Linux培训系列

————第八讲

将介绍安全 shell（ssh）和相关工具，并演示如何使用和配置网络文件系统（NFS）版本 3 服务器和客户机。Linux培训系列结束。您将具备成为 Linux 系统管理员所必需的知识。

内容基础，语言简短简洁

红联Linux论坛是致力于Linux技术讨论的站点，目前网站收录的文章及教程基本能满足不同水平的朋友学习。

红联Linux门户： www.linux110.com
红联Linux论坛： www.linuxdiyf.com/bbs
下载:Linux电子书籍：
http://www.linux286.com/linux/linuxdzsj.htm

目录

安全 shell

安全 shell －交互式登录

发布时间 :2007-01-28 13:12:36

回顾以往，如果希望建立网络上的交互式登录通话，则要使用 telnet 或 rsh。然而，随着联网越来越普及，这些工具变得越来越不适宜，因为它们极不安全。

telnet 客户机与服务器之间传递的数据是未经加密的，因而可以被任何正在监听网络的人读取。不仅如此，认证（向服务器发送密码）是以明文形式执行的，这使得捕获网络数据以即时获取密码对于某些人成了小事一桩。事实上，使用网络嗅探器，某些人可以重建您的整个 telnet 会话，并能看到您在屏幕上看到的一切。

很明显，这些在设计时假定网络是安全和不可嗅探的工具已不适应当今的分布式和公共网络。

安全 shell

发布时间 :2007-01-28 13:13:07

这就需要更好的解决方案，而该解决方案就是一个名为安全 shell（或 ssh）的工具。该工具最流行的现代版可以从 openssh 软件包获得，而该软件包几乎存在于每个 Linux 分发版中，更不用说许多其它的系统了。

ssh 与其不安全的“ 表亲 ”的显著区别在于：ssh 使用强加密对客户机和服务器之间的所有通信进行加密。通过这样做，监控客户机和服务器之间的通信就变得困难（甚至不可能）。用这样的方式，ssh 提供的服务正如宣传的那样 — 它是安全的 shell。事实上，ssh 具有极好的“ 全能 ”安全性 — 即使认证，也会利用加密和各种密钥交换策略，来确保用户的密码不会轻易被任何监控着网络上传输的数据的人截取。

在这个因特网普及化的时代，ssh 是使用 Linux 系统时增强网络安全性的有价值的工具。大多数了解安全性的网络管理员都不赞成 — 甚至根本不允许 — 在他们的系统上使用 telnet 和 rsh，因为 ssh 是非常有能力和安全的替代工具。

使用 ssh

发布时间 :2007-01-28 13:13:38

通常，大多数分发版的 openssh 软件包无需任何手工配置就可以使用。安装 openssh 后，将得到两个二进制文件。其中一个当然就是 ssh — 可以用来连接至任何运行着 sshd（安全 shell 服务器）的系统的安全 shell 客户机。要使用 ssh，通常要输入与下面相似的命令来启动会话：

$ ssh drobbins@otherbox

在上面，我指示 ssh 以 “ drobbins ” 用户帐户登录远程机器。和使用 telnet 一样，会提示您输入密码；密码输入后，就会向您提供新的远程系统上的登录会话。

启动 sshd

发布时间 :2007-01-28 13:14:11

如果允许 ssh 连接至您的机器，则需要启动 sshd 服务器。要启动 sshd 服务器，通常要使用与 openssh 包一起提供的 rc 脚本，输入如下内容：

/etc/init.d/sshd start

或

/etc/rc.d/init.d/sshd start

如有必要，可以通过修改 /etc/ssh/sshd_config 文件来调整 sshd 的配置选项。有关各种可用选项的更多信息，可输入 man sshd。

安全复制（secure copy）

发布时间 :2007-01-28 13:14:46

openssh 包本身还带有一个名为 scp（代表“ secure copy ”）的方便工具。可以使用这个命令在网络上各种系统之间安全地复制文件。例如，如果我希望将 ~/foo.txt 复制到我在远程机器的主目录，可以输入：

$ scp ~/foo.txt drobbins@remotebox:

提示输入我在远程机器上的密码后，将执行复制。或者，如果我希望将远程机器 /tmp 目录下名为 bar.txt 的文件复制到我本地系统的当前工作目录，我会输入：

$ scp drobbins@remotebox:/tmp/bar.txt .

