Лекция 6. Linux

К сожалению у меня не хватило времени переписать эту лекцию. Для самостоятельного изучения можно рассмотреть следующие вопросы:

Инсталляция Red Hat Linux 7.0. Использование пакетов RPM для инсталляции программного обеспечения в Linux Red Hat.

Принципы построения файловой системы Linux, файл /etc/fstab, структура каталогов, права доступа к файлам (команды chmod, chgrp, chown, umask), символические и жесткие ссылки (команда ln), монтирование и размонтирование файловых систем (команды mount и umount), создание и проверка файловых систем (команды mkfs и fsck), диспетчер файлов Midnight Comander.

Система безопасности Linux, пользователи (команда who, whoami), суперпользователь root, пароли пользователей и их затемнение (файлы /etc/passwd и /etc/shadow), проблема слабых паролей, добавление и удаление пользователей, временная блокировка пользователя, SUID-программы и проблемы безопасности.

Краткий перечень команд Linux для работы с файлами и файловыми системами: ls, cp, mv, rm, mkdir, rmdir, touch, cfdisk, df, dd, fdformat. Команды ввода-вывода: read, echo, cat, head, tail, more, page. Команды поиска и сравнения файлов: find, grep, cmp, diff. Архивация файлов: tar, gzip, gunzip. Управление процессами и остановка системы: команды ps, kill, &, bg, fg, nohup, nice, shutdown, halt, reboot, ctrlaltdel. Команды справочной системы: man, apropos, info. Перенаправление ввода вывода, конвейеры команд, команда tee, named pipes. Псевдонимы команд (команда alias). Утилита awk и потоковй редактор sed.

Оболочки (shell) в Linux - bash и tcsh, написание скриптов на shell: переменные среды, использование кавычек в сценарии (двойные, одинарные, обратные), символы подстановки, escape-последовательности, управляющие конструкции (test, if then else, while, for, until, case), передача параметров сценарию, использование функций в сценарии.

Загрузка системы: менеджер загрузки LILO, процесс init (файл /etc/inittab, уровни выполнения runlevel, команда telinit), сценарии начальной загрузки (rc-скрипты), процесс getty, профили пользователя (файлы /etc/profile, etc/bashrc, $HOME/.bash_profile, $HOME/ .bash_logout, $HOME/ .bashrc). Выполнение команд по расписанию: планировщик cron (файлы crontab), команда at. Настройка Linux при помощи пакета linuxconf. Внесение информации о сети в файлы /etc/hosts и /etc/networks, внесение информации о компьютере в файл /etc/issue.

Настройка IP-адресов сетевых интерфейсов и маршрутизации, фиктивный интерфейс, псевдонимы IP (команды ifconfig и route). Динамическая маршрутизация при помощи RIP (демон gated). Проверка работы сети при помощи команд ping, netstat, использование arp. Настройка подключения к Internet по протоколу PPP, автоматизация подключения при помощи chat, настройка подключения по требованию. Настройка ресолвера: указание порядка обращения к службам разрешения имен в файле /etc/hosts.conf . Службы разрешения имен: BIND (файл resolv.conf, демон named, программа nslookup) и NIS.

Удаленный вызов процедуры RPC: понятие, демон portmapper (файл /usr/sbin/rpc.portmap). Сетевая файловая система NFS, доступ к файловым системам Linux-сервера с рабочих станций Windows по протоколу SMB (настройка samba-сервера утилитой SWAT и вручную, запуск samba-сервера). Настройка суперсервера служб Интернета – демоны inetd и tcpd (файлы inetd.conf , hosts.allow, hosts.deny), и их замена – суперсервер xinetd (файл xinetd.conf). Файлы служб и протоколов (/etc/services и /etc/protocols). Настройка web-сервера Apache httpd (файлы httpd.conf, access.conf, srm.conf, .htaccess) и ftp-сервера wu-ftpd, установка и настройка почтового сервера sendmail, настройка прокси сервера squid.

R-службы и их настройка (файлы hosts.equiv и .rhosts). Использование ssh для безопасного подключения к системе: настройка демона sshd и клиентов ssh (файл /etc/ssh/sshd_config, команда ssh-keygen и др.), использование ssh (команды slogin, scp, ssh), туннелирование прикладных протоколов через соединение ssh.

Межсетевой экран IPChains (ipfwadm, iptables), правила фильтрации, цепочки правил, пользовательские цепочки правил, учет IP трафика, маскировка IP и NAT.

Аудит в Linux: bash.history, демон syslogd (файл /etc/syslog.conf) и log-файлы др. служб. Управление log-файлами - команда logrotate (файл logrotate.conf). Проверка изменений в файлах системы при помощи программы tripwire.

