Systems administration in Linux

DEPARTAMENTO DE SISTEMAS INFORMÁTICOS

Enrique Arias
Universidad de Castilla–La Mancha

Contents

- Main objectives
- User management
- System monitoring
- Basic system security

Contents

- Main objectives
- User management
- System monitoring
- Basic system security

Main objectives

- To know some commands related to system administration
  - User and group management
  - System monitoring
  - Security commands

Contents

- Main objectives
- User management
- System monitoring
- Basic system security

User management

- /etc/passwd and /etc/shadow files

root:x:0:0:root:/root:/bin/bash

earias:x:500:500:Enrique Arias:/home/earias:/bin/bash

- Commands
  - adduser <username> or useradd <username>
  - passwd <username>
  - userdel -r [username]
  - usermod -g [groupname] [username]
  - groupadd [groupname]
  - groupdel [groupname]
- Notes:
  - Always work with the minimum privileges account
  - Increase privileges using sudo -s

User management

- Exercise 1
  1. As root create a user with a password. Change the password to another.
  2. See if the user is in /etc/passwd file and the user directory has been created in /home
  3. Change the owner and group of some of our files
  4. Delete the user created in step 1.
  5. Verify if this user has been deleted from /etc/passwd. Also, if the user directory has been deleted from /home. If not, use rm or rmdir.
  6. Back the owner and group of the file in step 3.

Contents

- Main objectives
- User management
- System monitoring
- Basic system security

System monitoring

- System monitoring ≡ Accounting
- Commands
  - vmstat
    - Reports information about processes, memory, paging, block IO, traps, disks and cpu activity.
    - vmstat [options] [delay [count]]
      - delay → The delay between updates in seconds. If no delay is specified, only one report is printed with the average values since boot.
      - Count → Number of updates. In absence of count, when delay is defined, default is infinite.
    - Use man for Information about options

System monitoring

- Exercise 2
  - Displays up to 10 times the state of the system by sampling at 3-second intervals

System monitoring

- System monitoring ≡ Accounting
- Commands
  - Top
    - Provides a dynamic real-time view of a running system.
    - It can display system summary information, as well as a list of processes or threads currently being managed by the kernel: CPU use, memory, swap, running processes, etc
    - top -hv | -bcHisS -d delay -n limit -u|U user | -p pid -w [cols]
    - Use man for Information about options

System monitoring

- Exercise 3
  - Execute top and observe the information previously commented

System monitoring

- System monitoring ≡ Accounting
- Commands
  - ps
    - Reports a snapshot of the status of currently running processes.
    - Use man for Information about options

System monitoring

- Exercise 4
  - Using ps, tail, grep and pipes, show the last two active processes that belong to you. Do the same with those belonging to root.

System monitoring

- System monitoring ≡ Accounting
- Commands
  - du and df
    - du estimates and displays the disk space used by files (Kbytes).
    - du [OPTION]... [FILE]...
    - df reports the amount of available disk space being used by file systems.
    - df [OPTION]... [FILE]... (1K blocks)
    - Use man for Information about options

System monitoring

- Exercise 5
  - Use du (with the default options) over a directory. Now use the -k, -m and -h options. What do these options mean?
- Exercise 6
  - As in the previous exercise, execute df and observe the result without options and with the options -k, -m and -h.

System monitoring

- System monitoring ≡ Accounting
- Commands
  - ping
    - It is frequently used to test, at the most basic level, whether another system is reachable over a network, and if so, how much time it takes for that data to be exchanged.
    - ping [-LRUbdfnqrvVaAB] [-c count] [-m mark] [-i interval] [-l preload] [-p pattern] [-s packetsize] [-t ttl] [-w deadline] [-F flowlabel] [-I interface] [-M hint] [-N nioption] [-Q tos] [-S sndbuf] [-T timestamp option] [-W timeout] [hop ...] destination
    - Use man for Information about options

System monitoring

- System monitoring ≡ Accounting
- Commands
  - traceroute
    - traceroute prints the route that packets take to a network host.
    - traceroute [-46dFITUnreAV] [-f first_ttl] [-g gate,...] [-i device]
      [-m max_ttl] [-p port] [-s src_addr] [-q nqueries]
      [-N squeries] [-t tos] [-l flow_label] [-w waittime]
      [-z sendwait] [-UL] [-D] [-P proto] [--sport=port] [-M method]
      [-O mod_options] [--mtu] [--back] host [packet_len]
    - Use man for Information about options

System monitoring

- Exercise 7
  - See if a machine is active and where the traffic is routed to it.

Contents

- Main objectives
- User management
- System monitoring
- Basic system security

Basic system security

- nmap
  - nmap is used for exploring networks, perform security scans, network audit and finding open ports on remote machine.
  - It scans for Live hosts, Operating systems, packet filters and open ports running on remote hosts.
  - nmap [Scan Type...] [Options] {target specification}
  - Use man for Information about options

Basic system security

- Exercise 8
  - Show which ports are open in your own machine. You can obtain your IP address using the ifconfig command.

Contents

- Main objectives
- User management
- System monitoring
- Basic system security

Systems administration in Linux

DEPARTAMENTO DE SISTEMAS INFORMÁTICOS

Enrique Arias
Universidad de Castilla–La Mancha