Linux Network Administration

System Management
COMP1071 - Summer 2020

Managing Linux Systems

- We can consider several aspects of managing a Linux system

  System resources
  Users and access control
  Software
  Network services

- Small systems are typically run by a single individual performing all tasks, larger systems call for a role-based team approach

- No matter who performs these tasks, administrative access is required to make changes to the system configuration

Administrative Access

- Most commands in a system can be run by any user, e.g. cat, more, vi, mkdir, cd, rm, etc.

- Superuser privilege is required to make changes to the system, e.g. modify configuration files, enable or disable services or devices, etc.

- For increased security and logging of access, we login as a normal user and use su or sudo to perform superuser tasks

- Extended sessions requiring root are often performed by starting a root shell using su or sudo

- The installation process for most distributions includes setting up this basic access for a default account

Linux Installation

- Linux is distributed most commonly via http or ftp
- Most distributions are available from their vendor websites, redhat.com, fedora.redhat.com, centos.org, scientificlinux.org, ubuntu.com, debian.org, opensuse.org, kali.org
- distrowatch.com is a good website to find a purpose-built distro suited to your tasks and tastes
- Download a distro, burn it to a CD/DVD or a bootable USB device, and boot it

Basic Linux System Setup

- As part of the installation process, there are several configuration steps performed
- Typically, you will be prompted for the information necessary to set the following:
  - host name - simple or fully-qualified, do not use the default name
  - network config - dhcp, or static with address/mask, gateway, dns server
  - first end-user account - user name and password
- Additonally, you may be asked to configure:
  - host type - server or desktop, i.e. do you want a GUI?
  - storage - disks, possibly raid configs
  - software - as common bundles of packages, or from a list of available packages
  - localization - timezone, locale, etc.

Setting a Hostname

- Two files are used by Linux when booting which contain the hostname
- The /etc/hostname file contains a single line with the name of the host, this is used to set the system's hostname
- The /etc/hosts file contains the mappings of host name to IP addresses, the system's hostname often maps to a loopback address
- The hostnamectl command can be used to change the system hostname without editing files directly

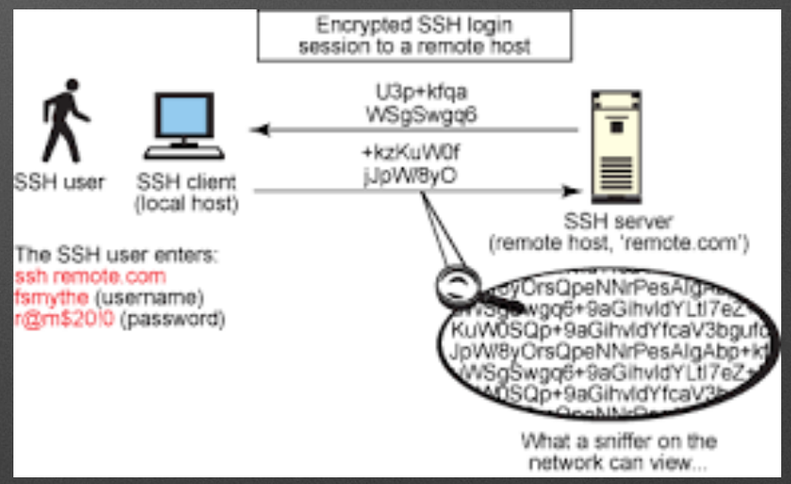
User Accounts

- User accounts can be managed with useradd, usermod, userdel or you can use adduser, deluser
- Groups can be managed with groupadd, groupmod, groupdel or you can use addgroup, delgroup
- Users may need to belong to a specific group to perform group-controlled tasks like sudo, wheel, or lpadmin
- Creating user accounts will copy the files in /etc/skel to the new user's home directory, giving them a directory structure and default environment to work with

Remote Access

- Using ssh is the primary method to remotely access a Linux server command line for adminstration, and ssh is enabled as a service by default in many distros

