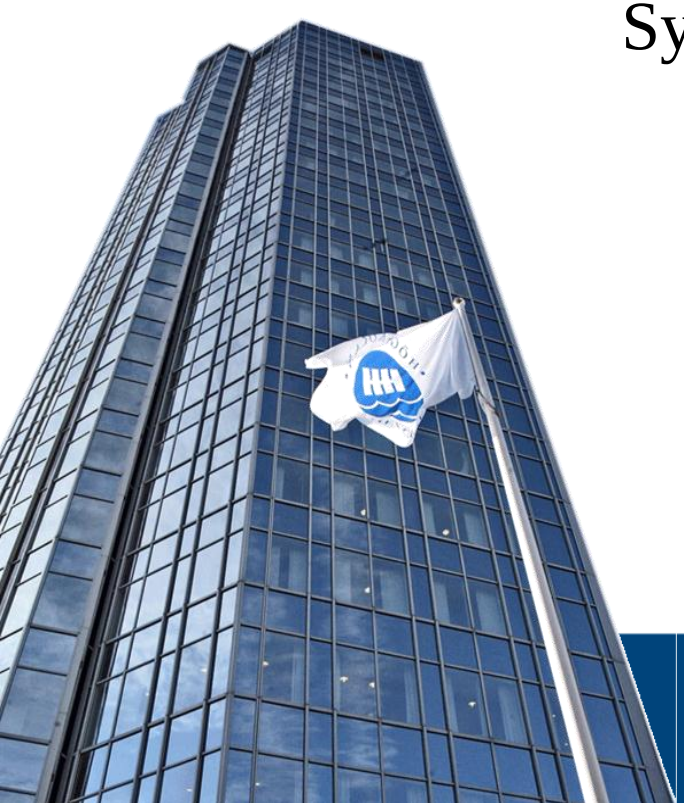
Administration of Operating Systems

DO2003

http://www.hh.se/do2003

System Administration: Core Concepts



System administration

- Consists of keeping one or more systems in a useful and convenient state for users, i.e., running properly
  - Runs quickly to address users' requirements
  - Has enough storage
  - Is safe
  - Is backed up regularly
  - Keeps software applications updated
- Performed by a System Administrator

Root or Superuser

- Some commands can compromise the system operation as well as users' privacy
- By default, ordinary users are not allowed to execute these commands neither to access some files
- However, a trusted user* must be responsible for keeping the system up and running as well as secure
- **root** or Superuser
  - Has *root privileges* (special prompt #)
  - Some commands can only be executed with root privileges
  - File and directory access permissions do not affect root
- The root can grant ordinary users can with root privileges

Gaining or granting root privileges

- If the root account is unlocked (default is locked)
  - Use the su (substitute user) command
  - Login as root
  - To unlock the root account: **`$ sudo passwd root`**
- Bring the system up in recovery-mode
- Using setuid
  - Run a program with the same privileges of its owner
- Use the sudo utility to grant users with root privileges on all (BAD) or selected (GOOD) commands
  - User password

Working with root privileges using sudo

- **Sudo** utility
  - Allows users to run programs with the security privileges of another user
    - Run commands with root privileges
  - By default in Ubuntu, the first user will be in the admin group which gives root privileges to its members
  - Advantages
    - Asks the user', not the root's, password
    - Logs all commands it executes
    - Enable specific users to execute specific commands
      - Fine-grain security policy

Working with root privileges using sudo

- **Sudo** particularities

```
$ sudo [options] [command]
```

  - Asks for your password the first time you run it
    - Unless you use the option `-k` it lasts for 15 minutes
  - `-i` option spawns a root shell, so many commands can be executed with root privileges
  - By default, the shell environment remains unmodified
  - Users with root privileges might be listed at the `/etc/sudoers` file

/etc/sudoers file and visudo

- `/etc/sudoers` is the sudo configuration file
  - Contains aliases and user privileges specifications
  - Entries follow a format specification
    - User_Alias DEVADM = wagner, slawomir
    - Cmd_Alias DEVCMD = /bin/bash
    - %DEVADM
  - Visudo is the utility used to change the sudoers file
    - Visudo checks the sudoers file for errors while other editors don't

If we have time: Demonstration

- Lab comments
- sudo
- su
- visudo
- Malware script

Upstart

- Upstart is an event-based replacement for the /sbin/init daemon (synchronous, not suitable for modern computers)
- Runs specified programs upon receiving an event
  - An event is a information that something on the system has changed
    - Addition or removal of a USB flash drive
- Programs can be scripts, start and stop services
- Operates asynchronously starting tasks and services during boot, stopping them during shutdown and supervising them while the system is running
- The /etc/init directory holds job definition files (.conf files) while the scripts to be executed are at /etc/init.d/

