

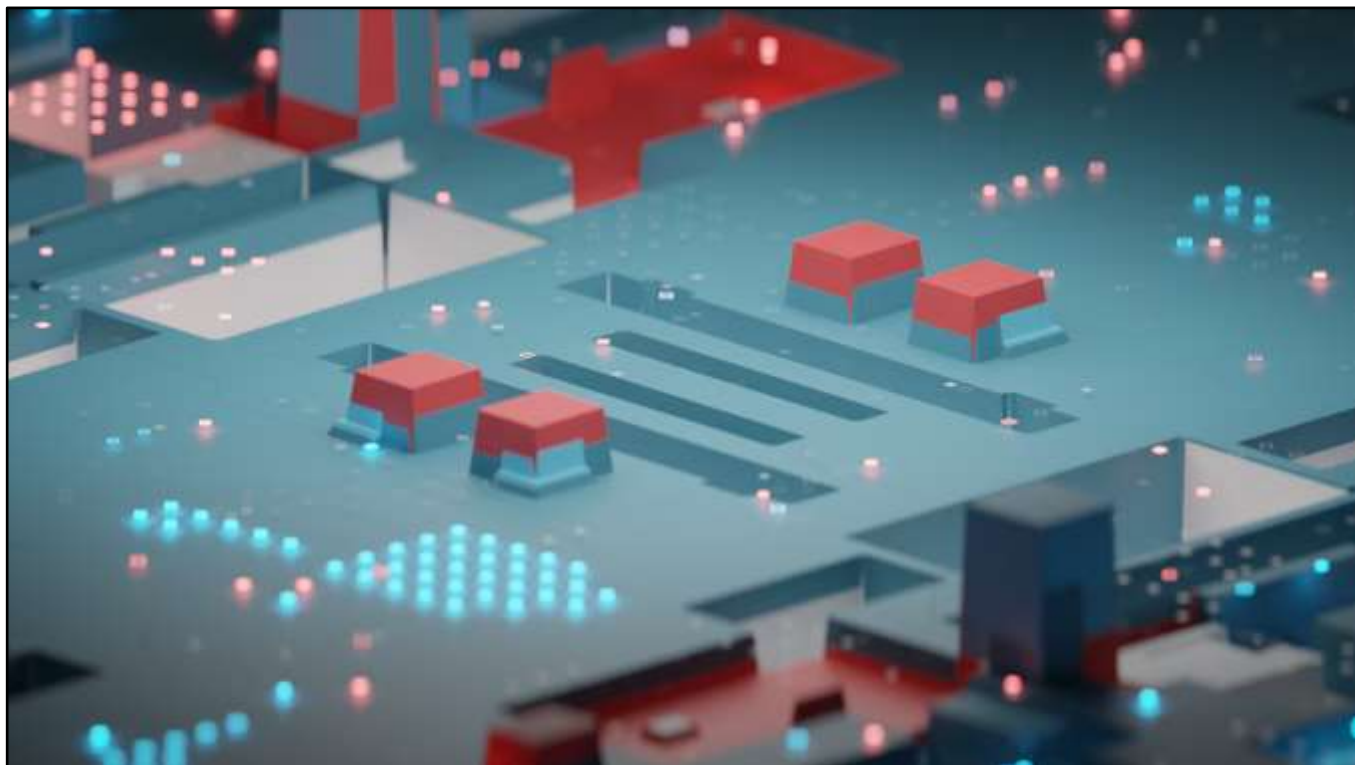


Linux + CompTIA XK0-005

©2023 by StormWind LLC. All rights reserved.

<https://t.me/learningnets>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.

<https://t.me/learningnets>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

About the Instructor

Shane Sexton

Linux+
CCNP Security
Cisco CyberOps Associate
CCNA R&S
CND
CySA+
Security+
A+

The Linux + 005 Exam

XK0-005

90 question maximum

Multiple choice

Performance based

Passing is 720 on a scale of 100 to 900

Course Prerequisites

Recommended experience only:

12 months hands-on experience

Up from 9-12 months for XK0-004

A+ , Network+, Server+, or equivalent

Exam Objectives

System Management

32%

Security

21%

Scripting, Containers, and Automation

19%

Troubleshooting

28%

Operating Systems: Desktop

End user systems

Multi-purpose computers whose size, capabilities, and price make it feasible for individual use. Personal computers are intended to be operated directly by an end user

Distribution examples

Ubuntu	Zorin OS
Mint	MX Linux

Examples of security-specific distributions

Kali	BlackArch
Parrot	



Operating System: Server

Server distributions

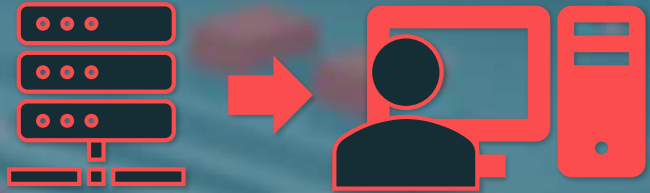
Ubuntu Server

Debian

OpenSUSE

RHEL

Fedora Server



"....a computer program or device that provides a service to another computer program and its user...."

Origin of Linux

Created 1991 by Linus Torvalds and Free Software Foundations

1992 relicensed under the GNU GPL

GNU: Free software collection

GPL : General Public License

1994 Linux 1.0 released

1996 Linux 2.0

1998 IBM, Compaq, Oracle

1999 Graphical Environment GNOME

2005 openSUSE

2013 Android has 75% of smartphone market share

2014 Ubuntu 22m users

2016 Linux 4.0

2017 All top 500 supercomputers running Linux

2019 Linux 5.0



Distributions: Open Source

Linux (and its many distributions): most popular open-source OS

Free as in freedom (not necessarily free as in beer)

General Public License (GPL)

Distributions: Paid

Red Hat Enterprise Linux

SUSE Enterprise Linux

Major Distributions

Debian-based

Ubuntu
Kali Linux
Parrot OS
Deepin



Major Distributions

Arch Linux

Archlabs Linux

ArcoLinux

EndeavourOS

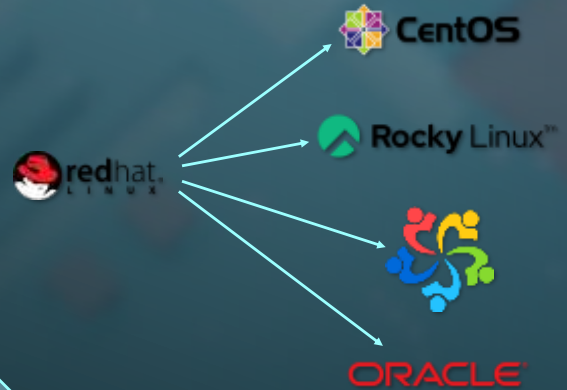
Manjaro



Major Distributions

Red Hat

CentOS
Rocky Linux
AlmaLinux
Oracle Linux
RHEL

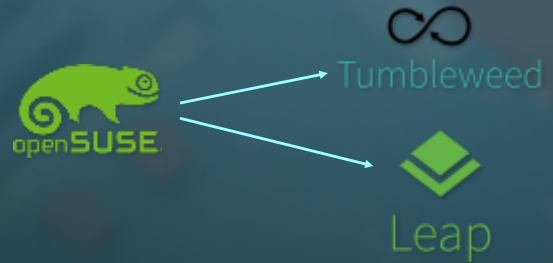


Major Distributions

openSUSE

Tumbleweed (rolling release)

Leap (stable regular release)



Linux Architecture

Hardware

SSD or HDD
CPU
RAM

Kernel

Interface with hardware and processes

Types:

Monolithic (Linux)
Micro
Exo
Hybrid

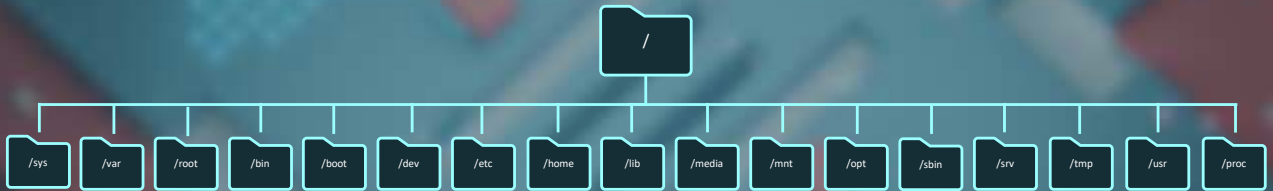
Shell

Interface for the user to interact with the kernel

Applications



File Hierarchy



Advantages

Free and open-source

Security

Fewer users means less malware.

Open-source means more eyes
for vulnerabilities

Constant updates

Servers

96.3% of the world's top 1 million
servers run on Linux



Disadvantages

Hardware

Support for some hardware is limited or nonexistent in Linux

Software

Often targets Windows and Apple due to:

- Lack of customers

- Vast amount of Linux distributions

Learning Curve

- Command-line interface

- Different software



Windows vs. Linux

Windows

Cost
Subscription model

Source Code
Proprietary; closed-source

Customization
Extremely limited

Software & Games
Vast selection from nearly every brand

Linux

Cost
Free for most distributions

Source Code
Open and available to the public

Customization
Highly customizable

Software & Games
More limited

GUI



LINUX MATE



GNOME

Terminal

Most common way to administer Linux

Often faster than the GUI

Chain commands

Automate actions

Learning curve

```
#!/bin/bash

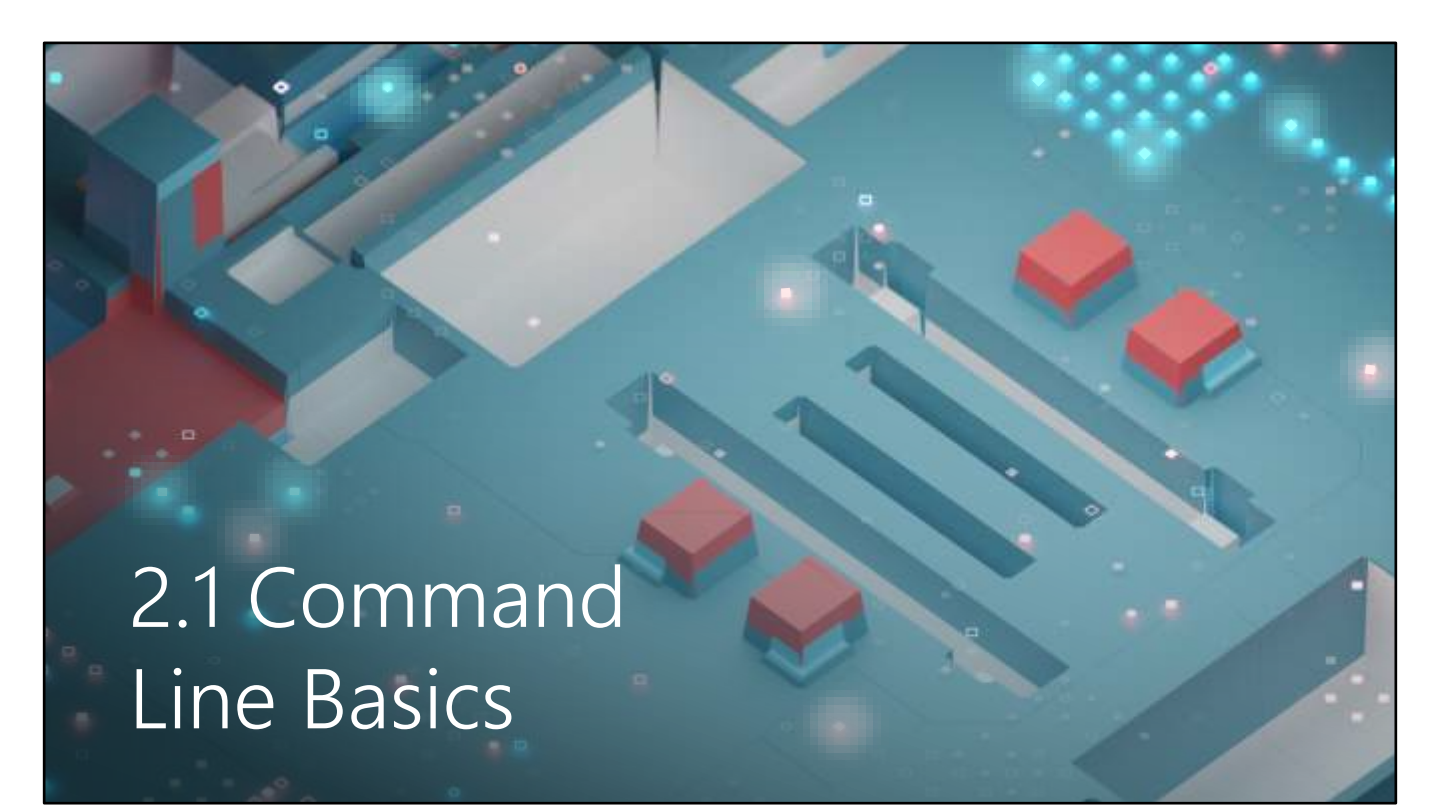
#ASKS USER NEW USERNAME
echo "What is the new Username"
read Username

#CREATES USERNAME
useradd $Username

#provide message
if [ $? -eq 0 ];
then
    echo "User created successfully"
fi

#SET USER PASSWORD
passwd $Username
```

```
root@Ubuntu:~/ex# bash ./createuser.sh
What is the new Username
nathan
User created successfully
New password:
Retype new password:
passwd: password updated successfully
```



2.1 Command Line Basics

Topics

- Introduction to the terminal
- Navigating with the CLI
- Absolute vs. relative paths
- Commonly used commands
Syntax

Terminal Navigation



pwd

Displays where you are located

```
joshua@Nitro5:~$ pwd  
/home/joshua
```

Terminal Navigation



ls <directory>

List contents of current directory (by default)

```
root@Ubuntu:~# ls
aaexample.sh  data      Documents Employees.txt  files    here.sh  Layer7.txt  Music    pictures  Public    sith      trcrt.txt  Videos
Application.txt Desktop  Downloads  ex           file.txt jediorder mess      OSI_Model.txt Pictures  sedexample.sh Templates videos     woodchuck.txt
```

Terminal Navigation



cd <directory>

Moves you to specific directory
(absolute or relative)

```
root@Ubuntu:~# cd Documents
root@Ubuntu:~/Documents#
```



cd ..