安全 shell 认证选项

发布时间 :2007-01-28 13:15:20

openssh 还有许多其它认证方法。使用得当的话，它们允许您与远程系统认证时无需每次连接都输入密码或密码短语。要学习有关如何做到这一点的更多知识，请参阅 developerWorks openssh 密钥管理文章（在本教程最后一章“ 参考资料 ”中列出）。

NFS

NFS

发布时间 :2007-01-28 13:15:57

网络文件系统（Network File System (NFS)）是一种允许透明文件共享的技术，这种共享出现在通过局域网（也就是 LAN）连接的 UNIX 和 Linux 系统之间。NFS 已出现了很长时间；它在 Linux 和 UNIX 世界里广为人知而且被广泛使用。特别地，NFS 常用于在网络上多台机器之间共享主目录，当用户登录至 LAN 上的一台机器（*任何一台*机器）时，这为他或她提供了一致的环境。由于 NFS，挂装远程文件系统树结构并将其完全集成到系统的本地文件系统成为可能。NFS 的透明性和成熟使它成为在 Linux 下进行网络文件共享的有用和流行的选择。

NFS 基础

发布时间 :2007-01-28 13:16:25

要使用 NFS 共享文件，首先需要设置 NFS 服务器。这个 NFS 服务器随后可以“ 导出 ”文件系统。当文件系统导出后，就意味着 LAN 上的其它系统可以访问它。然后，任何同样设置为 NFS 客户机的获授权的系统都可以用标准“ mount ”命令挂装这个导出的文件系统。挂装完成后，远程文件系统以与本地挂装的文件系统（象 /mnt/cdrom）挂装后相同的方式“ 嫁接 ”。正从 NFS 服务器而不是磁盘读取所有的文件数据这一事实对于任何标准 Linux 应用程序都完全不是问题。一切正常。

NFS 的属性

发布时间 :2007-01-28 13:16:58

共享的 NFS 文件系统有许多有趣的属性。第一个“ 极好的属性 ”是 NFS 的无状态设计的结果。因为客户机对 NFS 服务器的访问本质上就是无状态的，所以 NFS 服务器重新引导而不会导致客户机应用程序崩溃或失败是有可能的。所有对远程 NFS 文件的访问将只是“ 暂停 ”，直到服务器恢复为在线为止。同样，因为 NFS 的无状态设计，NFS 服务器可以处理大量客户机，除了在网络上传送实际文件数据的开销以外，不会有任何其它开销。换句话说，NFS 性能取决于正在网络上传送的 NFS 数据的数量，而不是碰巧正在请求上述数据的客户机数量。

Linux 下的 NFS 版本 3

发布时间 :2007-01-28 13:17:50

注：不知现在发展版本到多少了，对这个感兴趣请先在网上搜索。

设置 NFS 时，强烈推荐使用 NFS 版本 3 而不是版本 2。版本 2 有一些严重的文件锁定问题，而且通常因中断某些应用程序而声名狼藉。相反，NFS 版本 3 非常出色而且健壮，并且能胜任它的工作。既然 Linux 2.2.18+ 支持 NFS 3 客户机和服务器，那么没有任何理由再考虑使用 NFS 2 了。

