Unix/Linux 可信主机的配置与应用

Configurations and Applications of Unix/Linux Trusted Hosts

胡雪梅 （广东纺织职业技术学院 528000） 胡建荣 （佛山市城郊农村信用联社 528000）

摘要：本文介绍了Unix/Linux可信主机的概念，重点论述了其在不同应用条件下的配置，并简要探讨了相关的安全问题。

关键词：Unix Linux 配置 可信主机

1 Unix/Linux可信主机的概念及作用

在Unix/Linux系统中，由/etc/hosts.equiv和$HOME/.rhosts文件标识的远程主机的用户在远程登录或存取本地主机系统时无需提供口令，因而被称为是“可信的”。可信用户所在的远程主机被称为可信主机。彼此可信的主机被称为互信主机。其中，环境变量HOME标识用户的初始或安装目录，每个用户都有自己独特的$HOME值。

可信主机在实际工作中是非常有用的。例如，在需要后台运行rcp命令传输文件时就必须应用可信主机；将信息处理中心的双机热备系统配置成互信，可在同一控制台上登录两机（用rlogin命令），也可方便地用rcp命令在两者间拷贝文件；在网点前台主机上，将中心主机配置成可信的，则中心可方便地登录、管理远程的前台主机，或用rcp命令下发或更新前台文件；等等。

2 系统安全与授信原则

正是因为可信主机的用户在远程登录或存取本地主机系统时无需提供口令，因此，不正确地配置或应用可信主机会给本地系统的安全造成严重的危害。这一点在配置或应用可信主机时要特别注意。