Moves you to parent directory

```
root@Ubuntu:~# cd Documents
root@Ubuntu:~/Documents# cd ..
root@Ubuntu:~#
```



cd or **cd** ~

Moves you to home directory

```
root@Ubuntu:~/Pictures# cd Screenshots/
root@Ubuntu:~/Pictures/Screenshots# cd
root@Ubuntu:~#
```

Terminal Navigation



Absolute

Path from the root directory
Always begins with /

```
joshua@Nitro5:~$ cd /home/Joshua/Pictures/Vacation  
Joshua@Nitro5:~/Pictures/Vacation$
```



Relative

Path from the current directory

```
joshua@Nitro5:~$ cd Pictures/Vacation  
Joshua@Nitro5:~/Pictures/Vacation$
```

Creating, Viewing, Moving



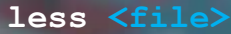
cat <file1> .. <fileX>

Output contents of file(s) into terminal

```
root@Ubuntu:~# cat file.txt  
This is a text file!
```

```
root@Ubuntu:~# cat cat.txt dog.txt  
This is cat.txt!  
This is dog.txt!
```

Creating, Viewing, Moving



View file one page at a time

[illegible]

Creating, Viewing, Moving



mkdir <directory>

Create a new directory

```
root@Ubuntu:~/jediorder# ls
root@Ubuntu:~/jediorder# mkdir clones
root@Ubuntu:~/jediorder# ls
clones
root@Ubuntu:~/jediorder#
```

Creating, Viewing, Moving



mv **<file>** **<directory>**

Moves file into directory



mv **<file1>** **<file2>** **<directory>**

Moves multiple files into directory



mv ***.txt** **<directory>**

Wildcard moves all ending with .txt



mv **<file>** **<newname>**

Renames file

```
root@Ubuntu:~/jedioder# ls
anakin.txt  clones
root@Ubuntu:~/jedioder# mv anakin.txt /root/sith/
root@Ubuntu:~/jedioder# cd /root/sith/
root@Ubuntu:~/sith# ls
anakin.txt
```


Removing Files and Directories



rm **<file>**

Deletes files



rm -rf **<directory>**

Delete directory and its contents

```
root@Ubuntu:~/jediorder# ls
anakin.txt  clones
root@Ubuntu:~/jediorder# rm anakin.txt
root@Ubuntu:~/jediorder# ls
clones
```

Removing Files and Directories



rmdir <directory>

Deletes empty directories

```
root@Ubuntu:~/jediorder# ls
clones
root@Ubuntu:~/jediorder# rmdir clones
root@Ubuntu:~/jediorder# ls
root@Ubuntu:~/jediorder#
```

Getting Help



man <command>

Display command
documentation

```
root@Ubuntu:~/edorder# man pwd
PWD(1)                                User Commands                                PWD(1)

NAME
  pwd - print name of current/working directory

SYNOPSIS
  pwd [OPTION]...

DESCRIPTION
  Print the full filename of the current working directory.

  -L, --logical
        use PWD from environment, even if it contains symlinks
  -P, --physical
        avoid all symlinks
  --help
        display this help and exit
  --version
        output version information and exit

  If no option is specified, -P is assumed.

NOTE: your shell may have its own version of pwd, which usually supersedes the version described here. Please refer to your shell's documentation for details about the options it supports.

AUTHOR
  Manual page pwd(1) line 1 (press h for help or q to quit)
```

Getting Help



man -k <term> or
apropos <term>
Search by word

```
anakin@localhost:~$ man -k move
aa-remove-unknown (8) - remove unknown AppArmor profiles
add-apt-repository (1) - Adds a repository into the /etc/apt/sources.list or /etc/apt/sources.list.d or removes an ex...
apt-add-repository (1) - Adds a repository into the /etc/apt/sources.list or /etc/apt/sources.list.d or removes an ex...
byobu-disable-prompt (1) - add and remove a nice color prompt to your shell configuration
byobu-enable-prompt (1) - add and remove a nice color prompt to your shell configuration
byobu-prompt (1) - add and remove a nice color prompt to your shell configuration
colrm (1) - remove columns from a file
cut (1) - remove sections from each line of files
delgroup (8) - remove a user or group from the system
deluser (8) - remove a user or group from the system
git-bundle (1) - Move objects and refs by archive
git-clean (1) - Remove untracked files from the working tree
git-mv (1) - Move or rename a file, a directory, or a symlink
git-prune-packed (1) - Remove extra objects that are already in pack files
git-rm (1) - Remove files from the working tree and from the index
git-stripspace (1) - Remove unnecessary whitespace
ipcrm (1) - remove certain IPC resources
kernel-install (8) - Add and remove kernel and initramfs images to and from /boot
lvremove (8) - Remove logical volume(s) from the system
modprobe (8) - Add and remove modules from the Linux Kernel
mv (1) - move (rename) files
psfstriptable (1) - remove the embedded Unicode character table from a console font
purge-old-kernels (1) - remove old kernel and header packages from the system
pvmove (8) - Move extents from one physical volume to another
pvremove (8) - Remove LVM label(s) from physical volume(s)
py3clean (1) - removes .pyc and .pyo files
remove-shell (8) - remove shells from the list of valid login shells
rescan-scsi-bus.sh (8) - script to add and remove SCSI devices without rebooting
rm (1) - remove files or directories
rmdir (1) - remove empty directories
rmmod (8) - Simple program to remove a module from the Linux Kernel
sg_sanitize (8) - remove all user data from disk with SCSI SANITIZE command
unlink (1) - call the unlink function to remove the specified file
update-rc.d (8) - install and remove System-V style init script links
vgreduce (8) - Remove physical volume(s) from a volume group
vgremove (8) - Remove volume group(s)
vgsplit (8) - Move physical volumes into a new or existing volume group
```

Getting Help



info <command>

More detailed info

Links

Table of contents

```
root@Ubuntu:~/jediorder# info ls
Next: dir invocation, Up: Directory listing
10.1 'ls': list directory contents
=====
The 'ls' program lists information about files (of any type, including
directories).  Options and file arguments can be intermixed arbitrarily,
as usual.

For non-option command-line arguments that are directories, by
default 'ls' lists the contents of directories, not recursively, and
omitting files with names beginning with '.'.  For other non-option
arguments, by default 'ls' lists just the file name.  If no non-option
argument is specified, 'ls' operates on the current directory, acting as
if it had been invoked with a single argument of '.'.

By default, the output is sorted alphabetically, according to the
locale settings in effect.(1)  If standard output is a terminal, the
output is in columns (sorted vertically) and control characters are
output as question marks; otherwise, the output is listed one per line
and control characters are output as-is.

Because 'ls' is such a fundamental program, it has accumulated many
options over the years.  They are described in the subsections below;
within each section, options are listed alphabetically (ignoring case).
The division of options into the subsections is not absolute, since some
options affect more than one aspect of 'ls's operation.

Exit status:

0 success
1 minor problems (e.g., failure to access a file or directory not
specified as a command line argument.  This happens when listing a
directory in which entries are actively being removed or renamed.)
2 serious trouble (e.g., memory exhausted, invalid option, failure
to access a file or directory specified as a command line argument
or a directory loop)

Also see "note Common options:".

* Menu:
* Which files are listed::
* What information is listed::
* Sorting the output::
* General output formatting::
* Formatting file timestamps::
* Formatting the file names::

----- Footnotes -----
(1) If you use a non-POSIX locale (e.g., by setting 'LC_ALL' to
```

Getting Help



pinfo <command>

User-friendly version of info
May need to install

```
root@Ubuntu:~/jediorder# pinfo ls
specified as a command line argument. This happens when listing a Up: Directory listing
10.1 'ls': list directory contents
=====

The 'ls' program lists information about files (of any type, including
directories). Options and file arguments can be intermixed arbitrarily,
as usual.

For non-option command-line arguments that are directories, by
default 'ls' lists the contents of directories, not recursively, and
omitting files with names beginning with '.'. For other non-option
arguments, by default 'ls' lists just the file name. If no non-option
argument is specified, 'ls' operates on the current directory, acting as
if it had been invoked with a single argument of '.'.

By default, the output is sorted alphabetically, according to the
locale settings in effect.(1) If standard output is a terminal, the
output is in columns (sorted vertically) and control characters are
output as question marks; otherwise, the output is listed one per line
and control characters are output as-is.

Because 'ls' is such a fundamental program, it has accumulated many
options over the years. They are described in the subsections below;
within each section, options are listed alphabetically (ignoring case).
The division of options into the subsections is not absolute, since some
options affect more than one aspect of 'ls's operation.

Exit status:

0 success
1 minor problems (e.g., failure to access a file or directory not
specified as a command line argument. This happens when listing a
directory in which entries are actively being removed or renamed.)
2 serious trouble (e.g., memory exhausted, invalid option, failure
to access a file or directory specified as a command line argument
or a directory loop)

Also see "note Common options:".

* Menu:

* Which files are listed::
* What information is listed::
* Sorting the output::
* General output formatting::
* Formatting file timestamps::
* Formatting the file names::

----- Footnotes -----

(1) If you use a non-POSIX locale (e.g., by setting 'LC_ALL' to
'en_US'), then 'ls' may produce output that is sorted differently than
Viewing line 33/36, 34.
```

Acquiring Basic System Information



uname

No flag prints brief OS name

-o prints full OS name

-a prints verbose information

-r prints kernel version

```
root@Ubuntu:~/jediorder# uname
Linux

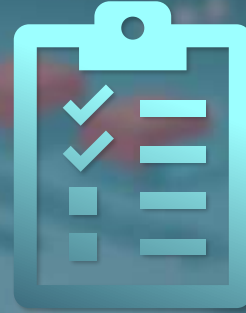
root@Ubuntu:~/jediorder# uname -o
GNU/Linux

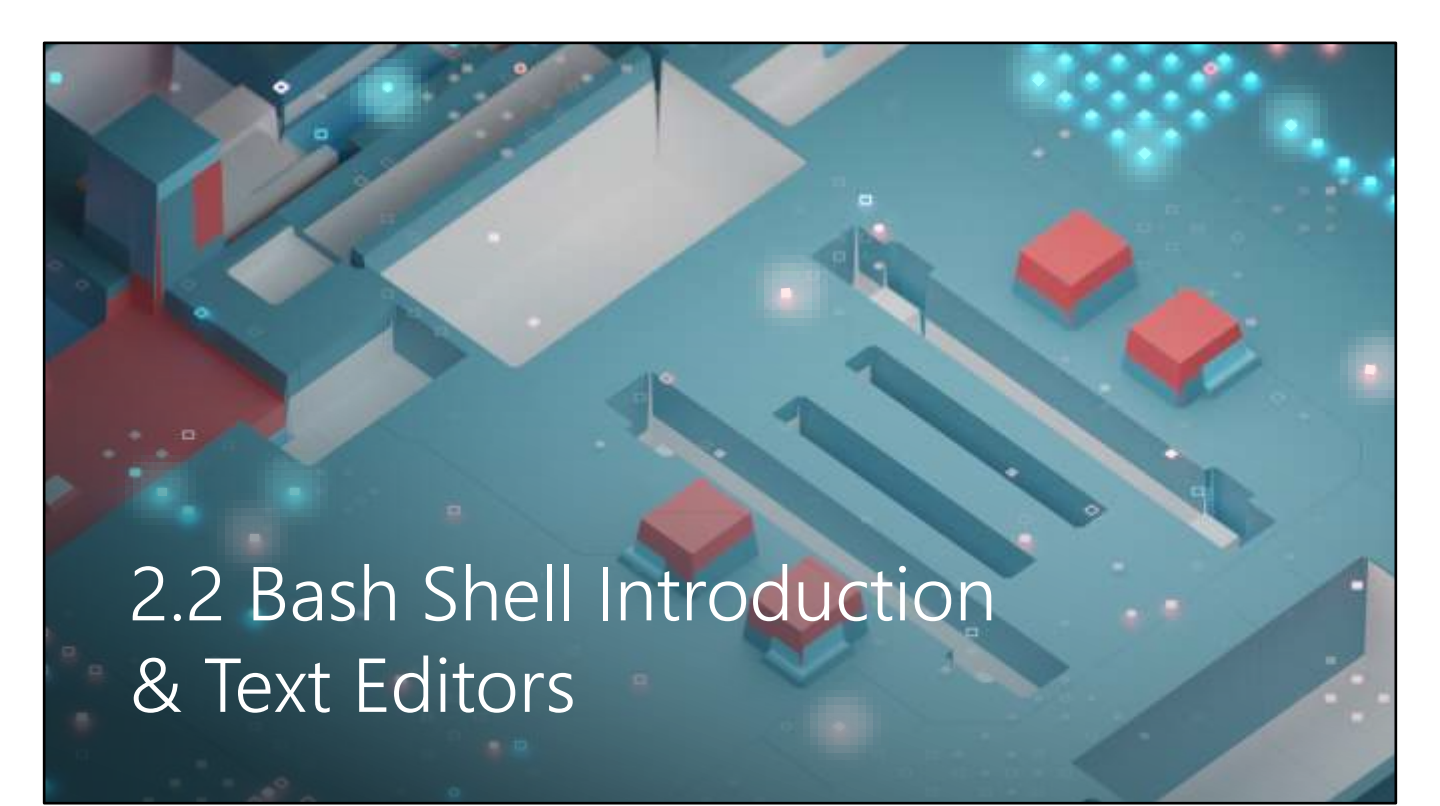
root@Ubuntu:~/jediorder# uname -a
Linux linux 5.13.0-27-generic #31-Ubuntu SMP Sat Jul 5 11:22:11
UTC 2021 x86_64 x86_64 x86_64 GNU/Linux

root@Ubuntu:~/jediorder# uname -r
5.13.0-27-generic
```

Summary

- Introduction to the terminal
- Navigating with the CLI
- Absolute vs relative paths
- Commonly used commands
Syntax





2.2 Bash Shell Introduction & Text Editors

Topics



Shell introduction



Text editors



Scripting introduction



Bash configuration files

What is a Shell?

Shell

User interface program

Command line interpreter

Programming language



Terminal



Command Prompt
App

Bash

Bash = Bourne Again Shell

Default shell in most instances

```
anakin@localhost:~$ echo $SHELL  
/bin/bash
```

Text Editors

nano

Single-mode interface

Ctrl – g = help

Ctrl – o = save

Ctrl – x = exit

Prompt for saving



Text Editors

$$v_i(m)$$

Command mode

i = Switch to Insert mode

dd = Delete line

u = Undo

Ctrl + r = Redo

:q = Quit (gives message if unsaved)

:q! = Quits without saving

:w = Save

:wq = Save and quit

Insert mode

Write output / script

Esc to switch to Command mode

```
-- INSERT --
```

Text Editors

vimtutor

Built-in tutorial

```
~~~~~
Lesson 1.1:  MOVING THE CURSOR

** To move the cursor, press the h,j,k,l keys as indicated. **
      ^
      k      Hint:  The h key is at the left and moves left.
    < h      l >      The l key is at the right and moves right.
      j      The j key looks like a down arrow.
      v

1. Move the cursor around the screen until you are comfortable.

2. Hold down the down key (j) until it repeats.
   Now you know how to move to the next lesson.

3. Using the down key, move to lesson 1.2.

NOTE: If you are ever unsure about something you typed, press <ESC> to place
      you in Normal mode.  Then retype the command you wanted.