- Typical defaults are:
  - TCP port 22
  - passwords are required on accounts
  - direct root access requires keys or is disabled



- Keys can allow access between trusted hosts to eliminate password snooping, they are essentially just really long passwords stored securely and automatically used

SSH Service

- SSH is a protocol and program suite that allows secure remote access for terminal login, file transfer, or tunneling applications

- It supports host identification, encryption and enhanced login security using key pairs, with all SSH services being provided by the sshd daemon program

- The sshd daemon configuration is kept in the /etc/ssh/sshd_config file and allows you to modify things like the port number and login options

- The AllowUsers or AllowGroups options can be used to restrict logins to specific user accounts

- Other interesting options include PasswordAuthentication, PermitEmptyPasswords, PermitRootLogin, PubkeyAuthentication

Using Keys With SSH

- To create keys for ssh login, use the ssh-keygen command on the client machine
- The private key gets saved on the client host in ~/.ssh/id_rsa, and the public key gets saved in ~/.ssh/id_rsa.pub
- Other encryption algorithms are also available
- Insert the public key from the id_rsa.pub file into ~/.ssh/authorized_keys on the target host for the target user
- ~/.ssh/known_hosts on the client host stores host keys for previously authorized connections, used to help prevent spoofing
- You should passphrase protect your private key file

Remote Access Tools

- On a UNIX or Linux platform, simply use a terminal window and the ssh command, or the sftp command if you want to transfer files instead of using a terminal login
  e.g. ssh [user[:password]@]hostname_or_ip_address

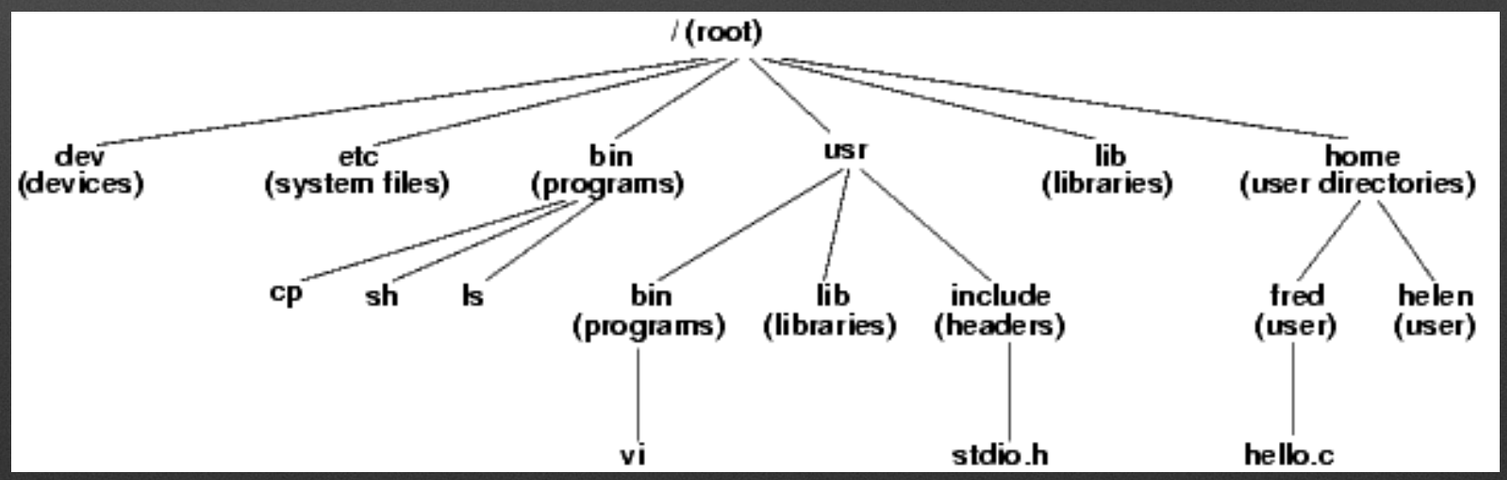
- On Windows, use a program like putty, input the hostname or ip you want, select ssh, and click connect

- If you have your server connected to your home network and the ability to forward a port on your router, you can forward the ssh port to the server's ip address and access the command line of your server from the internet
  Be certain you have assigned a strong password to any login user accounts on the server if you do this! Also install the fail2ban package.