Сетевая графическая система X-Window: сценарий startx, регистрация в системе через xdm, соединение с X-сервером (переменная DISPLAY, команда xhost, файл .Xauthority), графические рабочие среды Gnome и KDE. Инсталляция и использование пакета Star Office и др. ПО для Linux.

В будущем, лекция будет построена именно в соответствии с этим планом. Сейчас же, предлагаю для ознакомления старый, и далеко не самый полный вариант.

Linux - это один из клонов Unix, развившийся в самостоятельную операционную систему. Разработка ОС Linux выполнена Линусом Торвалдсом из университета Хельсинки. Отличительной чертой ОС Linux является то, что ее исходные тексты открыты и распространяются бесплатно (среди Unix-систем бесплатно распространяются тексты FreeBSD). Существует также множество коммерческих дистрибутивов (пакетов установки) Linux: Red Hat Linux, Mandrake Linux, Slackware Linux, Debian Linux, Corel Linux, Caldera OpenLinux, S.U.S.E. Linux, Black Cat Linux, Connectiva Linux и др.

Linux является надежной, эффективной и не требовательной к оборудованию многопользовательской, многозадачной операционной системой общего назначения, наилучшим образом подходящей для создания сервера Internet и использования в глобальных сетях TCP/IP. Linux является достаточно сложной и универсальной операционной системой, требующих профессиональных навыков для работы с ней. Только перечень команд Linux, с кратким описанием их параметров занимает больше 150 страниц. А для того, чтобы корректно настроить систему, необходимо тщательно изучить справку Linux (man-страницы) и специализированные руководства. И хотя в последнее время прилагаются значительные усилия, чтобы упростить использование Linux для обычных пользователей, но до сих пор Linux сохраняет статус удобной и эффективной операционной системы для профессионалов. Рядовому пользователю, не желающему тратить время на изучение и настройку операционной системы, для которого не столь важны производительность, надежность и сетевая безопасность, можно порекомендовать воспользоваться ОС Windows.

Возможности ОС Linux.

- обладает высоким быстродействием, работает надежно, устойчиво.
- эффективно управляет многозадачностью и приоритетами, фоновые задачи (длительный расчет, форматирование дискеты и т.д.) не мешают интерактивной работе;
- множественные виртуальные консоли: на одном дисплее несколько одновременных независимых сеансов работы, переключаемых с клавиатуры;
- графическая сетевая оконная система X Window (для Linux есть версия X Window, известная как XFree86; или версия X11R5).
- передовая файловая система объемом до 4 Терабайт и с именами файлов до 255 знаков, которая, в силу своей организации, мало подвержена вирусам;
- поддержка протоколов Internet (TCP/IP, поддержка ftp, telnet, NFS); работа с сетями на базе Novell и MS Windows;
- позволяет выполнять представленные в формате загрузки прикладные программы других ОС - различных версий Unix, DOS и MS Windows;
- доступ к дискам с файловыми системами в формате DOS, Windows, CD ROM (iso9660), hpfs.
- хорошо документирована, наличие исходного текста всех программ, включая тексты ядра, драйверов, средств разработки и приложений.

Графические рабочие среды, такие как KDE или Gnome делают использование Linux не сложнее, чем Windows, а Gnome еще и построена таким образом, чтобы максимально соответствовать Windows.

Оболочки Linux

При работе с командами Linux, пользователь чаще всего видит приглашение для ввода командной строки в виде " # " или " $ ". На самом деле, эти приглашения выдает не сам Linux, а оболочка - интерпретатор интерактивных команд Linux. Так например оболочки позволяют использовать в командах Linux символы подстановки, такие как * и ?. Кроме того, оболочка – это мощный командный язык, который позволяет писать программы (shell-scripts), объединяющие несколько команд в командный файл (аналог BAT-файлов в DOS). Две самые распространенные оболочки - это sh (shell Баурна) и csh (C shell). В Linux также используются bash (развитие sh) и tcsh (развитие csh). При работе с Linux пользователи фактически работают с одной из этих оболочек, однако они – не сам Linux, а лишь надстройки над ним.

Система X Window

Система X Window – это *сетевой оконный графическ*ий интерфейс для Linux/Unix-машин, построенный на идеологии клиент-сервер. X-Window была разработана в Массачусетском технологическом институте (MIT). Используя X Window, пользователь может одновременно иметь на экране несколько окон, при этом каждое может выполняться от имени другого пользователя. В X-Window используется мышь, хотя она необязательна. Используя протоколы TCP/IP, вы можете по сети смотреть у себя содержимое X-окон, выполняющихся на других машинах. Интерфейс X Window в большой степени контролируется менеджером окон (например Open Look). Эта программа отвечает за размещение окон, изменение их размеров, перемещение окон, вид оконных рамок и т.д.