NOTE: The cursor keys should also work.  But using hjkl you will be able to
      move around much faster, once you get used to it.  Really!

~~~~~
```

Scripting

`vim <filename>.sh`

.sh (Shell script)

`#!`

Shebang

`/bin/bash`

Shell to use

Python

Go

Bash

```
anakin@localhost:~$ nano example.sh
```

```
anakin@localhost:~$ vim example2.sh
```

```
#! /bin/bash
```


Configuration Files

/etc/profile

Read during

login

su

sudo

System-wide configuration
file for interactive shells

```
anakin@localhost:~$ cat /etc/profile
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).

if [ "${PS1-}" ]; then
  if [ "${BASH-}" ] && [ "$BASH" != "/bin/sh" ]; then
    # The file bash.bashrc already sets the default PS1.
    # PS1='\h:\w\$ '
    if [ -f /etc/bash.bashrc ]; then
      . /etc/bash.bashrc
    fi
  else
    if [ "$(id -u)" -eq 0 ]; then
      PS1='# '
    else
      PS1='$ '
    fi
  fi
fi

if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
  unset i
fi
```

Configuration Files

bashrc

rc = "run command"
Interactive shells
Non-interactive shells

Can add customization
/etc/bashrc affects all users
~/.bashrc affects single user
Aliases
Colors

```
anakin@localhost:~$ cat .bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
  *i*) ;;
  *) return;;
esac

# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
HISTCONTROL=ignoreboth

# append to the history file, don't overwrite it
shopt -s histappend

# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000

# check the window size after each command and, if necessary,
# update the values of LINES and COLUMNS.
shopt -s checkwinsize

# If set, the pattern "***" used in a pathname expansion context will
# match all files and zero or more directories and subdirectories.
#shopt -s globstar

# make less more friendly for non-text input files, see lesspipe(1)
[ -x /usr/bin/lesspipe ] && eval "$(SHELL=/bin/sh lesspipe)"

# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "${debian_chroot:-}" ] && [ -r /etc/debian_chroot ]; then
    debian_chroot=$(cat /etc/debian_chroot)
fi
```

Configuration Files

`.bash_profile`

Activated every login

```
[root@centos ~]#cat .bash_profile  
# .bash_profile
```

```
# Get the aliases and functions  
if [ -f ~/.bashrc ]; then  
    . ~/.bashrc  
fi
```

```
# User specific environment and startup programs
```

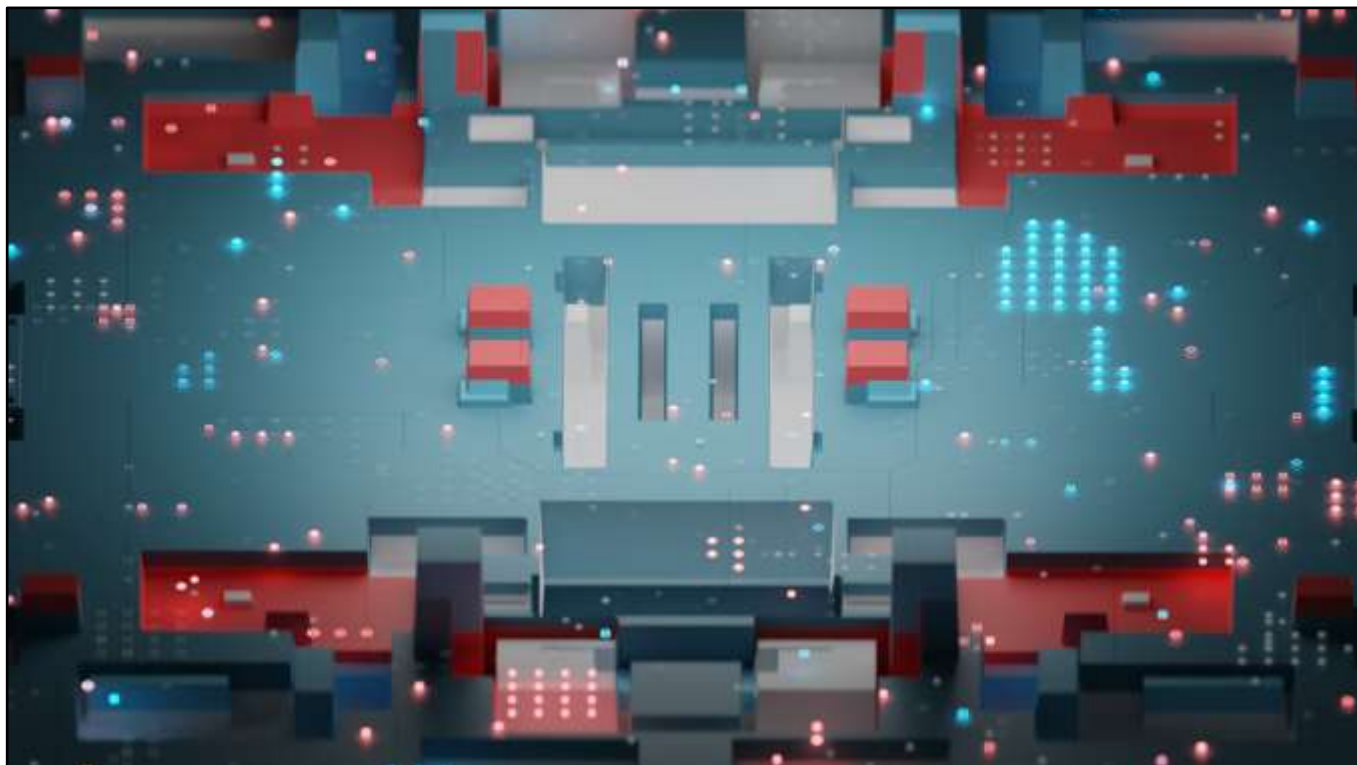
Summary

Shell introduction

Text editors

Scripting introduction

Bash configuration files



©2023 by StormWind LLC. All rights reserved.

<https://t.me/learningnets>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Understanding the Power of Sudo

©2023 by StormWind LLC. All rights reserved.

<https://t.me/learningnets>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Topics

sudo

visudo

sudoers file

What is Sudo?

su

Switches user to root (by default)

Root password

su -

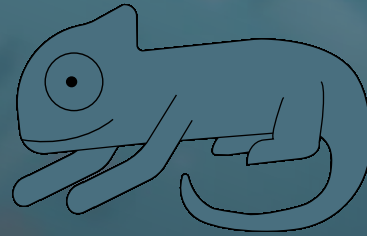
sudo ("substitute user do")

Run command as different user

Root by default

Other users

User password



SUDO

What is Sudo?

sudo group

User must be added to sudo group for sudo access

```
joshua@Ubuntu:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
joshua@Ubuntu:~$ sudo cat /etc/sudoers
[sudo] password for joshua:
joshua is not in the sudoers file. This incident will be reported.
```

```
root@Ubuntu:/home/joshua# cat /etc/group | grep sudo
sudo:x:27:
root@Ubuntu:/home/joshua# usermod joshua -aG sudo
root@Ubuntu:/home/joshua# cat /etc/group | grep sudo
sudo:x:27:joshua
```

Sudo

visudo

/etc/sudoers

Privileges

%sudo **ALL=(ALL:ALL) ALL**

% = Group

Host or Servers

Users:Groups

Commands

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@include /etc/sudoers.d
```

Sudo

sudo !!

Reruns last command with sudo

```
joshua@Ubuntu:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
joshua@Ubuntu:~$ sudo !!
sudo cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
```

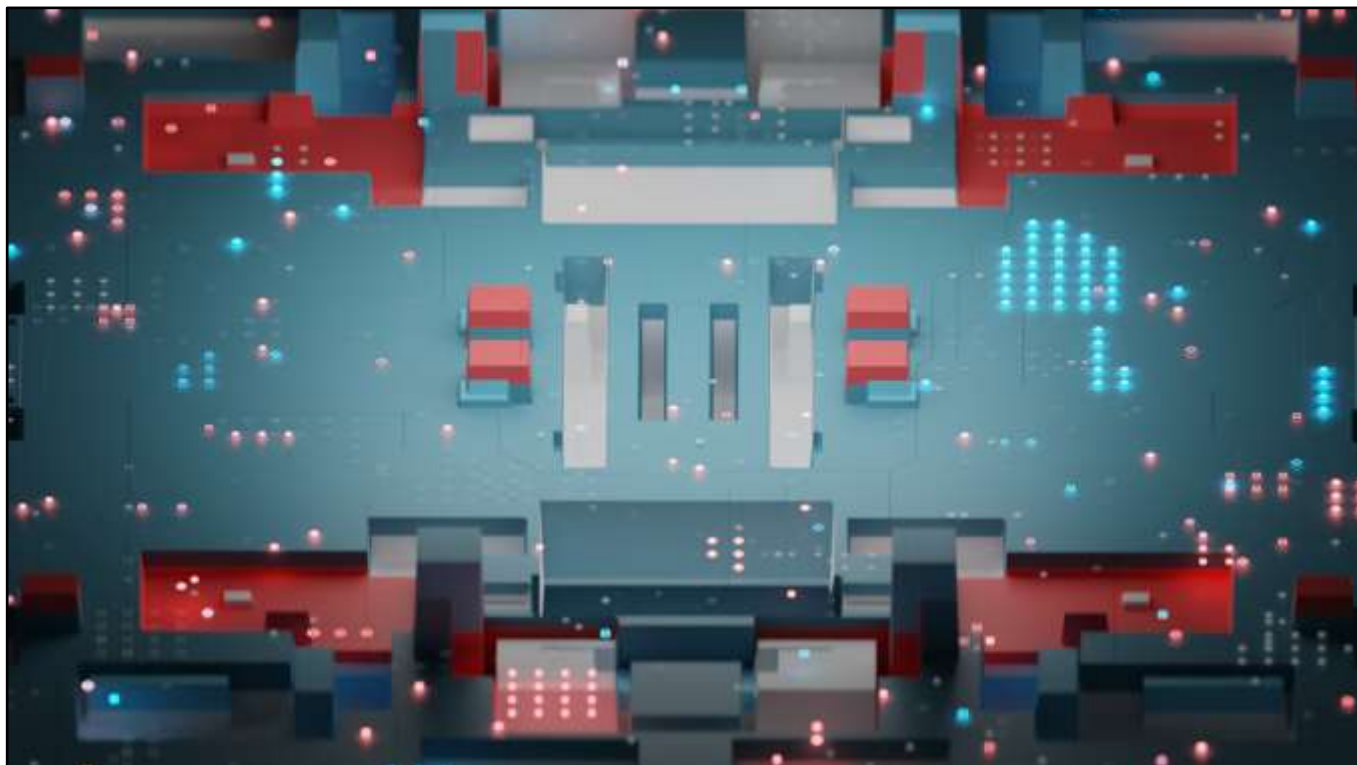
Summary

sudo

visudo

sudoers file

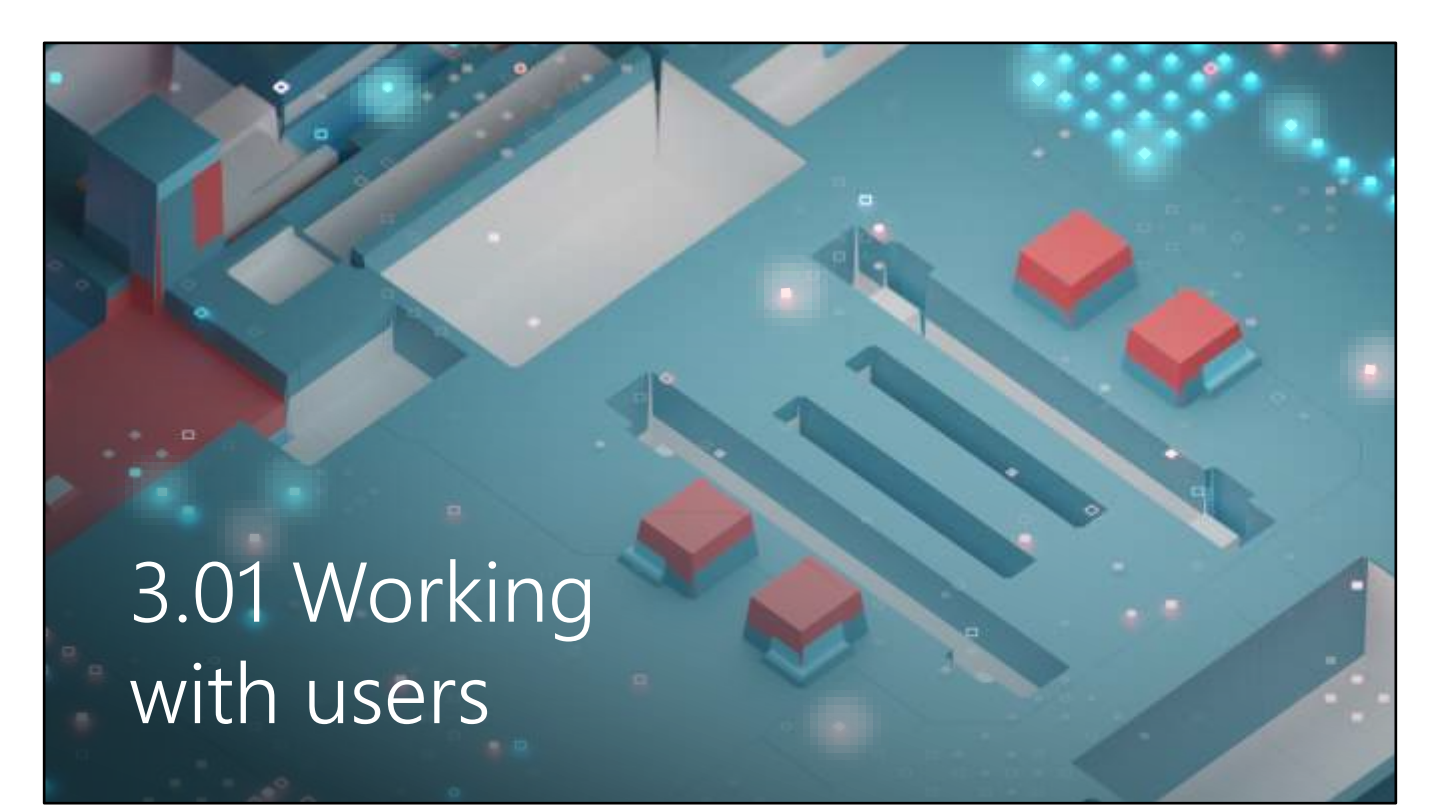




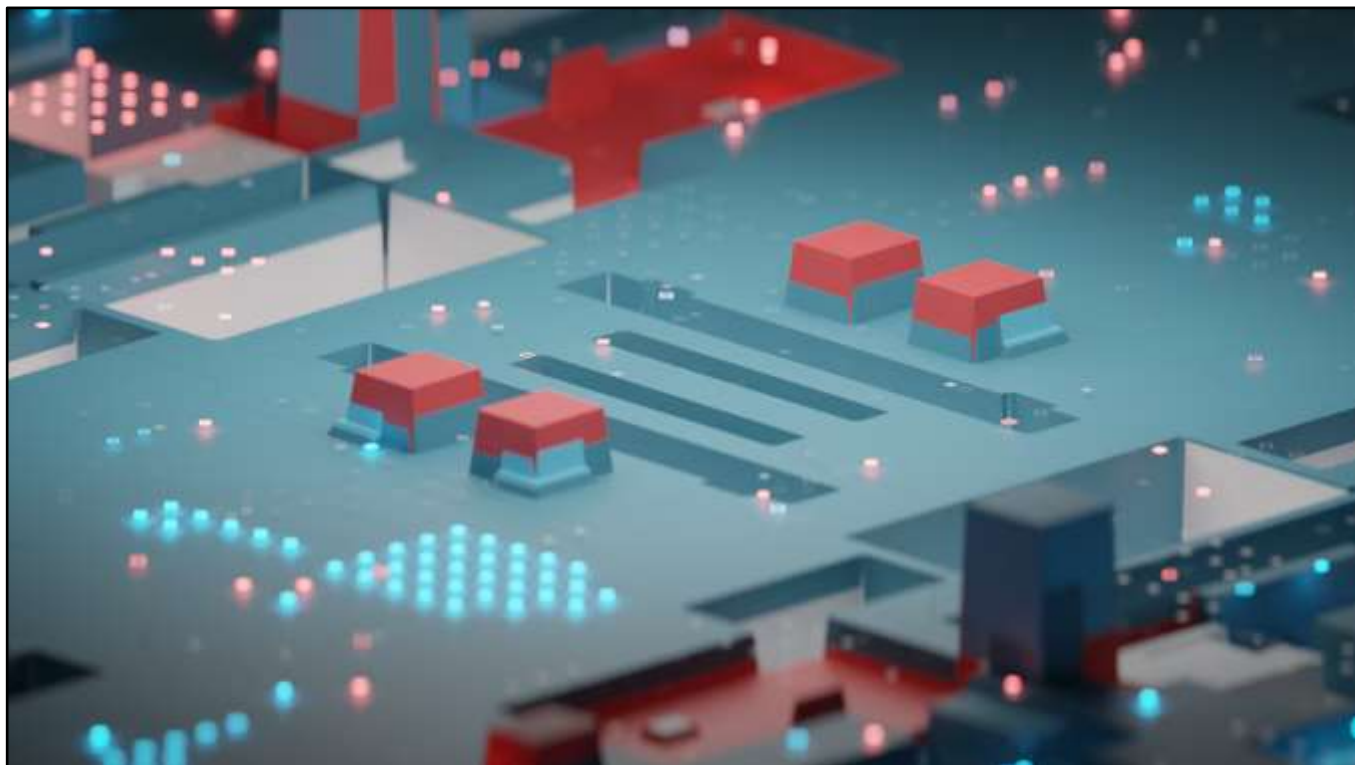
©2023 by StormWind LLC. All rights reserved.

<https://t.me/learningnets>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



3.01 Working with users



©2023 by StormWind LLC. All rights reserved.

<https://t.me/learningnets>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Topics

Users

- Creating accounts
- Setting passwords
- Managing users
- Configuration files
- Logging

Creating Users

useradd

- d Specify home directory
- e Disable date
- f Days after password expiration account will be disabled
- g Primary group
- G Secondary groups (separate with a comma)
- m Creates a home directory
- u Manually pick user ID