保护 NFS

发布时间 :2007-01-28 13:18:15

值得一提的是：NFS 版本 2 和 3 都有一些非常明显的安全性限制。它们被设计成在特殊的环境（安全、可信的 LAN）中使用。特别地，NFS 2 和 3 被设计成在只有管理员才被允许对机器进行 “ root ” 访问的 LAN 上使用。由于 NFS 2 和 NFS 3 的设计，如果恶意用户可以对您 LAN 上的机器进行 “ root ” 访问，则他或她将能够绕过 NFS 安全性，而且极有可能能够访问甚至修改 NFS 服务器上的文件，而这些用户通常是不能访问这些文件的。出于这个原因，不应该随便地部署 NFS。如果您打算在 LAN 上使用 NFS，很好 — 但请首先建立防火墙。要确保 LAN 之外的人不能访问 NFS 服务器。然后，确保内部 LAN 是相对安全的，并确保您完全清楚所有加入 LAN 的主机。一旦 LAN 的安全性经过彻底复查和（如果必要）改进，您就已经为安全地使用 NFS 做好了准备（有关这一点的更多信息，请参阅本教程系列的第 7 部分）。

设置 NFS

设置 NFS

发布时间 :2007-01-28 13:19:01

在 Linux 下设置 NFS

使用 NFS 3 的第一步是设置 NFS 3 服务器。选择将为 LAN 上其它机器提供文件服务的系统。在这台机器上，我们将需要在内核中启用 NFS 服务器支持。应该使用 2.2.18+ 内核（推荐 2.4+）以利用 NFS 3，它比 NFS 2 稳定得多。如果正在编译自己的定制内核，则进入 /usr/src/linux 目录并运行 make menuconfig。然后，选择“ File systems ”节，接着选择“ Network File Systems ”节，然后确保启用以下选项：

<*> NFS file system support
[*] Provide NFSv3 client support
<*> NFS server support
[*] Provide NFSv3 server support

准备好 /etc/exports

发布时间 :2007-01-28 13:19:31

接下来，编译并安装新内核，然后重新引导。系统现在将具有内置的 NFS 3 服务器和客户机支持。

既然我们的 NFS 服务器已在内核中支持 NFS，那么该是设置 /etc/exports 文件的时候了。/etc/exports 文件将描述可用于导出的本地文件系统，并描述哪些主机将能够访问这些文件系统，以及是将这些文件导出为读／写还是只读。还允许我们指定控制 NFS 行为的其它选项。

但在查看 /etc/exports 文件的格式以前，恰好有一个重大的实现警告！Linux 内核中的 NFS 实现只允许每个文件系统有一个本地目录的导出。这意味着：如果 /usr 和 /home 都在同一 ext3 文件系统上（例如，使用 /dev/hda6），那么在 /etc/exports 中不可能既有 /usr 导出行又有 /home 导出行。如果您试着添加这两行，则当重读 /etc/exports 文件（如果在 NFS 服务器启动并运行后输入 exportfs -ra，就会发生）时，您将看到如下错误：

sidekick:/home: Invalid argument

解决导出限制

发布时间 :2007-01-28 13:20:01

下面介绍如何解决这一问题。如果 /home 和 /usr 在同一底层本地文件系统上，则不能将两者都导出。因此只导出 /。NFS 客户机将能够毫无问题地通过 NFS 挂装 /home 和 /usr，而 NFS 服务器的 /etc/exports 文件现在是“ 合法的 ”，每个底层本地文件系统只包含一个导出行。既然您理解了 Linux NFS 的这一实现，我们就准备好查看 /etc/exports 的格式。

/etc/exports 文件

发布时间 :2007-01-28 13:20:34

理解 /etc/exports 格式的最好方法可能是查看一个快速示例。以下是我在 NFS 服务器上使用的一个简单的 /etc/exports 文件：

```
# /etc/exports: NFS file systems being exported.  See exports(5).
/ 192.168.1.9(rw,no_root_squash)
/mnt/backup 192.168.1.9(rw,no_root_squash)
```

如您所见，我的 /etc/exports 文件的第一行是一条注释。在第二行，我选择根（“ / ”）文件系统用于导出。请注意：尽管这会导出“ / ”下的所有东西，但不会导出任何其它本地文件系统。例如，如果我的 NFS 服务器有一台挂装在 /mnt/cdrom 上的 CD-ROM，则 CDROM 的内容将是不可用的，除非在 /etc/exports 中显式地将其导出。现在，请注意我的 /etc/exports 文件中的第三行。在这一行，我导出 /mnt/backup；正如您可能猜到的那样，/mnt/backup 在与 / 不同的文件系统上，并且包含我系统的备份。每一行都有“ 192.168.1.9(rw,no_root_squash) ”。该信息告诉 nfsd 只有 IP 地址为 192.168.1.9 的 NFS 客户机才可用使用这些导出文件。该信息还告诉 nfsd 使这些文件系统对于 NFS 客户机系统是可写和可读的，并指示 NFS 服务器允许远程 NFS 客户机允许超级用户帐户以获得对文件系统真正的“ root ”访问。