- Showing information about who is, or was, logged in can be done with the id, who, w, and last commands

Filesystems in Linux

- A filesystem is a data structure on a storage device, created using the mkfs command
- It stores user data using file types, names, directories, and attributes
- The file names are used to uniquely identify containers for data, directories, or mechanisms for accessing data stored elsewhere (i.e. links or devices)
- The names are hierarchically structured using directories in a tree structure with one root directory and all other files contained either in that directory, or in a subdirectory one or more levels below that

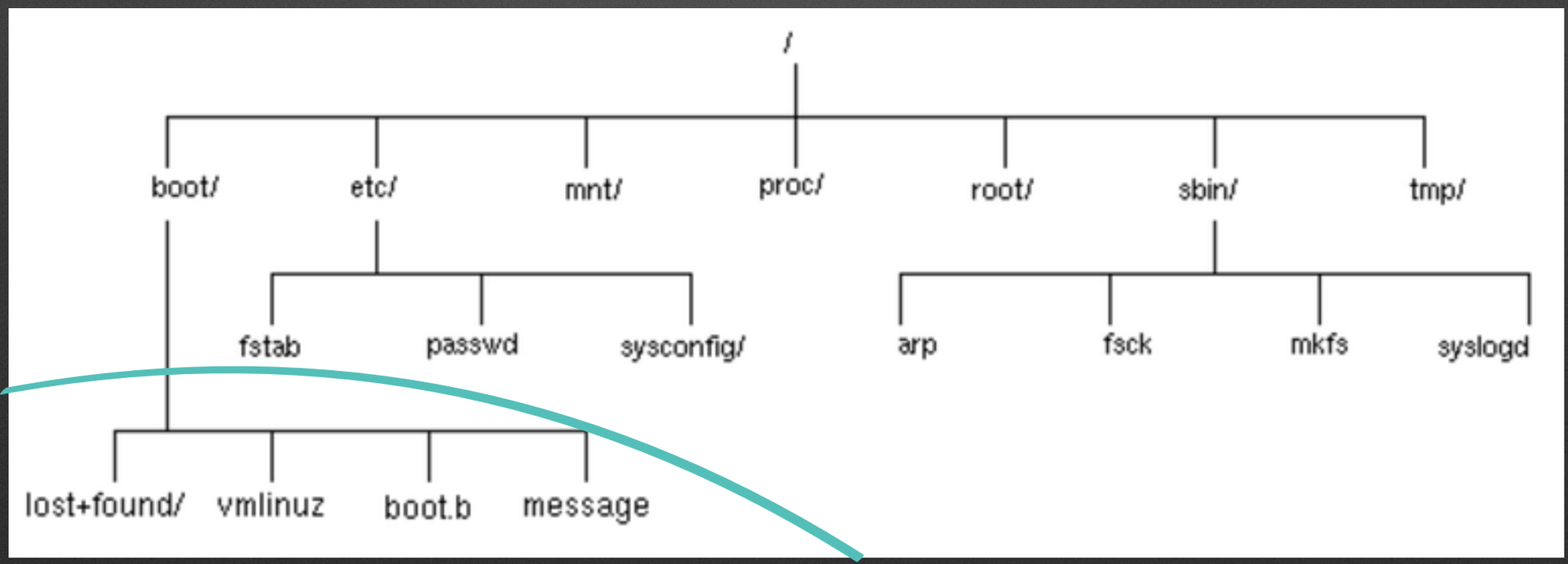


Storage Devices

- Storage devices in Linux have corresponding files in the /dev directory
- Each partition or slice of a storage device can hold a filesystem, and each gets a unique name in /dev
- The name in /dev is constructed using a device type name followed by a unit number, optionally followed by a partition letter
  e.g. /dev/sd0a, /dev/md0, /dev/disk/sd4g
- The lsblk and fdisk -l commands can be used to show your attached block storage devices and their partitions with names