```
joshua@Ubuntu:~$ sudo useradd ben -c General -f 3 -m
joshua@Ubuntu:~$ cat /etc/passwd | grep ben
ben:x:1010:1010:General:/home/ben:/bin/sh
```

Creating Passwords

passwd

- l Locks account; leaves password
- u Unlocks account
- d Removes password
- n Minimum number of days required before password can be changed
- x Maximum number of days before a password must be changed
- w Number of days warning will be issued before expiration
- i Days password is expired before disabling account
- S Password aging information

```
joshua@Ubuntu:~$ sudo passwd palpatine
New password:
Retype new password:
passwd: password updated successfully
```

Managing Users

chage

- l **<user>**
View password age, expiration
inactive time
- E **<expiration> <user>**
Edit expiration period (-1 for
none)
- m **<minimum days>**
Set minimum password age
- M **<maximum days>**
Set maximum password age

```
joshua@Ubuntu:~$ sudo chage palpatine
Changing the aging information for palpatine
Enter the new value, or press ENTER for the default

Minimum Password Age [0]: 1
Maximum Password Age [99999]: 365
Last Password Change (YYYY-MM-DD) [2022-07-06]:
Password Expiration Warning [7]: 14
Password Inactive [-1]: -1
Account Expiration Date (YYYY-MM-DD) [-1]:
```

Managing Users

```
sudo usermod <username> -s <shell>
```

Change a user's shell

Use /usr/sbin/nologin to prevent logins

```
sudo usermod -aG <group> <user>
```

Add user to a secondary group

```
joshua@Ubuntu:~$ sudo usermod anakin -s /sbin/nologin
joshua@Ubuntu:~$ cat /etc/passwd | grep anakin
anakin:x:1012:1012::/home/anakin:/sbin/nologin
```

Configuration Files

/etc/login.defs
Default settings for
useradd and groupadd

```
#
# Password aging controls:
#
#     PASS_MAX_DAYS   Maximum number of days a password may be used.
#     PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#     PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN         1000
UID_MAX         60000
# System accounts
#SYS_UID_MIN    100
#SYS_UID_MAX    999

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN         1000
GID_MAX         60000
# System accounts
#SYS_GID_MIN    100
#SYS_GID_MAX    999
```

Configuration Files

/etc/passwd

User account information

Fields separated by colon (:)

Username

Password ("x" indicates located elsewhere)

User ID (UID)

Root = 0

Under 500 = system user

Over 1000 = user

Group ID (GID)

Comment

Home directory

Default shell

```
joshua@Ubuntu:~$ tail -n 6 /etc/passwd
mary:x:1006:1006::/home/mary:/bin/sh
frank:x:1007:1007::/home/frank:/bin/sh
joejoe:x:1008:1008::/home/joejoe:/bin/bash
nathan:x:1009:1009::/home/nathan:/bin/sh
ben:x:1010:1010:General:/home/ben:/bin/sh
palps:x:1011:1011::/home/palps:/bin/bash
```

Configuration Files

/etc/shadow

Password information

Fields

Username

Password hash

Last modified (epoch date)

Minimum days

Maximum days

Warning days

Inactive

Expiration date

Final : Reserved and unused

```
joshua@Ubuntu:~$ sudo tac /etc/shadow
palpatine:$y$j9T$DvRJxX73wOVXTQY03/8iz0$MR
k3z6XLUayJ6dNccWjRGYiboiah054LFmOAE2JNSGD:
19179:1:365:14:::
ben:!:19179:0:99999:7:3::
joshua:$y$j9T$NJqNoSDHrAHZQYCeG5nVM.$tXyM2
NMozVC1H0c0WvZC/Kur/VzyGBV0CgPPIbxYjp2:191
79:0:99999:7:::
nathan:$y$j9T$5EbWL82TxqucMvBobJum3/$6fX0v
2b4UylLoEGd.sAGEiExrtm8jbbhtegPcHELK1v/:191
78:0:99999:7:::
mary:!:19178:0:99999:7:::
frank:!:19178:0:99999:7:::
_flatpak:*:19167:0:99999:7:::
```



Managing Users



usermod

-aG

Add to Group

-d

Change home directory

-L

Locks user

-U

Unlocks user

-s

Change Shell

```
joshua@Ubuntu:~$ sudo usermod -aG sudo palpatine
joshua@Ubuntu:~$ sudo groups palpatine
palpatine : palpatine sudo
```

Managing Users



mkhomedir_helper

Creates home directory

```
joshua@Ubuntu:~$ ls -l /home | grep "^d"
drwxr-x--- 2 ben      ben      4096 Jul  6 14:19 ben
drwxr-x--- 2 joshua   sudo      4096 Jul  6 14:09 joshua
drwxr-x--- 2 palpatine palpatine 4096 Jul  6 14:31 palpatine
joshua@Ubuntu:~$ sudo mkhomedir_helper anakin
joshua@Ubuntu:~$ ls -l /home | grep "^d"
drwxr-xr-x 2 anakin   anakin   4096 Jul  6 15:41 anakin
drwxr-x--- 2 ben      ben      4096 Jul  6 14:19 ben
drwxr-x--- 2 joshua   sudo      4096 Jul  6 14:09 joshua
drwxr-x--- 2 palpatine palpatine 4096 Jul  6 14:31 palpatine
```

Configuration Files



/etc/skel

Files are automatically copied over to new user directory

```
joshua@Ubuntu:~$ ls -a /etc/skel  
.  ..  .bash_logout  .bashrc  .profile
```

Managing Users

whoami

View your username

who

View who is logged in

w

View who is logged in
and what they are
doing

```
joshua@Ubuntu:~$ whoami
joshua
joshua@Ubuntu:~$ who
root    ttyS0      2022-06-14 19:27
root    tty1       2022-06-17 14:09
root    pts/0      2022-07-06 12:07 (
joshua  pts/1      2022-07-06 15:52 (
joshua@Ubuntu:~$ w
 15:52:43 up 21 days, 20:31,  4 users,  load average: 0.06, 0.01, 0.00
USER    TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
root    ttyS0    -             14Jun22 11days 0.55s   0.54s -bash
root    tty1     -             17Jun22 11days 43:06   0.00s xinit
/etc/xdg/xfce4/xinitrc -- /etc/X11/xinit/xserverrc vt1
root    pts/0    -             12:07    1.00s   0.29s   0.00s w
joshua  pts/1    -             15:52    24.00s  0.01s   0.01s -bash
```

Log authentication errors

pam_tally2

Deprecated in PAM 1.5.0

Replaced with pam_faillock

pam_faillock

/etc/security/faillock.conf

Config file

/var/run/faillock

Files logging failures

Removing Users

userdel

Deletes user

/etc/passwd

/etc/shadow

-r

Removes home directory

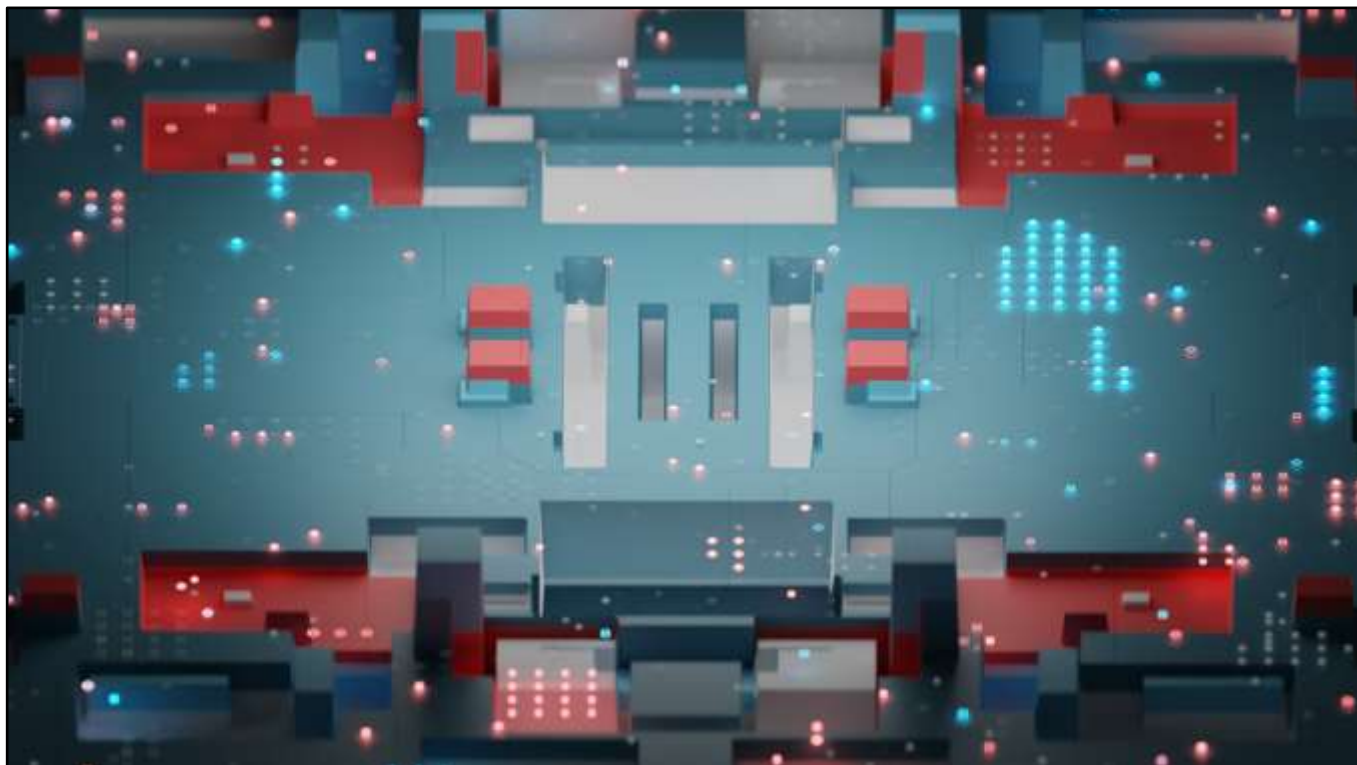
```
joshua@Ubuntu:~$ sudo userdel nathan
```

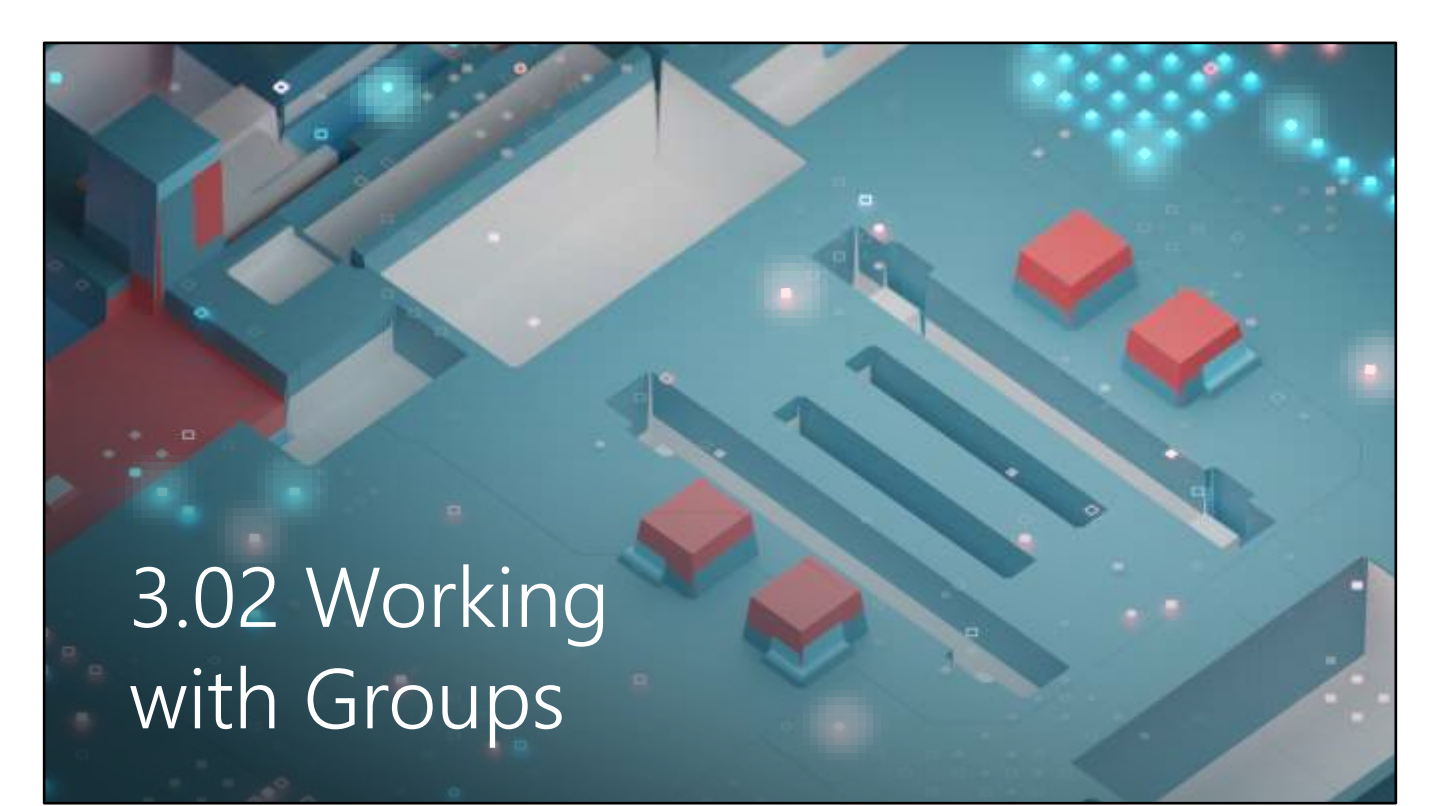
Review

Users

- Creating accounts
- Setting passwords
- Managing users
- Configuration files
- Logging







3.02 Working with Groups

Topics

-  Primary and secondary groups
-  Creating groups
-  Managing groups
-  Deleting groups
-  Group configuration files
-  Wheel group

Groups



Group

Collection of users assigned specific permissions

Primary group

Each user has a primary group

Only one per user

Secondary group

Optional

Limit of 15 per user

Creating Groups



groupadd <group>

Creates new group



Common options

-g

Let's you choose group ID.

-r

Creates system group