Файловая система Linux

В Linux все есть файл: принтер – файл, клавиатура, монитор или мышь – файл (/dev/console/, /dev/mouse), выполняющаяся в данный момент программа – файл. Например, вывод данных на принтер получается перенаправлением вывода информации в файл принтера, причем Linux не делает никакого отличия между файлом на диске и самим принтером. При работе в Linux необходимо учитывать, что она различает регистр символов и файлы myfail.txt и MyFail.TXT – это не одно и то же. Слэш - разделитель пути в каталогах Linux направлен в другую строну чем в Windows, т.е. не "path \ fail", а " path / fail". Более того, в Linux отсутствуют, привычные для пользователей DOS и Windows, диски A, B, C, D и т.д. Вместо этого, CD-ROM, гибкие и жесткие диски, подключаются как часть корневого каталога. При запуске компьютера сначала монтируется корневая файловая система, т.е. корневой каталог “/” (указанный при инсталляции Linux), а затем к нему монтируются все остальные жесткие диски и их разделы, указанные в файле /etc/fstab.

Таблица 6.1.

Структура каталогов Linux

Каталог	Пояснения
/	Корневой каталог. В Linux/Unix – системах слэш – в другую сторону, чем в MS DOS или Windows. Кстати, поскольку Internet – это исторически сеть Unix машин, то и адреса в Internet тоже с обратным слэшем.
/bin	Важные системные программы Linux, используемые при загрузке системы и обычными пользователями.
/sbin	То же, что и /bin, только находящиеся здесь команды не предназначены для пользователей с общими правами.
/etc	Конфигурационные файлы. Например, /etc/fstab – список подключаемых жестких дисков, /etc/rc – команды, выполняемые при запуске системы, /etc/passwd - файл паролей, /etc/shadow – теневая база паролей, /etc/group – информация о группах пользователей, /etc/securetty - терминалы, с которых может подключаться к системе пользователь root..
/usr	Каталог куда устанавливаются все программы пользователей.
/usr/etc	Файлы конфигурации несущественные для системы, но необходимые для пользовательских программ.
/usr/X11R6 /usr/X386	Файлы, используемые системой X Windows.
/usr/bin /usr/sbin	Практически все команды Linux не предназначенные для размещения в корневом каталоге (например, здесь находится большинство программ-серверов).
/usr/local	Отдельно устанавливаемые пакеты программ и другие файлы.
/root	Личный каталог пользователя root.
/home	Домашние каталоги пользователей. Например, /home/Ivan - домашний каталог пользователя Ivan
/mnt	Каталог куда обычно подключаются файловые системы: cdrom, дискетты, жесткие диски.
/dev	Файлы драйверов устройств. Они используются для доступа к устройствам и ресурсам системы, таким как диски, модемы, память и т.д. Например, имея доступ к файлу /dev/mouse вы можете читать входные сигналы от мыши, считывая данные из этого файла.
/proc	В действительности не существует на диске, а создается ядром ОС в памяти компьютера. Предоставляет информацию о системе (например /proc/meminfo - информация об использовании памяти) и выполняющихся программах. Так каталог /proc/1 содержит информацию о процессе номер 1 и т.д.
/boot	Файлы, используемые начальным загрузчиком ОС
/lib	Разделяемые библиотеки программ (аналог dll).
/var	Файлы, размер которых постоянно изменяется во время работы системы, такие как буферные каталоги (для почты, новостей и т.д.), журнальные файлы, страницы справки, а также временные файлы.
/tmp	Временные файлы.

Система безопасности Linux

ОС Linux является высоконадежной и устойчивой к повреждению вирусами. К Linux-машинам возможно удаленное подключение по протоколам HTTP, FTP, SMTP, TELNET, через механизм *демонов* (=серверы в Windows NT) – специальных программ, постоянно активных на Linux машине и позволяющих пользователю удаленно подключаться к ним. Все пользователи в Linux подразделяются на:

1) Суперпользователя – имеет неограниченные права и стандартное имя "root".
2) Обычный пользователь – имеет права с ограничениями, установленными суперпользователем ему и группе в которую входит пользователь.
3) Специальный пользователь – имеет дополнительные права для работы с конкретным приложением.

4) Псевдопользователь – пользователь, подключившийся к Linux-машине удаленно, через программу-демон. Не имеет никаких прав, не идентифицируется системой, все действия такого пользователя определяются возможностями программы-демона.
5) Владелец – пользователь создавший файл или каталог. Владелец имеет полный доступ к созданным им объектам, если он сам или root не установит дополнительные ограничения.