Upstart

- Feature Highlights
  - Tasks and Services are started and stopped by events
  - Events are generated as tasks and services are started and stopped
  - Events may be received from any other process on the system
  - Services may be respawned if they die unexpectedly
  - Supervision and respawning of daemons which separate from their parent process
- initctl utility
  - start, stop, list and status of jobs
  - emit events

Upstart

- Creating your own job
  - Requires root privileges

```
$ sudo touch /etc/init/myjob.conf
…
$ sudo nano /etc/init/myjob.conf
start on myevent
script
    echo "Hi there, here I am!" >> /tmp/myjob.out
    date >> /tmp/myjob.out
end script
$ sudo initctl emit myevent
$ cat /tmp/myjob.out
Hi there, here I am!
Wed Mar 10 11:59:23 PST 2010
$ status myjob
myjob stop/waiting
$ sudo initctl emit control-alt-delete
```

System Operation

- **Booting the system**
  - Is the process of reading the Linux kernel into system memory and starting it running
  - The last step of the boot procedure, Linux starts the Upstart init daemon as PID number 1
    - init is the first genuine process to run after booting
    - init is the parent of all system processes
    - If you kill process 1, the system will crash
      - Kill is a textual utility that sends a signal to a process that might terminate (kill) the process

```
$ kill [signal] PID
```

System Operation

- **Bringing the system down**
  - Shutdown utility
    - Prepares the system to be turned off
    - You must indicate what time to bring the system down
    - Warns all before bringing the system down
  - CONTROL-ALT-DEL (etc/init/control-alt-delete)
    - Reboots the system
    - Can be disabled
- DO NOT TURN THE POWER OFF BEFORE BRINGING THE SYSTEM DOWN

System Operation

- CRASH
  - Occurs when the system unexpectedly stops or fails
    - Caused by SW or HW problems or power loss
  - The filesystem is checked automatically during the boot process
  - A system administrator might prefer to check manually the filesystem for possible problems
    - The fsck (filesystem check) utility checks the consistency of a file system
    - It is recommended to perform a filesystem backup before using fsck

System Operation

- Communicating with system users
  - You can edit the `/etc/motd` file to change the "message of the day" presented when the user logs in
  - Use the utility `wall` to communicate immediately with all users who are logged in

Setting Up a Server

- Standard Rules in Configuration
- Rpcinfo and portmap
- The inetd and xinetd Superservers
- Securing a Server
- DHCP

Setting Up a Server

- Standard Rules in Configuration
  - Standard Rules in writing Configuration Files
    - Blank lines, comment, …
  - Specifying clients and subnets

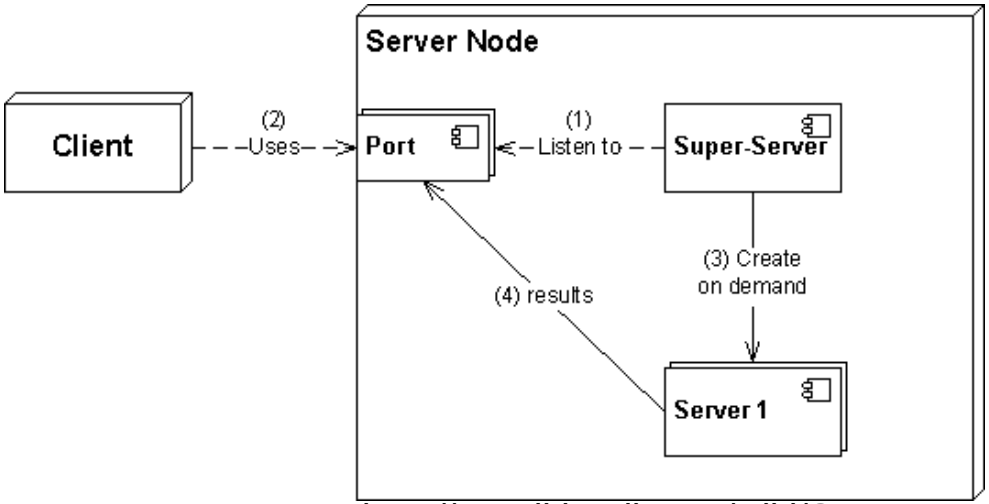
Pattern	Matches
n.n.n.n	One IP address, e.g., 192.168.231.125
name	One hostname, e.g., localhost
name starts with .	name ending with the specified string
IP addr ending with .	IP addresses starting with the specified numbers
n.n.n.n/m.m.m.m	IP addresses based on subnet mask
ALL	Always match