```
joshua@Ubuntu:~$ sudo groupadd Mandalorian
joshua@Ubuntu:~$ cat /etc/group | grep Mandalorian
Mandalorian:x:1013:
```

Managing Groups



groupmod

Modify group



Common options

-g

Change group ID

-n

Change group name

```
joshua@Ubuntu:~$ sudo groupmod Mandalorian -g 2356
joshua@Ubuntu:~$ cat /etc/group | grep Mandalorian
Mandalorian:x:2356:
```

Managing Groups



Adding user to a group

```
usermod -aG <group> <user>
```

```
joshua@Ubuntu:~$ sudo usermod -aG Mandalorian Grogu
joshua@Ubuntu:~$ cat /etc/group | grep Mandalorian
Mandalorian:x:2356:Din,Grogu
```

Managing Groups



Group permissions

Allow certain commands

```
sudo visudo
```

```
# Mandalorian Group Permissions
%Mandalorian ALL=(ALL:ALL) /usr/bin/useradd,/usr/bin/groupadd
```

Managing Groups



id <user>

Displays users' group IDs

```
joshua@Ubuntu:~$ id
uid=1004(joshua) gid=27(sudo) groups=27(sudo)
joshua@Ubuntu:~$ sudo id anakin
uid=1012(anakin) gid=1012(anakin) groups=1012(anakin)
```


Deleting Groups



groupdel <group>

Deletes a group

```
joshua@Ubuntu:~$ sudo groupdel Mandalorian
joshua@Ubuntu:~$ sudo groups Din
Din : Din
joshua@Ubuntu:~$ cat /etc/group | grep Mandalorian
```

Configuration Files



/etc/group

Group information

Group name

Group password

Group ID

Group members

```
joshua@Ubuntu:~$ tail -n 4 /etc/group
joshua:x:1004:
frank:x:1007:
mary:x:1008:
anakin:x:1012:
```

Wheel Group



wheel

Used in Red Hat systems; akin the sudo group

Grants administrator access to users in this group

Review



Creating groups



Managing groups



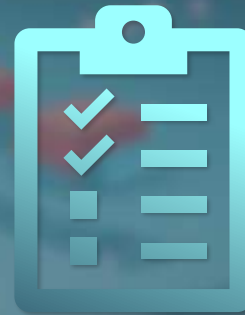
Deleting groups



Group configuration files



Wheel group





4.01 Understanding Permissions

Topics



Understanding permissions



Sticky bit



Reading permissions



Attributes



Changing permissions



umask

Understanding Permissions

```
joshua@Ubuntu:~$ ls -l | grep Iownthis.txt  
-rw-r--r-- 1 joshua sudo 0 Jul  6 17:22 Iownthis.txt
```

New Files

Creator of file/directory is the owner

Read = r

Write = w

Execute = x

Reading Permissions

```
joshua@Ubuntu:~$ ls -l
total 4
-rw-r--r-- 1 joshua sudo    0 Jul  6 17:22 Iownthis.txt
-rwxr-xr-x 2 joshua sudo 4096 Jul  6 17:35 Pictures
```

ls -l

File type

Regular file = -

Directory = d

Symbolic Link = l

Block Device = b

Character Device = c

Reading Permissions

```
joshua@Ubuntu:~$ ls -l
total 4
-rw-r--r-- 1 joshua sudo    0 Jul  6 17:22 Iownthis.txt
drwxr-xr-x 2 joshua sudo 4096 Jul  6 17:35 Pictures
```

ls -l

Owner permissions

Read = r

Write = w

Execute = x

Reading Permissions

```
joshua@Ubuntu:~$ ls -l
total 4
-rw-r--r-- 1 joshua sudo    0 Jul  6 17:22 Iownthis.txt
drwxr-xr-x 2 joshua sudo 4096 Jul  6 17:35 Pictures
```

ls -l

Group permissions

Read = r

Write = w

Execute = x

Reading Permissions

```
joshua@Ubuntu:~$ ls -l
total 4
-rw-r--r-- 1 joshua sudo  0 Jul  6 17:22 Iownthis.txt
Drwxr-xr-x 2 joshua sudo 4096 Jul  6 17:35 Pictures
```

ls -l

Other permissions

Read = r

Write = w

Execute = x

Reading Permissions

```
joshua@Ubuntu:~$ ls -l
total 4
-rw-r--r-- 1 joshua sudo    0 Jul  6 17:22 Iownthis.txt
drwxr-xr-x 2 joshua sudo 4096 Jul  6 17:35 Pictures
joshua@Ubuntu:~$ mkdir Pictures/Screenshots
joshua@Ubuntu:~$ ls -l
total 4
-rw-r--r-- 1 joshua sudo    0 Jul  6 17:22 Iownthis.txt
drwxr-xr-x 3 joshua sudo 4096 Jul  6 18:02 Pictures
```

ls -l

Link count

Files = 1

Directories = 2 plus
amount of subdirectories

Reading Permissions

```
joshua@Ubuntu:~$ ls -l
total 4
-rw-r--r-- 1 joshua sudo  0 Jul  6 17:22 Iownthis.txt
drwxr-xr-x 2 joshua sudo 4096 Jul  6 17:35 Pictures
```

ls -l

Owner username

Reading Permissions

```
joshua@Ubuntu:~$ ls -l
total 4
-rw-r--r-- 1 joshua sudo  0 Jul  6 17:22 Iownthis.txt
drwxr-xr-x 2 joshua sudo 4096 Jul  6 17:35 Pictures
```

ls -l
Group

Reading Permissions

```
joshua@Ubuntu:~$ ls -l
total 4
-rw-r--r-- 1 joshua sudo 0 Jul 6 17:22 Iownthis.txt
drwxr-xr-x 2 joshua sudo 4096 Jul 6 17:35 Pictures
```

ls -l

File size in bytes

Reading Permissions

```
joshua@Ubuntu:~$ ls -l
total 4
-rw-r--r-- 1 joshua sudo    0 Jul  6 17:22 Iownthis.txt
drwxr-xr-x 2 joshua sudo 4096 Jul  6 17:35 Pictures
```

ls -l

Modification date/time

Reading Permissions

```
joshua@Ubuntu:~$ ls -l
total 4
-rw-r--r-- 1 joshua sales    0 Jul  6 17:22 Iownthis.txt
drwxr-xr-x 2 joshua sales 4096 Jul  6 17:35 Pictures
```

s

ls -l

File or directory name

Changing Permissions



chmod - Change permissions on file/directory

Symbolic Mode

Section Changed

u = User

g = Group

o = Other

a = All

Operator

+ (Add permission)

- (Remove Permission)

= (Re-assign Permission)

Permission

r = Read

w = Write

x = Execute

```
palpatine@Ubuntu:~$ ls -l Clones/order66.txt
-rw-r--r-- 1 Sifo sudo 0 Jul  6 20:08 Clones/order66.txt

palpatine@Ubuntu:~$ chmod u+x Clones/order66.txt

palpatine@Ubuntu:~$ ls -l Clones/order66.txt
-rwxr--r-- 1 sifo sudo 0 Jul  6 20:08 Clones/order66.txt

palpatine@Ubuntu:~$ chmod o-r Clones/order66.txt

palpatine@Ubuntu:~$ ls -l Clones/order66.txt
-rwxr----- 1 sifo sudo 0 Jul  6 20:08 Clones/order66.txt
```

Changing Permissions



chmod - Change permissions on file/directory

Octal Formatting

- 0 = No Permission
- 1 = Execute
- 2 = Write
- 3 = Write + Execute
- 4 = Read
- 5 = Read + Execute
- 6 = Read + Write
- 7 = All Permission

```
palpatine@Ubuntu:~$ chmod 760 Clones/order66.txt
```

User Group Other

Changing Permissions



umask

Sets default file/directory permissions

Directory max = 777

File max = 666

Automatic execute is not allowed

Amount will be inverse of octal value

Default value is 0002

umask Examples

rw- r-- ---

U=6 G=4 O=0

File umask =
666-640 = 026

```
joshua@Ubuntu:~$ umask
0022
joshua@Ubuntu:~$ touch ex_1
joshua@Ubuntu:~$ ls -l | grep ex_1
-rw-r--r-- 1 joshua sudo    0 Jul  6 20:22 ex_1
joshua@Ubuntu:~$ umask 026
joshua@Ubuntu:~$ touch ex_2
joshua@Ubuntu:~$ ls -l | grep ex_2
-rw-r----- 1 joshua sudo    0 Jul  6 20:22 ex_2
```

umask Examples

rwX **rw-** **rw-**
U=7 **G=6** **O=6**

Directory umask =
777-766 = 011

```
joshua@Ubuntu:~$ umask 026  
  
joshua@Ubuntu:~$ mkdir ex_directory  
  
joshua@Ubuntu:~$ ls -l | grep ex_directory  
drwxrw-rw- 2 joshua sudo 4096 Jul  6 20:25  
ex_directory
```

Protections



Sticky bit - Prevents deletion of directory and files

Only root and owner can delete

Does nothing if put on a file

Indicated by a "t" in *other* category

```
joshua@Ubuntu:/home$ ls -l | grep shared
drwxrwxrwt 2 root  root  4096 Jul  6 21:30 shared
```

```
sith@Ubuntu:/home$ rm shared/important
rm: cannot remove 'shared/important': Operation not
permitted
```

Protections



Sticky bit - Octal Formatting

`chmod 1777 <directory>`

A "1" before basic permissions will activate sticky bit

```
joshua@Ubuntu:/home$ sudo chmod 1777 shared
```


Protections



Sticky bit - Symbolic mode

`chmod +t <directory>`

Adds sticky bit

`chmod -t <directory>`

Removes sticky bit

```
joshua@Ubuntu:/home$ sudo chmod +t shared
```

```
joshua@Ubuntu:/home$ sudo chmod -t shared
```

Changing Permissions



chown <user><:group> <object>

Changes ownership

Username

:Group

Username:group

```
joshua@Ubuntu:/home$ ls -l | grep OSI_Model
-rw-r--r-- 1 root  root   99 Jun 13 19:04 OSI_Model

joshua@Ubuntu:/home$ sudo chown Grogu OSI_Model

joshua@Ubuntu:/home$ ls -l | grep OSI_Model
-rw-r--r-- 1 Grogu root   99 Jun 13 19:04 OSI_Model
```

Changing Permissions



chgrp <group> <object>

Changes group associated with file or directory

```
joshua@Ubuntu:/home$ sudo chgrp Mandalorian  
OSI_Model  
joshua@Ubuntu:/home$ ls -l | grep OSI_Model  
-rw-r--r-- 1 Grogu Mandalorian    99 Jun 13  
19:04 OSI_Model
```

Changing Permissions



Order66



Emperor



Clones



Anakin



Masters

```
emperor@Ubuntu:~$ ls -l
total 4
-rwxrwx---+ 1 emperor Clones 99 Jun 13 19:04 order66.txt
```

Changing Permissions

chmod

SUID

Executable runs as owner instead of user

```
chmod u+s <filename>
```

Example:

```
/usr/bin/passwd
```

SGID

Executable runs as group owner instead of user

Sub-directories and files inherit parent group

```
chmod g+s <directory>
```

Changing Permissions

FACLs - ACL for files/directories
getfacl shows files permissions

```
emperor@Ubuntu:~$ getfacl order66.txt
# file: order66.txt
# owner: emperor
# group: Clones
user::rwx
group::rwx
other::---
```

Changing Permissions

FACLs

setfacl adds and deletes FACLs

- m = modify
- x = remove
- u:<username>
- g:<group>

Changing Permissions

1 `anakin@Ubuntu:/home/emperor$ cat order66.txt`
`cat: order66.txt: Permission denied`

2 `emperor@Ubuntu:~$ setfacl -m u:anakin:rwx`
`order66.txt`

4 `anakin@Ubuntu:/home/emperor$ cat order66.txt`
`Dew it`
`Dew it now`
`$`

3 `emperor@Ubuntu:~$ getfacl order66.txt`
`# file: order66.txt`
`# owner: emperor`
`# group: Clones`
`user:anakin:rwx`
`group::rwx`
`other::---`



Attributes

Common file attributes

- e Don't fragment file
- i Cannot be modified
- a Append only
- s Secure deletion

Attributes

lsattr

List file attributes

-l will read out the attribute

chattr

Change file attributes

+ attribute to add

- attribute to delete