При подключении к Linux-системе пользователь вводит свой пароль. Пароли в зашифрованном виде хранятся на Linux-машине в специальном файле (/etc/passwd). Каждый подключившийся пользователь характеризуется своим уникальным идентификатором UID (User Identifier) и идентификатором группы GID (Group Identifier). Любой файл, созданный пользователем или запускаемая от его имени программа получают UID и GID пользователя. --> В Linux нет "ничьих" программ или файлов. Каждая программа может выполнять действия в пределах прав пользователя и его группы, а каждый файл может создаваться, читаться или изменяться только если у пользователя достаточно для этого прав. Таким образом всегда известен "автор" последних изменений в файле, а вирус, случайно принесенный пользователем , сможет разрушить только файлы пользователя и не сможет повредить системные файлы (нет прав) или файлы других пользователей. Такой подход обеспечивает достаточно стройную систему защиты, однако и в ней есть слабые места – во первых вирус принесенный пользователем root сможет повредить любые файлы, во-вторых катастрофической будет ситуация когда пароль root-а подберет какой-нибудь злобный вандал или сам root решит "насолить" начальству. Во-вторых, в Linux есть ряд программ, называемых SetUID (SUID/SGID)-программ, которые выполняются не от имени человека подключившегося к Linux, а от имени человека создавшего эти программы. Поясним на примере. Допустим, пользователю необходимо сменить собственный пароль подключения к Linux-машине. Естественно, пользователь должен иметь возможность сделать это, т.к. одно из основных правил безопасности – это периодическая смена паролей. Однако для смены пароля, пришлось бы разрешить пользователю чтение и запись в файл паролей (/etc/passwd), что недопустимо, т.к. в таком случае пользователь сможет его случайно испортить (и больше никто не получит доступ на Linux-машину) или сменить чужие пароли. Поэтому пользователю доступ к файлу паролей не разрешается. Вместо этого, системная команда смены пароля запускается с атрибутом SUID/SGID, т.е. не от имени пользователя, а от имени администратора root - владельца этой команды, создавшего ее при инсталляции Linux. Root имеет право чтения-записи в файл паролей, что позволяет пользователю изменить свой пароль, но только при помощи системной команды, созданной Root-ом. Любые другие программы пользователя доступа к файлу паролей не получат.

Краткий перечень наиболее употребимых команд Linux

Ниже будет приведен просто перечень базовых команд Linux. Более подробную информацию можно получить из справки Linux (команды справки также см. в списке команд):

Команды общего назначения

apropos	Поиск справки по ключевому слову
man, whatis	Поиск справки по точному названию команды Linux.
xman	Оконная графическая справочная система.
startx	Запуск графической оконной системы X-Window.
ls	Вывод оглавления каталога
pwd	Вывод имени текущего каталога.
cd	Смена текущего каталога.
mkdir	Создание каталога.
rmdir	Удаление каталога.
cp	Копирование файла.
mv	Перемещение файла.
rm	Удаление файла.
cat	Создание файла.
ln	Создание ярлыка.

find	Поиск файла.
grep	Поиск текста в файлах.
lp	Отправка файла на печать.
lpstat	Вывод информации о состоянии очереди печати.
cancel	Отмена печати.
ps	Вывод списка всех запущенных программ.
kill	Прерывание выполнения программы.
clear	Очистка экрана.
date	Текущая дата и время.
echo	Вывод текста на экран.
more	Вывод файла на экран по частям.
page	Постраничный вывод на экран.
sort	Сортировка.
crypt	Шифрование / дешифрование файла.
reboot	Перезагрузка компьютера.
halt	Выключение компьютера.

Администрирование

login	Вход систему, как определенный пользователь.
exit, logout	Завершение сеанса пользователя, выход из системы.
logname	Вывод имени текущего пользователя.
groups	Вывод списка групп, к которым принадлежит пользователь.
id	Вывод имени пользователя, его GID и UID.
passwd	Смена пароля пользователя.
chmod	Смена прав доступа к файлу, каталогу (чтение, запись, исполнение файла для владельца, членов группы владельца, прочих пользователей, всех пользователей).

chgrp	Смена группы, к которой принадлежит файл.
chown	Смена владельца файла.
adduser	Добавление нового пользователя.
who	Список пользователей, подключенных в данный момент к Linux-машине.
finger	Вывод подробной информации о конкретном пользователе, подключенном к Linux-машине: имя, UID/ GID, время работы и др.)
cron, crontab	Ежедневное (еженедельное, ежемесячное) выполнение программы.
at	Одноразовое выполнение программы в заданное время.

.