另一个 /etc/exports 文件

发布时间 :2007-01-28 13:21:06

下面是一个 /etc/exports，它导出的文件系统与前一页的相同，只不过它将使我的导出文件对 LAN 上所有的机器（从 192.168.1.1 到 192.168.1.254）都可用：

```
# /etc/exports: NFS file systems being exported.  See exports(5).
/ 192.168.1.1/24(rw,no_root_squash)
/mnt/backup 192.168.1.1/24(rw,no_root_squash)
```

在这个样本 /etc/exports 文件中，我用主机掩码 /24 屏蔽掉我指定的 IP 地址中的最后八位。IP 地址说明和 “ (” 之间不能有空格，这一点也很重要，否则 NFS 将错误地解释您的信息。而且，与您猜想的一样，除了 “ rw ” 和 “ no_root_squash ” 以外，还可以指定其它选项；请输入 “ man exports ” 以获得完整列表。

启动 NFS 3 服务器

发布时间 :2007-01-28 13:21:39

一旦 /etc/exports 配置完毕，就可以准备启动 NFS 服务器了。大多数分发版都有可用来启动 NFS 的“ nfs ”初始化脚本 — 请输入 /etc/init.d/nfs start 或 /etc/rc.d/init.d/nfs start 以使用它。一旦启动了 NFS，输入 rpcinfo 应该显示与下面相似的输出：

```
# rpcinfo -p
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  32802  status
    100024    1   tcp  46049  status
    100011    1   udp    998  rquotad
    100011    2   udp    998  rquotad
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100021    1   udp  32804  nlockmgr
    100021    3   udp  32804  nlockmgr
    100021    4   udp  32804  nlockmgr
    100021    1   tcp  48026  nlockmgr
    100021    3   tcp  48026  nlockmgr
    100021    4   tcp  48026  nlockmgr
    100005    1   udp  32805  mountd
    100005    1   tcp  39293  mountd
    100005    2   udp  32805  mountd
    100005    2   tcp  39293  mountd
    100005    3   udp  32805  mountd
    100005    3   tcp  39293  mountd
```

更改导出选项

发布时间 :2007-01-28 13:22:08

如果曾在 NFS 守护程序运行时更改了 /etc/exports 文件，只需输入 exportfs -ra 来应用更改。既然 NFS 服务器已经启动并运行，则可以准备好配置 NFS 客户机以使它们能挂装导出的文件系统。

配置 NFS 客户机

发布时间 :2007-01-28 13:22:42

只需确保启用了以下选项，NFS 3 客户机的内核配置与 NFS 服务器的内核配置基本类似：

<*> NFS file system support
[*] Provide NFSv3 client support

启动 NFS 客户机服务

发布时间 :2007-01-28 13:23:19

要启动适当的 NFS 客户机守护程序，通常可以使用名为 “ nfslock ” 或 “ nfsmount ” 的系统初始化脚本。通常，该脚本将启动 rpc.statd，它就是 NFS 3 客户机需要的一切 — rpc.statd 允许文件锁定以正确地工作。设置了所有的客户机服务后，在本地机器上运行 rpcinfo 将显示如下所示的输出：

```
# rpcinfo
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  32768  status
    100024    1   tcp  32768  status
```

也可以通过输入 rpcinfo -p myhost 从远程系统执行这一检查，如下所示：

```
# rpcinfo -p sidekick
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  32768  status
    100024    1   tcp  32768  status
```