为了保障系统安全，建议最好遵循以下授信原则，正确配置可信主机：

(1) 各主机系统上由同一个人管理的用户之间方可授信。

(2) 只授信予能确保系统安全的用户，尽量避免授信予特权用户。

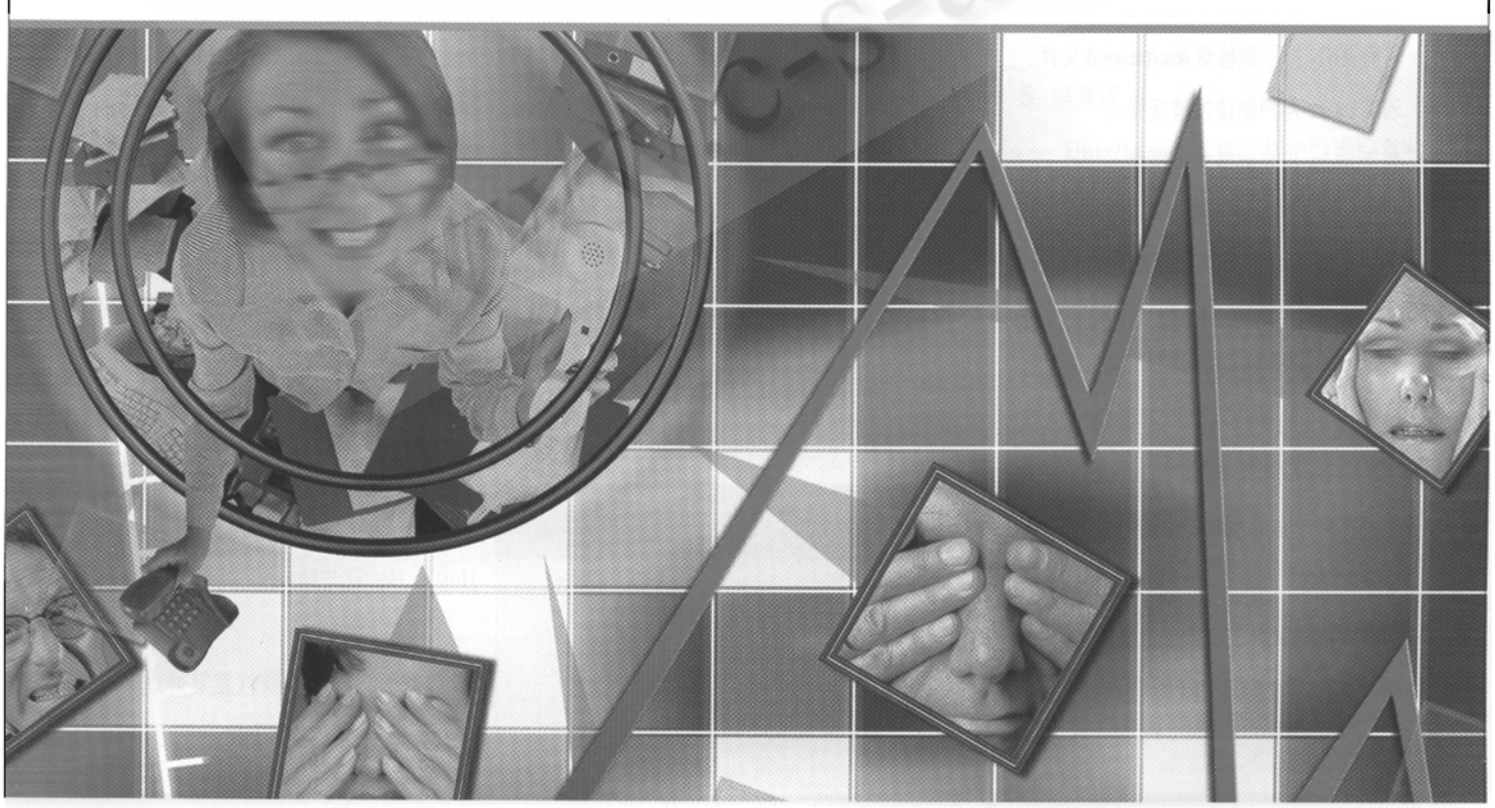
(3) 授信只在特定的用户之间进行，尽量避免在全系统范围内授信。

(4) 不需要时，及时取消对对方的信任。

3 Unix/Linux可信主机的配置与应用

在基本的操作系统和网络系统已安装调配好，各相关主机能ping通的前提下，Unix/Linux可信主机的配置主要是根据不同应用需求编辑/etc/hosts.equiv和$HOME/.rhosts两个配置文件。它们具有如下相同的格式：

hostname [username]



其中，username是可选的，建议不用。每个可信主机单独占一行，且hostname必须是/etc/hosts文件中正规的远程主机名(Official Remote Host Name)，别名(aliases)是不予识别、认可的。hostname前加一个减号（-），表示明确拒绝。在某些系统上，一行单独包含一个加号（+），表示任何主机都可信。除非该系统的安全无关紧要，否则，建议不要包含单独一个加号的行。

/etc/hosts.equiv文件定义全系统范围即所有用户的行为，而$HOME/.rhosts文件只定义某个特定用户的行为。

在本文中，远程请求专指由rlogin、rcp、rsh或rcmd命令发起的请求。系统接受或拒绝远程请求的检查、判断过程如下：

(1) 名为RHN的远程主机上的任意一个普通用户userx向本地主机发远程请求时，本地主机系统先检查/etc/hosts.equiv文件：

① 若其中有RHN行，则直接检查/etc/passwd文件：

· 若有userx用户则请求被接受；

· 若无userx用户则请求被拒绝。

② 若其中无RHN行，再检查$HOME/.rhosts文件：

· 若无RHN行，则请求被拒绝。

· 若有RHN行，则检查/etc/passwd文件：

· 若有userx用户则请求被接受；

· 若无userx用户则请求被拒绝。

(2) 名为RHN的远程主机上的超级用户root向本地主机发远程请求时，本地主机系统只检查/.rhosts（/root/.rhosts for Linux）文件：

① 若/.rhosts文件的权限大于0600或属主不是root，则请求被拒绝。

② 若/.rhosts文件的权限不大于0600且属主是root，但是/.rhosts文件无RHN行，则请求被拒绝。

③ 若/.rhosts文件的权限不大于0600且属主是root，同时/.rhosts文件有RHN行，则请求被接受。

以上检查、判断规则实际上指明了如何根据不同应用需求配置Unix/Linux可信主机的一般方法。

下面以如图所示的网络环境举例说明Unix/Linux可信主机的配置与应用。图1中，每个方框表示一台主机，并分别标明了主机名和其操作系统；云图表示TCP/IP网络，可同时包含LAN和WAN。

在下述所有配置中，/etc/hosts.equiv和.rhosts文件的属主均设为root；/etc/hosts.equiv文件和各普通用户的.rhosts文件的存取权限设为0644；root用户的.rhosts文件的存取权限设为0600。