```
joshua@Ubuntu:~$ lsattr
-----e----- ./order66.txt
-----e----- ./ex_1
-----e----- ./ex_2
-----e----- ./Pictures
-----e----- ./Iownthis.txt
-----e----- ./Clones
```

Review

Understanding permissions

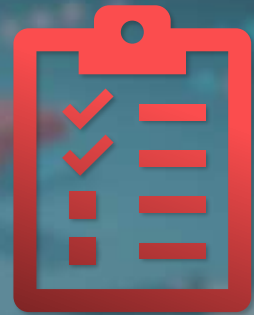
Reading permissions

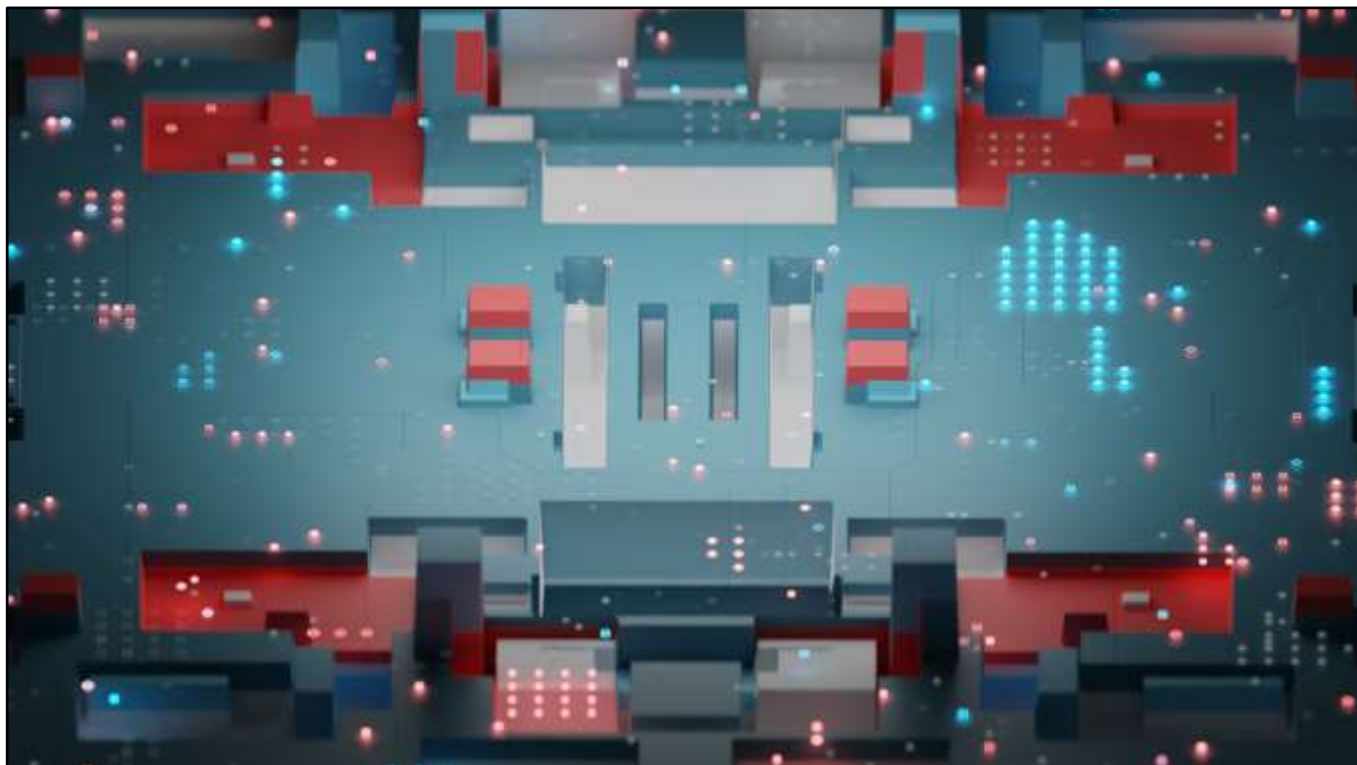
Changing permissions

umask

Sticky bit

Attributes





An isometric illustration of a cityscape at night. The scene features various buildings in shades of blue, grey, and red. In the foreground, there are several red, cube-like structures. The background is filled with glowing blue and red lights, suggesting a vibrant urban environment. The overall style is modern and digital.

4.02 SELinux & AppArmor

Topics

- Intro to SELinux
- Access control
- SELinux modes
- SELinux booleans
- SELinux logs
- Intro to AppArmor
- Editing AppArmor profiles

Security Enhanced Linux (SELinux)

What does it do?

- Distinct separation of services
- Granular level of access control
- Administratively-defined policy
- Robust privilege escalation protection

What doesn't it do?

- Antimalware
- Replacement for other security mechanisms
- All-encompassing security solution

Access Control

Discretionary Access Control (DAC)

Users control permissions on their directory and files

Mandatory Access Control (MAC)

Only the admin can control access

Even if user changes RWX, the MAC policy can stop access to it

Format

user:role:type:level

```
root@CENTOS ~]# ls -lZ
total 4
drwxr-xr-x. 2 root root unconfined_u:object_r:admin_home_t:s0 4096 Jun 16 14:43 Documents
-rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0 0 Jun 16 16:23 file1.txt
-rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0 0 Jun 16 16:23 file2.txt
-rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0 0 Jun 16 16:23 file3.txt
```


SELinux Modes

Enabled

Enforcing

Blocking and logging

Permissive

Logging

/var/log/audit/audit.log

Disabled

```
[root@CENTOS ~]# cat /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux/#getting-started-with-selinux-states-and-modes
#
# NOTE: In earlier Fedora kernel builds, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=enforcing

# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected.
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

SELinux Modes

Change modes

/etc/selinux/config

setenforce <bool>

1 - Enforcing

0 - Permissive

```
[root@CENTOS ~]# cat /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux/#getting-started-with-selinux-states-and-modes
#
# NOTE: In earlier Fedora kernel builds, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=enforcing

# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

```
[root@CENTOS ~]# setenforce enforcing
[root@CENTOS ~]# getenforce
Enforcing

[root@CENTOS ~]# setenforce permissive
[root@CENTOS ~]# getenforce
Permissive

[root@CENTOS ~]# setenforce 1
[root@CENTOS ~]# getenforce
Enforcing

[root@CENTOS ~]# setenforce 0
[root@CENTOS ~]# getenforce
Permissive
```

SELinux Modes

getenforce

SELinux state

sestatus

Status

Policy

Current mode

Config file mode

```
[root@CENTOS ~]# getenforce
Enforcing
```

```
[root@CENTOS ~]# sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:         enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     33
```

SELinux Booleans

setsebool

Modify an SELinux boolean

getsebool

View an SELinux boolean

httpd_enable_cgi --> off



```
[root@CENTOS ~]# setsebool -P httpd_enable_cgi off
[root@CENTOS ~]#
[root@CENTOS ~]# getsebool -a | grep httpd_enable_cgi
httpd_enable_cgi --> off
```

SELinux Booleans

semanage boolean -l

Provides:

Current state

Default state

Description

```
[root@CENTOS ~]# semanage boolean -l
```

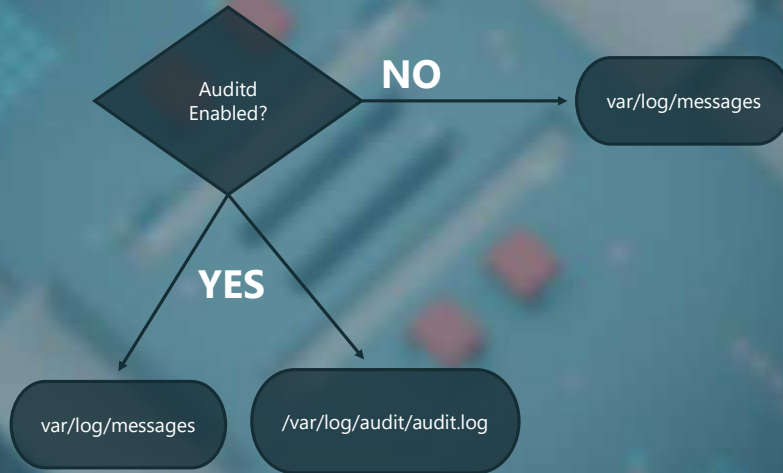
SELinux boolean	State	Default	Description
abrt_anon_write	(off , off)		Allow abrt to anon write
abrt_handle_event	(off , off)		Allow abrt to handle event
abrt_upload_watch_anon_write	(on , on)		Allow abrt to upload watch anon write
antivirus_can_scan_system	(off , off)		Allow antivirus to can scan system
antivirus_use_jit	(off , off)		Allow antivirus to use jit
auditadm_exec_content	(on , on)		Allow auditadm to exec content
authlogin_nsswitch_use_ldap	(off , off)		Allow authlogin to nsswitch use ldap
authlogin_radius	(off , off)		Allow authlogin to radius
authlogin_yubikey	(off , off)		Allow authlogin to yubikey
awstats_purge_apache_log_files	(off , off)		Allow awstats to purge apache log files
boinc_execmem	(on , on)		Allow boinc to execmem
cdrecord_read_content	(off , off)		Allow cdrecord to read content
cluster_can_network_connect	(off , off)		Allow cluster to can network connect
cluster_manage_all_files	(off , off)		Allow cluster to manage all files
cluster_use_execmem	(off , off)		Allow cluster to use execmem
cobbler_anon_write	(off , off)		Allow cobbler to anon write
cobbler_can_network_connect	(off , off)		Allow cobbler to can network connect
cobbler_use_cifs	(off , off)		Allow cobbler to use cifs
cobbler_use_nfs	(off , off)		Allow cobbler to use nfs
collectd_tcp_network_connect	(off , off)		Allow collectd to tcp network connect
colord_use_nfs	(off , off)		Allow colord to use nfs
condor_tcp_network_connect	(off , off)		Allow condor to tcp network connect
conman_can_network	(off , off)		Allow conman to can network
conman_use_nfs	(off , off)		Allow conman to use nfs
cron_can_relabel	(off , off)		Allow cron to can relabel
cron_system_cronjob_use_shares	(off , off)		Allow cron to system cronjob use shares
cron_userdomain_transition	(on , on)		Allow cron to userdomain transition

Troubleshooting SELinux

setroubleshootd

Daemon that listens for audit events
and runs various actions after analysis

Troubleshooting SELinux



AppArmor

Akin to SELinux; used in Debian distributions

systemctl status apparmor

Status

Enabled on boot?

systemctl start apparmor

Starts apparmor

systemctl enable apparmor

Enable on boot

```
root@localhost:~# systemctl status apparmor
• apparmor.service - Load AppArmor profiles
   Loaded: loaded (../apparmor.service; enabled; vendor preset: enabled)
   Active: active (exited) since Tue 2022-06-14 19:21:16 UTC; 2 days ago
     Docs: man:apparmor(7)
           https://gitlab.com/apparmor/apparmor/wikis/home/
   Main PID: 399 (code=exited, status=0/SUCCESS)
    CPU: 28ms

Jun 14 19:21:16 localhost apparmor.systemd[399]: Restarting AppArmor
Jun 14 19:21:16 localhost apparmor.systemd[399]: Reloading AppArmor profiles
Jun 14 19:21:15 localhost systemd[1]: Starting Load AppArmor profiles...
Jun 14 19:21:16 localhost apparmor.systemd[423]: Skipping profile in
/etc/apparmor.d/disable: usr.sbin.rsyslogd
Jun 14 19:21:16 localhost systemd[1]: Finished Load AppArmor profiles.
```


aa-status

aa-status

Shows Profiles enforcing modes

Enforce

Will enforce policies on the profile

Complain

Will not enforce policies but will report them

```
root@localhost:~# aa-status
apparmor module is loaded.
19 profiles are loaded.
18 profiles are in enforce mode.
  /snap/snapd/16010/usr/lib/snapd/snap-confine
  /snap/snapd/16010/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
  /usr/bin/man
  /usr/bin/vim.basic
  /usr/lib/NetworkManager/nm-dhcp-client.action
  /usr/lib/NetworkManager/nm-dhcp-helper
  /usr/lib/connman/scripts/dhclient-script
  /usr/lib/snapd/snap-confine
  /usr/lib/snapd/snap-confine//mount-namespace-capture-helper
  /usr/sbin/haveged
  /usr/sbin/dhclient
  lsb_release
  man_filter
  man_groff
  nvidia_modprobe
  nvidia_modprobe//kmod
  snap-update-ns.blender
  tcpdump
1 profiles are in complain mode.
  snap.blender.blender
0 profiles are in kill mode.
0 profiles are in unconfined mode.
1 processes have profiles defined.
1 processes are in enforce mode.
  /usr/sbin/haveged (424)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
0 processes are in mixed mode.
0 processes are in kill mode.
```

Adding AppArmor Profile

Add profile

aa-genprof <application>

```
root@localhost:~# aa-genprof aaexample.sh
Updating AppArmor profiles in /etc/apparmor.d.
Writing updated profile for /root/aaexample.sh.
Setting /root/aaexample.sh to complain mode.
```

Before you begin, you may wish to check if a profile already exists for the application you wish to confine. See the following wiki page for more information:
<https://gitlab.com/apparmor/apparmor/wikis/Profiles>

Profiling: /root/aaexample.sh

Please start the application to be profiled in another window and exercise its functionality now.

Once completed, select the "Scan" option below in order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the opportunity to choose whether the access should be allowed or denied.

[(S)can system log for AppArmor events] / (F)inish
Reading log entries from /var/log/syslog.

Profile: /root/aaexample.sh
Execute: /usr/bin/touch
Severity: 3

(I)nhérit / (C)hild / (N)amed / (X)ix On / (D)eny / Abo(r)t / (F)inish
Complain-mode changes:

Profile: /root/aaexample.sh
Path: /dev/tty
New Mode: owner rw
Severity: 9

[1 - include <abstractions/consoles>]
2 - owner /dev/tty rw,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t)
Adding include <abstractions/consoles> to profile.

Adding AppArmor Profile

```
root@localhost:~# aa-status
apparmor module is loaded.
22 profiles are loaded.
20 profiles are in enforce mode.
/root/aaexample.sh
```

```
root@localhost:~# ./aaexample.sh
touch: cannot touch
'sith/anakin.txt': Permission denied
changed sides
```

```
#!/bin/bash

#Create new file
touch sith/anakin.txt

echo "changed sides"
```

```
Profile: /root/aaexample.sh
Path: /root/jediorder/anakin.txt
New Mode: owner w
Severity: unknown
```

Editing AppArmor Profile

aa-logprof

```
root@localhost:~# aa-logprof
Updating AppArmor profiles in /etc/apparmor.d.
Reading log entries from /var/log/syslog.
Complain-mode changes:
Enforce-mode changes:

Profile: /root/aaexample.sh
Path: /root/sith/anakin.txt
New Mode: owner w
Severity: unknown

[1 - owner /root/sith/anakin.txt w,]
(A)llow / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
Adding owner /root/sith/anakin.txt w, to profile.
```

```
root@localhost:~# ./aaexample.sh
changed sides
```

Editing AppArmor Profile

Manually

Directory

/etc/apparmor.d

Save

apparmor_parser

restart apparmor

```
root@localhost:~# ls -l /etc/apparmor.d
total 88
drwxr-xr-x 2 root root 4096 May  2 17:38 abi
drwxr-xr-x 4 root root 4096 May  2 17:38 abstractions
drwxr-xr-x 2 root root 4096 May  2 17:38 alsablib
drwxr-xr-x 2 root root 4096 Dec 30 2021 forcecomplain
drwxr-xr-x 2 root root 4096 May  2 17:38 local
-rw-r--r-- 1 root root 1339 Mar 10 01:35 lsb_release
-rw-r--r-- 1 root root 1189 Mar 10 01:35 nvidia_modprobe
-rw----- 1 root root  440 Jul  1 15:43 root.aexample.sh
-rw----- 1 root root 3222 Aug  9 2021/sbin.dhclient
drwxr-xr-x 5 root root 4096 May  2 17:38 samples
-rw-r--r-- 1 root root 3448 Mar 17 19:03 usr.bin.man
-rw-r--r-- 1 root root 1421 Jun 20 2021/usr.bin.tcpdump
-rw----- 1 root root  407 Jun 16 13:54/usr.bin.vim.basic
-rw-r--r-- 1 root root 28376 Apr 21 08:50/usr.lib.snapd.snap-confine.real
-rw-r--r-- 1 root root  645 Aug 18 2021/usr.sbin.havedged
-rw-r--r-- 1 root root 1592 Nov 16 2021/usr.sbin.rsyslogd
```

```
# Last Modified: Fri Jul  1 15:43:42 2022
abi {abi/3.0,

include <tunables/global>

/root/aexample.sh {
    include <abstractions/base>
    include <abstractions/bash>
    include <abstractions/consoles>

    deny owner /root/example.txt w,

    /root/aexample.sh r,
    /usr/bin/bash ix,
    /usr/bin/ls -l mix,
    owner /etc/ld.so.cache r,
    owner /root/files/example.txt w,
    owner /root/jediorder/anakin.txt w,
    owner /root/sith/anakin.txt w,
}