挂装导出的 NFS 文件系统

发布时间 :2007-01-28 13:23:53

正确设置客户机和服务器后（并假设 NFS 服务器配置成允许客户机连接），就可以着手在客户机上挂装导出的 NFS 文件系统了。在本示例中，inventor 是 NFS 服务器，而 sidekick （IP 地址是 192.168.1.9）是 NFS 客户机。inventor 的 /etc/exports 文件包含与下面相似的一行，这一行允许来自 192.168.1 网络上任何机器的连接：

/ 192.168.1.1/24(rw,no_root_squash)

现在，以 root 用户身份登录至 sidekick 后，可以输入：

mount inventor:/ /mnt/nfs

inventor 的根文件系统现在就被挂装在 sidekick 上的 /mnt/nfs；现在可以输入 cd /mnt/nfs，然后查看 inventor 的文件。请再次注意：如果 inventor 的 /home 树结构在另一个文件系统上，则 /mnt/nfs/home 将不会包含任何东西 — 访问那些数据需要另一个 mount（以及 inventor 的 /etc/exports 文件中的另一项）。

挂装导出文件 *内部的* 目录

发布时间 :2007-01-28 13:24:26

请注意：inventor 的 / 192.168.1.1/24(rw,no_root_squash) 行还允许挂装 / 内部的目录。例如，如果 inventor 的 /usr 和 / 在同一个物理文件系统上，而您只对在 sidekick 上挂装 inventor 的 /usr 感兴趣，则可以输入：

mount inventor:/usr /mnt/usr

inventor 的 /usr 树结构现在以 NFS 方式挂装至已经存在的 /mnt/usr 目录。再次强调：inventor 的 /etc/exports 文件无需显式地导出 /usr；它 “ 免费 ” 包含在 “ / ” 导出行中。

Linux文章汇集

海量Linux技术文章

发布时间 :2006-11-24 16:50:29

下面是linux技术文章快速入口。需要联网：
Linux 技术交流

http://www.linuxdiyf.com/bbs/forum-3-1.html

Linux 应用

http://www.linuxdiyf.com/bbs/forumdisplay.php?fid=3&filter=type&typeid=1

Linux 安装及学习指导

http://www.linuxdiyf.com/bbs/forum-45-1.html

Linux 系统安装

http://www.linuxdiyf.com/bbs/forumdisplay.php?fid=45&filter=type&typeid=11

Linux 学习指导

http://www.linuxdiyf.com/bbs/forumdisplay.php?fid=45&filter=type&typeid=12

Linux 软件安装

http://www.linuxdiyf.com/bbs/forumdisplay.php?fid=45&filter=type&typeid=13

shell

http://www.linuxdiyf.com/bbs/forumdisplay.php?fid=3&filter=type&typeid=3

Linux 壁纸

http://www.linuxdiyf.com/bbs/forumdisplay.php?fid=3&filter=type&typeid=4

红旗

http://www.linuxdiyf.com/bbs/forumdisplay.php?fid=3&filter=type&typeid=5

Redhat

http://www.linuxdiyf.com/bbs/forumdisplay.php?fid=3&filter=type&typeid=6

SuSE

http://www.linuxdiyf.com/bbs/forumdisplay.php?fid=3&filter=type&typeid=7

Linux 认证

http://www.linuxdiyf.com/bbs/forumdisplay.php?fid=3&filter=type&typeid=9

Linux下载分享{酷件、书籍、视频分享 }

http://www.linuxdiyf.com/bbs/forum-6-1.html

服务器应用

http://www.linuxdiyf.com/bbs/forum-7-1.html

数据库应用

http://www.linuxdiyf.com/bbs/forum-8-1.html

Linux 编程与内核

http://www.linuxdiyf.com/bbs/forum-9-1.html

UniX 技术文章

http://www.linuxdiyf.com/bbs/forum-32-1.html

Linux 业界声音、新闻

http://www.linuxdiyf.com/bbs/forum-11-1.html

Linux 人才招聘信息

http://www.linuxdiyf.com/bbs/forum-46-1.html

网络转载，感谢原创作者！
制作：红联Linux论坛
祝您阅读愉快！