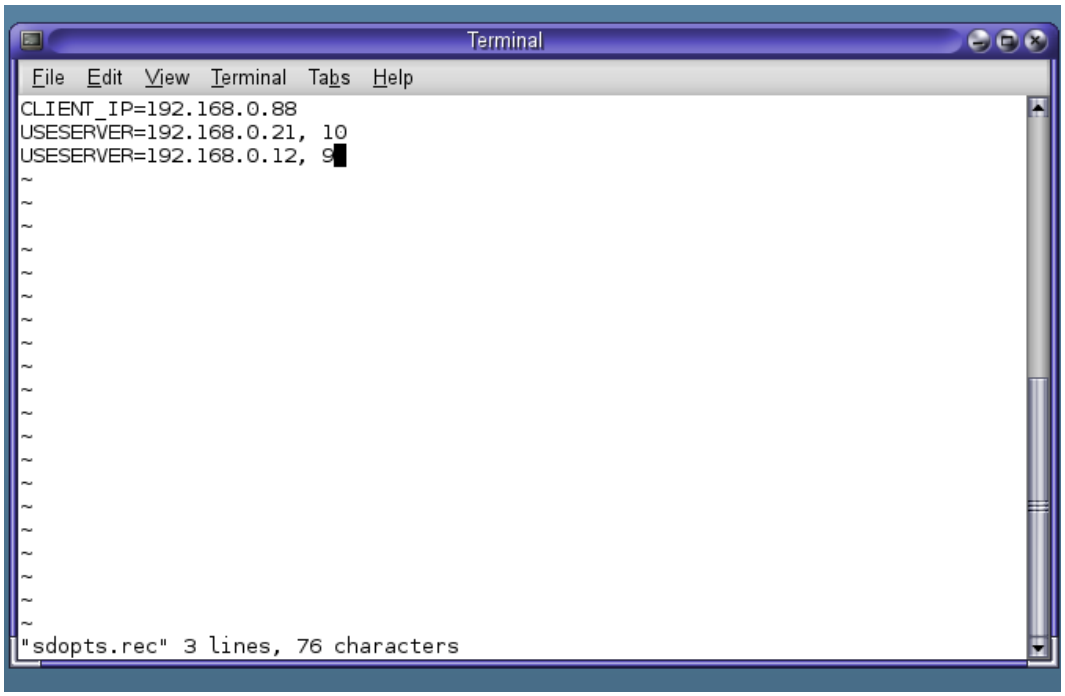
在此自动负载平衡过程中，管理员可以通过指定每个代理主机应该请求哪一个服务器来手工地平衡负载。这个指定也给每个服务器指定一个优先值使得代理主机对一些服务器的认证请求比其他的更频繁。为了使用这个选项，代理管理员在一个名为 sdopts.rec 的明文文本文件中指定优先值设置。

如果主机是多宿主机服务器，必须为代理主机指定一个基本的 IP 地址。这些依赖于控制面板高级选项中指定的设置。

如果使用 sdopts.rec 文件，管理员对于服务器优先级的设置是特别重要的。因为在这些文件中设置的优先值不是自动调整的，过多的设置代理主机发送请求给同一个服务器

可能会在执行中产生不利的影响或使优先值的有效设置随着环境变化变成无效。安盟认证服务器软件管理员应该保持与代理主机管理员之间的联系与合作以确保系统运行尽可能平稳和有效。

创建一个 sdopts.rec 文件。它为使用 sdopts.rec 文件进行手工平衡负载提供指导。



5.2 指定一个IP

代理主机有不止一块网卡时，需要指定一个主要地址，使用参数 CLIENT_IP

CLIENT_IP=<IP 地址>： 为代理主机指定一个 IP 地址。CLIENT_IP 关键字只能在文件中出现一次。

该设置与地址 IP 映射是一个概念。

5.3 指定认证服务器优先级

USESERVER=<IP 地址>， <优先级>： 为每一个代理主机所使用的服务器指定一个优先级，服务器将根据优先级接收代理主机端的认证请求。每个服务器只能指定一个 USESERVER 关键字。每个 USESERVER 关键字由一个服务器 IP 地址和优先级组成，中间用逗号分隔。优先级必须是下列值其中之一。

优先级	含义
2-10	根据分配给服务器的优先级，代理主机发送认证请求给服务器端。数字越大，优先级越高。优先级为10 的服务器接收的认证请求数是优先级为2 的服务器的24 倍
1	只有没有比优先级1 高的服务器的时候，优先级为1 的服务器才起作用
0	优先级为0 的服务器，被看作是不可用的。

注意：必须为每一个服务器指定一个优先级，否则视为非法的键值对并且关键字必须是大写。如果这些被指定关键字的服务器都没有响应，则默认的服务器是主服务器或者被用来创建配置文件sdconf.rec 的服务器。需要特别注意，服务器的最大数目为配置文件sdopts.rec 和sdconf.rec 中配置的总和，且总数不能大11。