Setting Up a Server

- ~~Standard Rules in Configuration~~
- Rpcinfo and portmap
  - rpcinfo displays information about programs registered with portmap
  - Portmap is a deamon that holds information about **which servers** are running on the local system and **which port** the each server is running on
  - rpcinfo makes RPC to programs: Are you alive?
  - Security
    - /etc/host.allow and /etc/hosts.deny

Setting Up a Server

- ~~Standard Rules in Configuration~~
- ~~Rpcinfo and portmap~~
- The inetd and xinetd Superservers
  - Service dispatchers. Start other servers when needed
  - Listens and responds to network connections



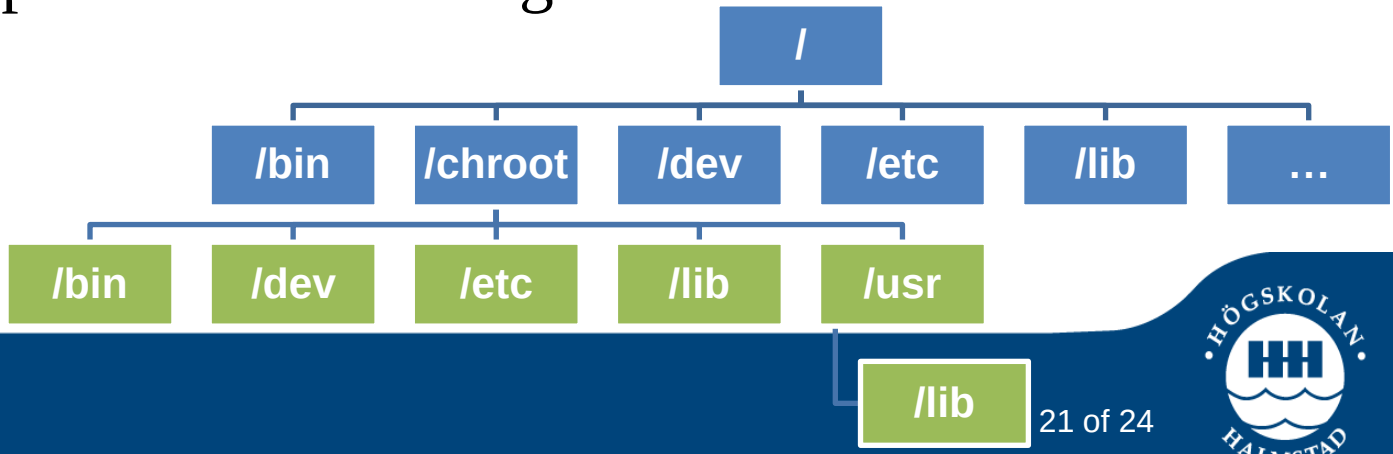
http://en.wikipedia.org/wiki/Super-server

Setting Up a Server

- ~~Standard Rules in Configuration~~
- ~~Rpcinfo and portmap~~
- ~~The inetd and xinetd Superservers~~
- Securing a Server
  - Using TCP wrappers
    - Host-based Networking ACL system, used to filter network access to servers
    - Control who can use which system services by editing the /etc/hosts.allow and /etc/hosts.deny files
  - Set up a chroot jail

Setting Up a Server

- ~~Standard Rules in Configuration~~
- ~~Rpcinfo and portmap~~
- ~~The inetd and xinetd Superservers~~
- Securing a Server
  - Using TCP wrappers
  - Set up a chroot jail
    - Limits the portion of the filesystem a user sees, so it can help control the damage a malicious user can do



Setting Up a Server

- ~~Standard Rules in Configuration~~
- ~~Rpcinfo and portmap~~
- ~~The inetd and xinetd Superservers~~
- ~~Securing a Server~~
- DHCP (Dynamic Host Configuration Protocol)
  - Enables client systems to retrieve the necessary network configuration information from a DHCP server each time they connect to the network
  - A DHCP server assigns an IP addresses from a pool of addresses to clients as needed
    - Dynamic or static allocation

Setting Up a Server

- DHCP Client (dhcp3-client)
  - A DHCP client requests network configuration parameters from the DHCP server and uses those parameters to configure its network interface
  - DHCP lease information is stored in dhclient.leases
- DHCP Server (dhcp3-server)
  - Maintains a list of IP addresses and other configuration parameters. When requested, the DHCP server provides configuration parameters to a DHCP client
  - Some devices should NOT have an IP address assigned via DHCP

Total number of MCQs: 744 and counting