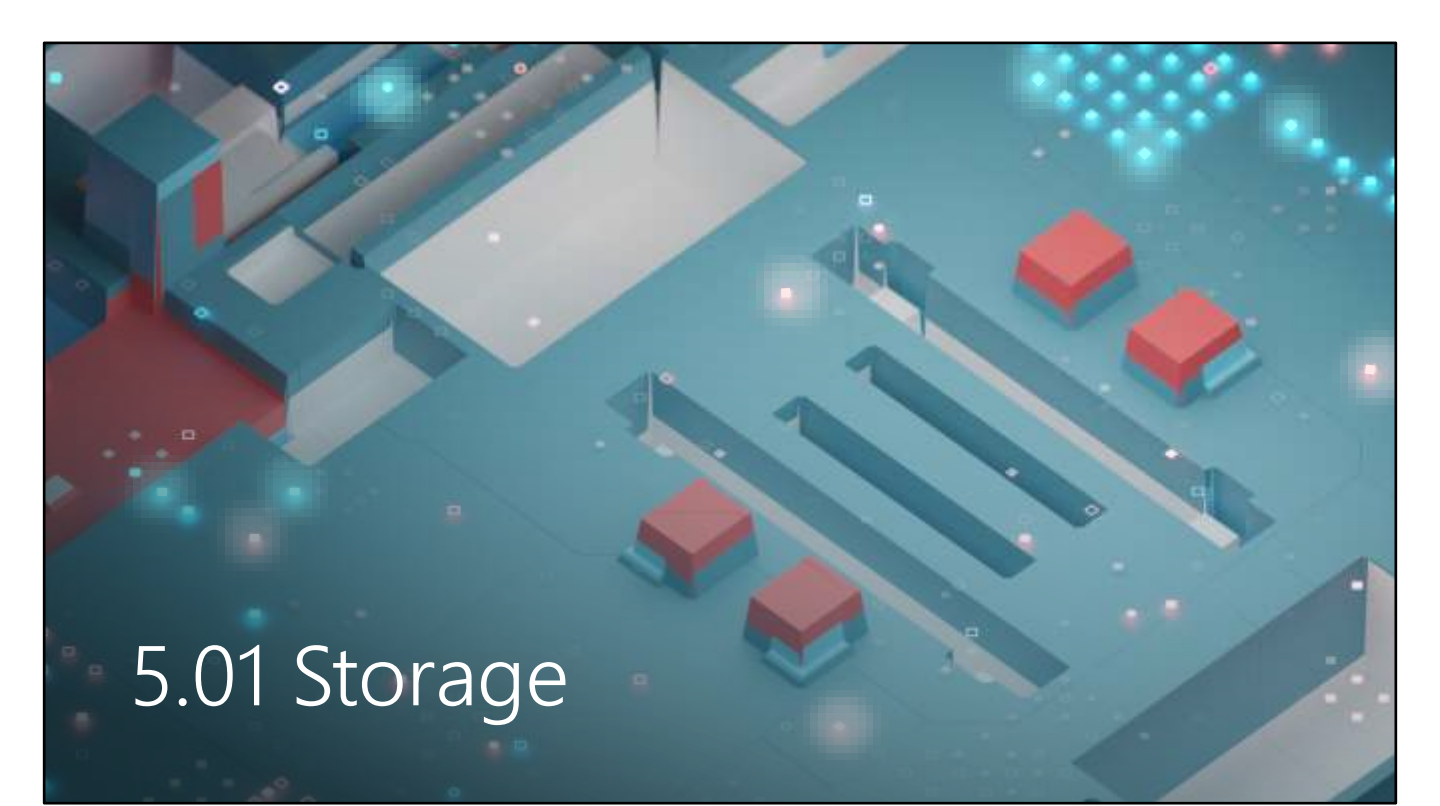
}
```

```
root@localhost:~# apparmor_parser -r
/etc/apparmor.d/root.aexample.sh
```

Review

- Intro to SELinux
- Access control
- SELinux modes
- SELinux booleans
- SELinux logs
- Intro to AppArmor
- Editing AppArmor profile





5.01 Storage

Topics



Intro to block storage



Partitioning



MBR vs GPT



Filesystems



Mounting



LVM



File system hierarchy



Compression and archiving

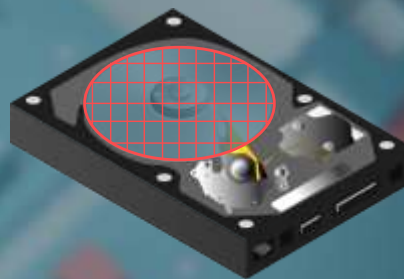
Topics



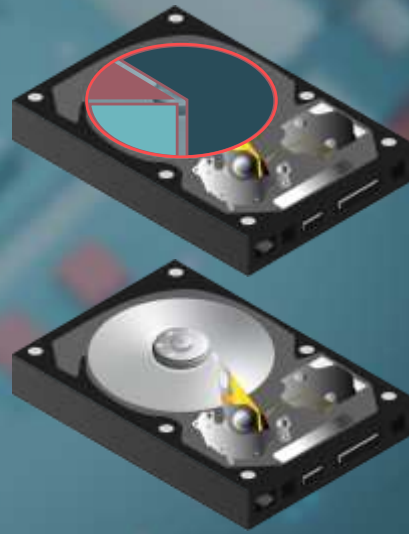
Block storage

Segmented into blocks

Filesystem added after segmentation



Partitioning





lsblk

List block storage devices



blkid

Show UUIDs of storage devices

```
[root@CENTOS ~]# lsblk
NAME MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda    8:0      0 24.5G  0 disk /
sdb    8:16     0   512M  0 disk [SWAP]
```



/dev directory

Device files

/dev/sda
/dev/zero
/dev/urandom
/dev/null

```
[root@CENTOS ~]# ls /dev
autofs      fb0          loop-control pts      snd          tty14  tty24  tty34  tty44  tty54  tty7    vcs     vcsa4  vga_arbiter
block       fd           mapper      random  stderr      tty15  tty25  tty35  tty45  tty55  tty8    vcs1    vcsa5  vhci
bsg         full        mcelog      rfcill  stdin       tty16  tty26  tty36  tty46  tty56  tty9    vcs2    vcsa6  vhost-net
char        fuse        mem         rtc      stdout      tty17  tty27  tty37  tty47  tty57  ttyS0   vcs3    vcsu   vhost-vsock
console     hpet        mqueue      rtc0     tty         tty18  tty28  tty38  tty48  tty58  ttyS1   vcs4    vcsu1  watchdog
core        hugepages   net          sda      tty0        tty19  tty29  tty39  tty49  tty59  ttyS2   vcs5    vcsu2  watchdog0
cpu         hwrng       null         sdb      tty1        tty2   tty3   tty4   tty5   tty6   ttyS3   vcs6    vcsu3  zero
cpu_dma_latency initctl     nvram        sg0      tty10       tty20  tty30  tty40  tty50  tty60  uhid    vcsa    vcsu4
disk        input      port         sg1      tty11       tty21  tty31  tty41  tty51  tty61  uinput  vcsa1    vcsu5
dma_heap    kmsg       ppp          shm      tty12       tty22  tty32  tty42  tty52  tty62  urandom vcsa2    vcsu6
dri         log        ptmx         snapshot tty13       tty23  tty33  tty43  tty53  tty63  usbmon0 vcsa3    vfio
```



fdisk

fdisk /dev/<storage>

Commands

- l** known partition types
- F** free space for partition
- i** information
- o** new partition table
- n** new partition
- d** delete partition

```
root@CENTOS ~]# fdisk /dev/sda
```

```
Welcome to fdisk (util-linux 2.37.2).
```

```
Changes will remain in memory only, until you decide to write them.  
Be careful before using the write command.
```

```
This disk is currently in use - repartitioning is probably a bad idea.  
It's recommended to unmount all file systems, and swapoff all swap  
partitions on this disk.
```

```
The device contains 'ext4' signature and it will be removed by a write command.  
See fdisk(8) man page and --wipe option for more details.
```

```
Device does not contain a recognized partition table.  
Created a new DOS disklabel with disk identifier 0x53bb4df4.
```

```
Command (m for help):
```

```
[root@CENTOS ~]# fdisk /dev/sda
```

```
Welcome to fdisk (util-linux 2.37.2).
```

```
Changes will remain in memory only, until you decide to write them.  
Be careful before using the write command.
```

```
This disk is currently in use - repartitioning is probably a bad idea.  
It's recommended to umount all file systems, and swapoff all swap  
partitions on this disk.
```

```
The device contains 'ext4' signature and it will be removed by a write command. See  
fdisk(8) man page and --wipe option for more details.
```

```
Device does not contain a recognized partition table.  
Created a new DOS disklabel with disk identifier 0x53bb4df4.
```

```
Command (m for help): n
```

```
Partition type
```

```
  p   primary (0 primary, 0 extended, 4 free)  
  e   extended (container for logical partitions)
```

```
Select (default p): p
```

```
Partition number (1-4, default 1): 1
```

```
First sector (2048-51380223, default 2048): 2048
```

```
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-51380223, default 51380223): 12000000
```

```
Created a new partition 1 of type 'Linux' and of size 5.7 GiB.
```

```
Command (m for help): w
```

```
The partition table has been altered.
```

```
Syncing disks.
```

```
[root@CENTOS ~]# lsblk
```

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINTS
sda	8:0	0	24.5G	0	disk	/
└─sda1	8:1	0	5.7G	0	part	
sdb	8:16	0	512M	0	disk	[SWAP]

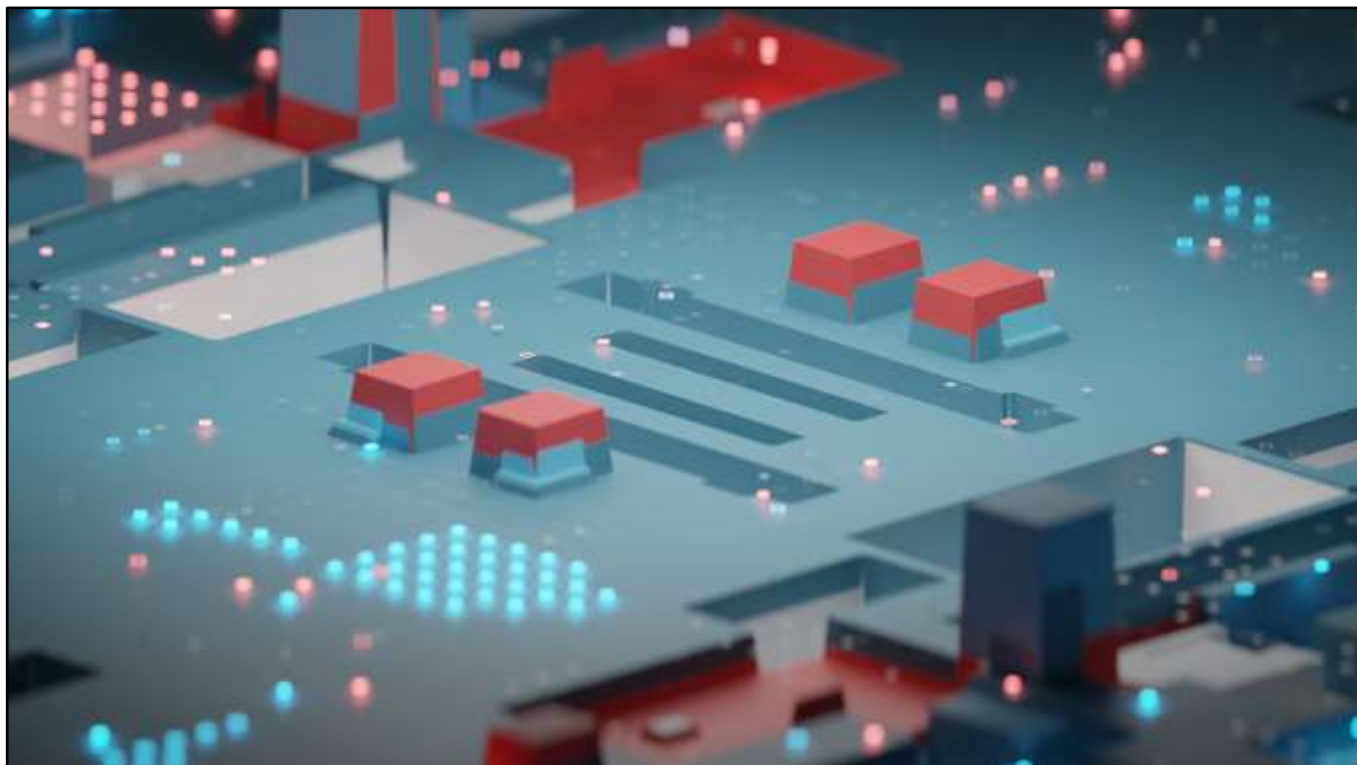
Master Boot Record

512-bytes		
446-bytes Bootcodes, error messages (boot loader/bootstrap)	64-bytes Partition table	2-bytes Disk Signature

16-byte Partition
16-byte Partition
16-byte Partition
16-byte Extended partition

GUID Partion Table (GPT)

Protective MBR	Primary GPT Header	Partition Entries	Partitions	Backup Partion Entries	Backup primary GPT Headers
1	2	3-34	35	36	37



©2023 by StormWind LLC. All rights reserved.

<https://t.me/learningnets>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MBR vs GPT

MBR

Older; more limited
2 TB or less
Four partition limit
Data not easily recoverable

GPT

Newer
Supports massive drives
Limited to 255 partitions (Linux)
Data can be recovered more easily

ext4

Stable

Supports large sizes

- Filesystems up to 1 exbibyte

- Files up to 16 tebibytes

- Subdirectories up to 64,000

Multiblock allocation

- Multiple blocks at a time

Extent-based block mapping

Delayed allocation



XFS

Filesystems up to 8 exbibyte

Files up to 16 terabytes

Datacenter-oriented

RedHat Linux default

Parallel I/O

New kid on the block Created by Oracle

Features:

- Automatic defragmentation
- Pooling
- Snapshots
- Checksums
- Multi-device spanning
- Transparent compression
 - zlib
 - LZO
- SSD Optimized

Issues

- Raid 5 + 6 unsupported

mkfs

mkfs

Make file system on partition

mkfs .<filesystem>

```
root@localhost:~# mkfs.  
mkfs.bfs      mkfs.cramfs  mkfs.ext3     mkfs.fat      mkfs.msdos   mkfs.vfat  
mkfs.btrfs    mkfs.ext2    mkfs.ext4     mkfs.minix    mkfs.ntfs    mkfs.xfs
```

Swap partition

Temporarily uses nonvolatile storage if
RAM becomes full
Much slower

```
[root@CENTOS ~]# sysctl vm.swappiness  
vm.swappiness = 60
```

mount

Attaches storage to a directory
location of users' choice



```
J@Nitro5:~$ sudo mount /dev/sdb1 /data/  
J@Nitro5:~$ lsblk | grep sdb1  
sdb1 8:17 1 3.4G 0 part /data
```