Multiple Filesystems

- At powerup, the boot program creates the root point in memory and mounts the root filesystem onto it
- The boot filesystem is then mounted onto the /boot directory
- The kernel can access the files it needs using normal filesystem semantics
- The /etc/fstab file specifies the disk devices containing filesystems to be mounted along with their attributes such as filesystem type and options
- Filesystems may be manually connected and disconnected using the mount and umount commands, use eject for removable media drives such as USB drives, optical media, etc.



Storage Usage

- Hardware identification and monitoring
  - lshw, lspci, lsusb will show installed and recognized hardware
  - iostat displays storage subsystems activity
- Storage monitoring and investigation
  - df shows storage in use and amount remaining
  - du can be used to identify what space is being used by specific files and directories
  - tree can be used to show the hierarchy of files in a directory tree
  - more detailed usage tracking can be done with many tools, e.g. sar

Resource Investigation

- Hardware investigation
  - lshw, lspci, lsusb, lscpu, lsblk will show installed and recognized hardware
- Activity monitoring
  - ps, vmstat, prtstat, netstat, top show system utilization; there are many flavours of the top command (e.g. htop, vtop, iftop, slabtop)
  - memstat, mpstat, nfsiostat, cifsiostat show additional information about specific resources

sar

- sar is a system accounting report tool
- It can be run manually, collecting current data to report, or automatically for long term data collection
- It is disabled by default to avoid consuming log space
- Change the enabled setting in the file
  /etc/default/sysstat
  if you want it to collect data at all times

Software Installation

- Software is managed using packages, Debian uses the deb packaging format

- apt-get (or just apt) is used to install software packages, it is a friendly face for the dpkg tool e.g. apt-get install memstat

- APT uses a database of software packages kept in /var, and updated with apt-get update

- Always make sure your package database is up to date before doing software installations or upgrades

Software Configuration

- Many packages include scripts which run at installation to perform basic configuration of the software
- dpkg is the tool that does all the package management work and is useful for some manual tasks
  e.g. dpkg -l
- Re-running the installation scripts for a package is done using dpkg-reconfigure packagename
- After installation, some software packages are further configured by editing configuration files or by running additional tools, typically installed as part of the package

Software Management

- Reviewing installed software and identifying which files belong to which packages is done with dpkg
  e.g. dpkg -l packagename
  dpkg -L packagename
  dpkg -S filename

- unattended-upgrades is a package you can use to automatically install updates, use dpkg-reconfigure unattended-upgrades
  to turn it on

- You can manually update your software by using apt upgrade, be sure to have an updated software database when doing this

- Removing software is done using apt remove or apt autoremove for software which is no longer required
  e.g. apt-get remove bfgminer
  e.g. apt-get autoremove

Interesting Commands

- hostnamectl
- useradd, usermod, userdel
- adduser,deluser
- groupadd, groupmod, groupdel
- addgroup, delgroup
- ssh, ssh-keygen
- id, who, w, last
- mkfs, mount, umount, eject, fdisk
- lshw, lspci, lsusb, lscpu, lsblk
- iostat
- df, du, lstree
- sar
- ps, vmstat, prtstat, vmstat, top
- memstat, mpstat, nfsiostat, cifsiostat
- apt, apt-get
- dpkg, dpkg-reconfigure

Interesting Files

- /dev
- /boot
- /etc/fstab
- /etc/default/sysstat
- /var
- /etc/hostname
- /etc/hosts
- /etc/skel
- /etc/sshd_config
- ~/.ssh