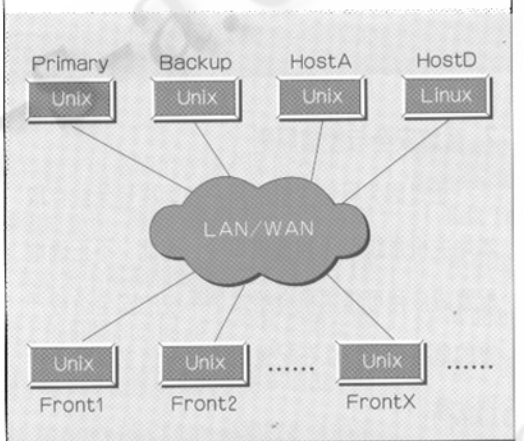


图1

表1 Primary的配置

/etc/hosts.equiv	User root
	/.rhosts
Backup	Backup

表2 Backup的配置

/etc/hosts.equiv	User root
	/.rhosts
Primary	Primary

表3 FrontX的配置

/etc/hosts.equiv	User root
	/.rhosts
Primary	Primary
Backup	Backup

双机热备系统Primary和Backup完全互信，但不信任其他任何主机，则Primary和Backup的配置文件内容分别如表1和表2。主机Primary能受理来自Backup上的所有用户的远程请求，反之也然。但两机都不受理来自其他主机的任何远程请求。这样，既方便了Primary和Backup的系统管理，特别是可方便地用rcp命令使两机的程序保持一致，又保证了系统的安全性。

任意一个网点的前台主机FrontX只信任Primary和Backup中心主机，其配置文件内容如表3。FrontX将受理来自Primary或Backup的远程请求。因此，Primary或Backup上的用户可通过rlogin命令登录FrontX后对其进行操控、管理，如对网点前台主机的系统用户口令进行统一管理并定期更新等，也可用rcp命令将文件拷贝到FrontX。反之则不行，即由FrontX向Primary或Backup发起的远程请求都将被拒绝。

主机HostD除了信任Primary和Backup外，还信任HostA上的userx用户，并已在安装时设定HostD上的root和userx用户的初始目录$HOME分别为/root和/home/userx，其配置文件内容如表4。HostD可受理来自Primary或Backup的远程请求，还可受理来自HostA的userx用户的远程请求。这一配置使Primary或Backup可后台运行rcp命令将数据库备份文件拷贝到HostD保存。

主机HostA只信任Primary和Backup上的root用户，及HostD上的userx用户，并已在安装时设定HostA上的userx用户的初始目录$HOME为/home/userx，其配置文件内容如表5。HostA只能受理来自Primary或Backup的root用户及来自HostA的userx用户的远程请求。因此，Primary或Backup的root用户可远程操控、管理HostA；HostD与HostA可共享userx用户的资源。

4 Linux系统的特殊性及其处理

Linux主机正确配置了可信的Unix主机

后，一般还不能受理来自可信Unix主机的远程请求。

反之，当Linux主机向授信予己的Unix主机发远程请求时也会失败。原因是Linux系统的rsh-server和xinetd软件包还未安装。因此，需要安装它们。

以RedHat Linux为例，运行命令：

```
# rpm -q -a | grep rsh
# rpm -q -a | grep xinetd
```

如果没有显示“rsh-server-0.17-2.2”和“xinetd-2.1.8.9pre11-1”，则需要安装它们（先将RHL OS光盘装入cdrom驱动器）：

```
# mount /dev/cdrom  /mnt
# cd /mnt/RPMS/RedHat
# rpm -i ./rsh-server-0.17-2.2.i386.rpm
# rpm -i ./xinetd-2.1.8.9pre11-1.i386.rpm
# cd;  umount /mnt
```

取出OS光盘，激活xinetd中的“rsh”服务：

```
# chkconfig rsh on
# /sbin/service xinetd reload
```

对于RHL 7.0，现在应能受理来自可信Unix主机的远程请求了。

表4　HostD的配置

/etc/hosts.equiv	User root	User userx
	/root/.rhosts	/home/userx/.rhosts
Primary	Primary	HostA
Backup	Backup	

表5　HostA的配置

/etc/hosts.equiv	User root	User userx
	/.rhosts	/home/userx/.rhosts
	Primary	HostD
	Backup	

但对于RHL 7.1，仍会拒绝来自任何可信主机的root用户的远程请求。原因是RHL 7.1增加了pam_securetty安全模块，使root用户只能从/etc/securetty文件限定的终端设备上登录。因此，为了使系统能受理来自可信主机的root用户的远程请求，还必须在/etc/securetty文件中增加一行“rsh”：

```
echo "rsh" >> /etc/securetty
```

5 结束语

Unix/Linux可信主机的恰当配置和应用既可最大限度地实现资源共享、提高工作效率，又可保证系统安全。但是，不恰当的配置和应用也会产生安全隐患，试想，如果在银行中心主机上将网点前台主机配置成可信的，因而网点前台主机的用户能以root身份通过rlogin命令，无需任何口令便进入了中心主机的情况，这有多么危险？因此，在配置和应用可信主机时一定要充分考虑本地系统资源的安全，尽量遵循本文总结提出的授信原则，在无法确保系统安全的情况下，最好不要授信予人。