```
J@Nitro5:~$ sudo umount /data  
J@Nitro5:~$ lsblk | grep sdb1  
sdb1 8:17 1 3.4G 0 part
```


Persistent Mounts

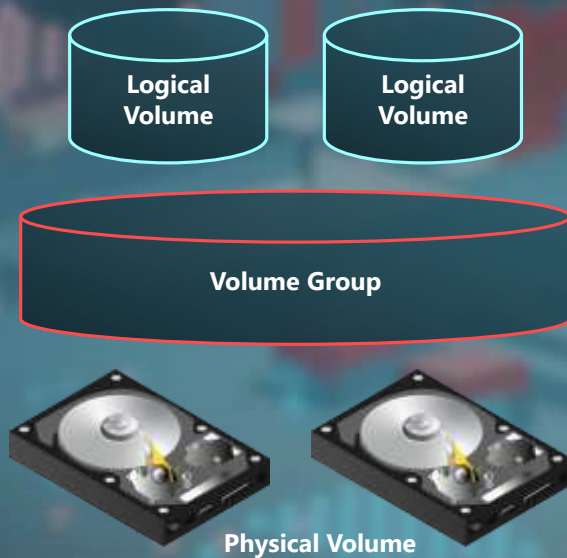
/etc/fstab

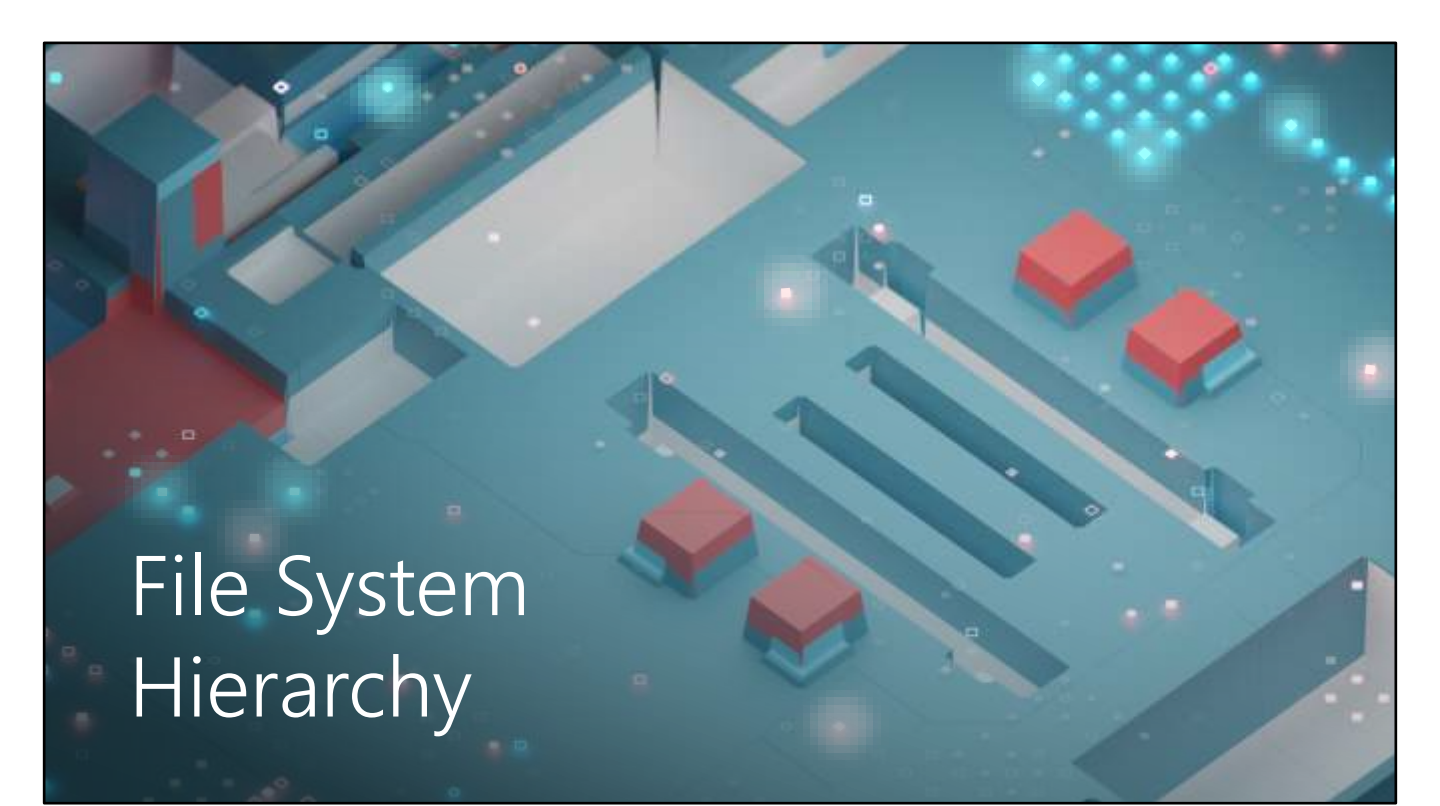
Filesystem table

Automate mounting
of partitions

```
[root@CENTOS ~]# cat /etc/fstab
#
# /etc/fstab
#
# Accessible filesystems, by reference, are maintained
under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or
blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload'
to update systemd
# units generated from this file.
#
/dev/sda / ext4 defaults 1 1
/dev/sdb none swap defaults 0 0
```

Logical Volume Management (LVM)





File System Hierarchy

File Hierarchy



Instructor Lab

/bin/

/boot/

/dev/

/etc/

/home/

/root/

/media/

/mnt/

/opt/

/sbin/

/srv/

/tmp/

/sys/

/var/

/usr/

/proc/

/lib/

File Hierarchy



/bin

Commonly linked to /usr/bin

/boot

Files required to boot your system

/boot/grub

/boot/efi/EFI

/dev

Devices (physical and logical)

/etc

Global configuration files

File Hierarchy



- /home
 - Contains users' home directories
- /root
 - Home directory for root user
- /media
 - Used as mount points for removable media
- /mnt
 - Commonly used for mounts

File Hierarchy



- /opt
Third-party applications
- /sbin
Commonly links to /usr/sbin
- /srv
Data for services like HTTP and FTP (sometimes)
- /tmp
Temporary files

File Hierarchy



/sys

Virtual filesystem

/var

Variably-sized data files

Logs

Webserver files

File Hierarchy



- /usr
Contains most binaries
- /proc
Processes and system information
- /lib
System library files

File Hierarchy

man hier

Describes filesystem
hierarchy directories

```
HIER(7)                                Linux Programmer's Manual                                HIER(7)

NAME
    hier - description of the filesystem hierarchy

DESCRIPTION
    A typical Linux system has, among others, the following directories:

    /      This is the root directory.  This is where the whole tree starts.

    /bin   This directory contains executable programs which are needed in single user mode and to bring the sys-
            tem up or repair it.

    /boot  Contains static files for the boot loader.  This directory holds only the files which are needed during
            the boot process.  The map installer and configuration files should go to /sbin and /etc.  The operat-
            ing system kernel (initrd for example) must be located in either / or /boot.

    /dev   Special or device files, which refer to physical devices.  See mknod(1).

    /etc   Contains configuration files which are local to the machine.  Some larger software packages, like X11,
            can have their own subdirectories below /etc.  Site-wide configuration files may be placed here or in
            /usr/etc.  Nevertheless, programs should always look for these files in /etc and you may have links for
            these files to /usr/etc.

    /etc/opt
            Host-specific configuration files for add-on applications installed in /opt.

    /etc/sgml
            This directory contains the configuration files for SGML (optional).

Manual page hier(7) line 1 (press h for help or q to quit)
```

Compression and Archiving

dd – Duplicate files, partitions, and devices

if=<source of data>

of=<destination of data>

```
# Overwrite /dev/sda with zeros
user@lnx$ sudo dd if=/dev/zero bs=1M of=/dev/sda
524008 bytes copied, 2.065s, 240kB/s

# Overwrite /dev/sda with random data
user@lnx$ sudo dd if=/dev/urandom bs=1M of=/dev/sda
524008 bytes copied, 2.065s, 240kB/s

# Copy /dev/sdb to /dev/sdc exactly
user@lnx$ sudo dd if=/dev/sdb bs=1M of=/dev/sdc
524008 bytes copied, 2.065s, 240kB/s
```

Compression and Archiving

tar – Archive and compress files

- c – Create archive
- x – Extract archive
- v – Verbose output
- f – Specify archive filename
- j – Compress with bzip2
- z – Compress with gzip

```
user@lnx$ ls
file1 file2 file3

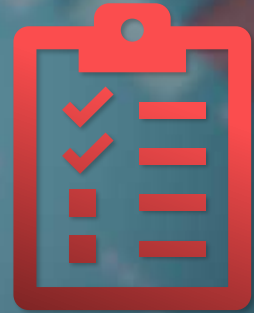
user@lnx$ tar -cvzf myarchive.tar.gz file*
file1
file2
file3

user@lnx$ ls
file1 file2 file3 myarchive.tar.gz

user@lnx$ tar -xvf myarchive.tar.gz
file1
file2
file3
```

Review

Intro to block storage
Partitioning
MBR vs GPT
Filesystems
Mounting
LVM
File System Hierarchy
Compression and Archiving





5.02 RAID

What is RAID?

Redundant Array of Independent Disks

Generally offers additional protection if drive fails

Not always the case

RAID 0

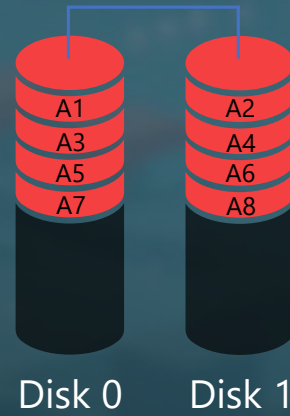
Not fault tolerant

Data striped across two or more disks

Fast

If one disk fails, all data is lost

RAID 0



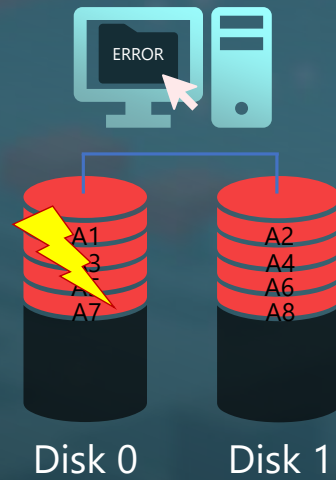
RAID 0

Not fault tolerant

Data striped across two or more disks

Fast

If one disk fails, all data is lost



RAID 1

Mirrors data across drives
All but one drive can fail
Not space-efficient



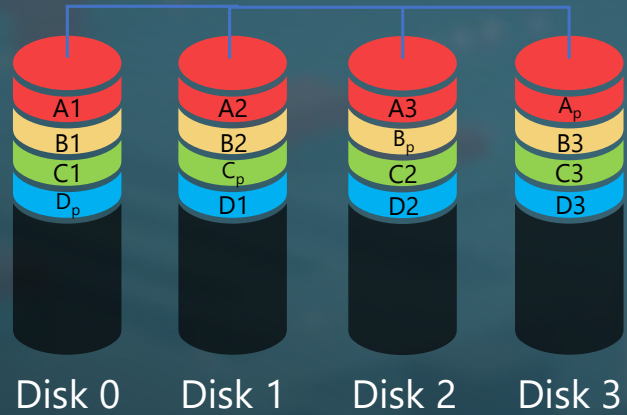
RAID 5

Minimum 3 or more drives

Striping with parity

One drive can be lost

RAID 5

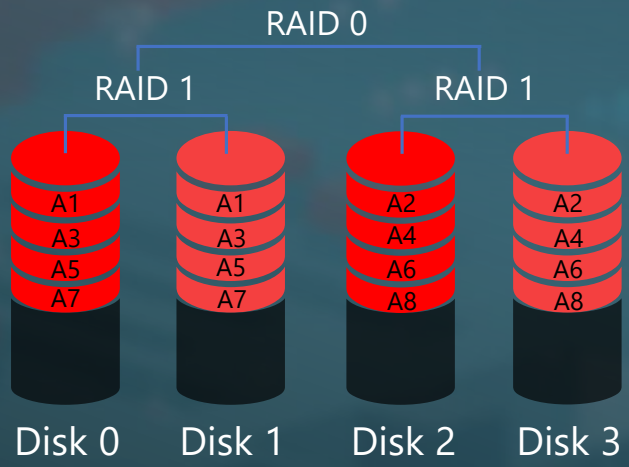


RAID 10

Combines RAID 1 and 0

Striped and mirrored

Four disk minimum



Review

Intro to RAID

RAID levels

0

1

5

10

mdadm





Kernel Modules

Topics



Intro to kernel modules



Kernel module commands



Troubleshooting

Kernel Modules

The Linux kernel is intended to be streamlined, monolithic, and only load what is necessary

It is expanded through modules which provide:

- Device driver
- Support for filesystems
- Other additional features

Kernel Modules

lsmod

Displays kernel modules

modinfo

Details about modules

modprobe

Add and remove modules

insmod

Add module

rmmod

Remove module

```
[root@CENTOS Deathstar]# lsmod
Module                  Size  Used by
tls                     110592  0
nft_fib_inet            16384  1
nft_fib_ipv4            16384  1 nft_fib_inet
nft_fib_ipv6            16384  1 nft_fib_inet
nft_fib                 16384  3 nft_fib_ipv6,nft_fib_ipv4,nft_fib_inet
nft_reject_inet         16384  6
nf_reject_ipv4          16384  1 nft_reject_inet
nf_reject_ipv6          20480  1 nft_reject_inet
nft_reject              16384  1 nft_reject_inet
nft_ct                  20480  10
nft_chain_nat           16384  2
nf_nat                  53248  1 nft_chain_nat
nf_conntrack            176128  2 nf_nat,nft_ct
nf_defrag_ipv6          24576  1 nf_conntrack
nf_defrag_ipv4          16384  1 nf_conntrack
ip_set                  61440  0
bochs_drm               16384  0
rfkill                  32768  1
drm_vram_helper         24576  1 bochs_drm
drm_ttm_helper          16384  2 drm_vram_helper,bochs_drm
ttm                     86016  2 drm_vram_helper,drm_ttm_helper
drm_kms_helper          311296  4 drm_vram_helper,bochs_drm
nf_tables               270336  188
nft_ct,nft_reject_inet,nft_fib_ipv6,nft_fib_ipv4,nft_chain_nat,nft_reject,nft_fib,nft_fib_inet
intel_rapl_rsr          20480  0
itCO_wdt                16384  0
libcrc32c               16384  3 nf_conntrack,nf_nat,nf_tables
nfnetlink               20480  3 nf_tables,ip_set
```

1

```
[root@CENTOS Deathstar]# lsmod | grep cdrom
cdrom                   81920  0
[root@CENTOS Deathstar]# modprobe -r cdrom
[root@CENTOS Deathstar]# lsmod | grep cdrom
[root@CENTOS Deathstar]# modprobe -a cdrom
[root@CENTOS Deathstar]# lsmod | grep cdrom
cdrom                   81920  0
```

2

modprobe

/etc/modprobe.d directory

Files ending in .conf do the following:

- Specify options
- Create aliases
- Insert more than one module

```
anakin@localhost:~$ ls /etc/modprobe.d
amd64-microcode-blacklist.conf  blacklist-firewire.conf  intel-microcode-blacklist.conf
blacklist-ath_pci.conf          blacklist-framebuffer.conf  iwlwifi.conf
blacklist.conf                  blacklist-rare-network.conf  mdadm.conf
```

Review



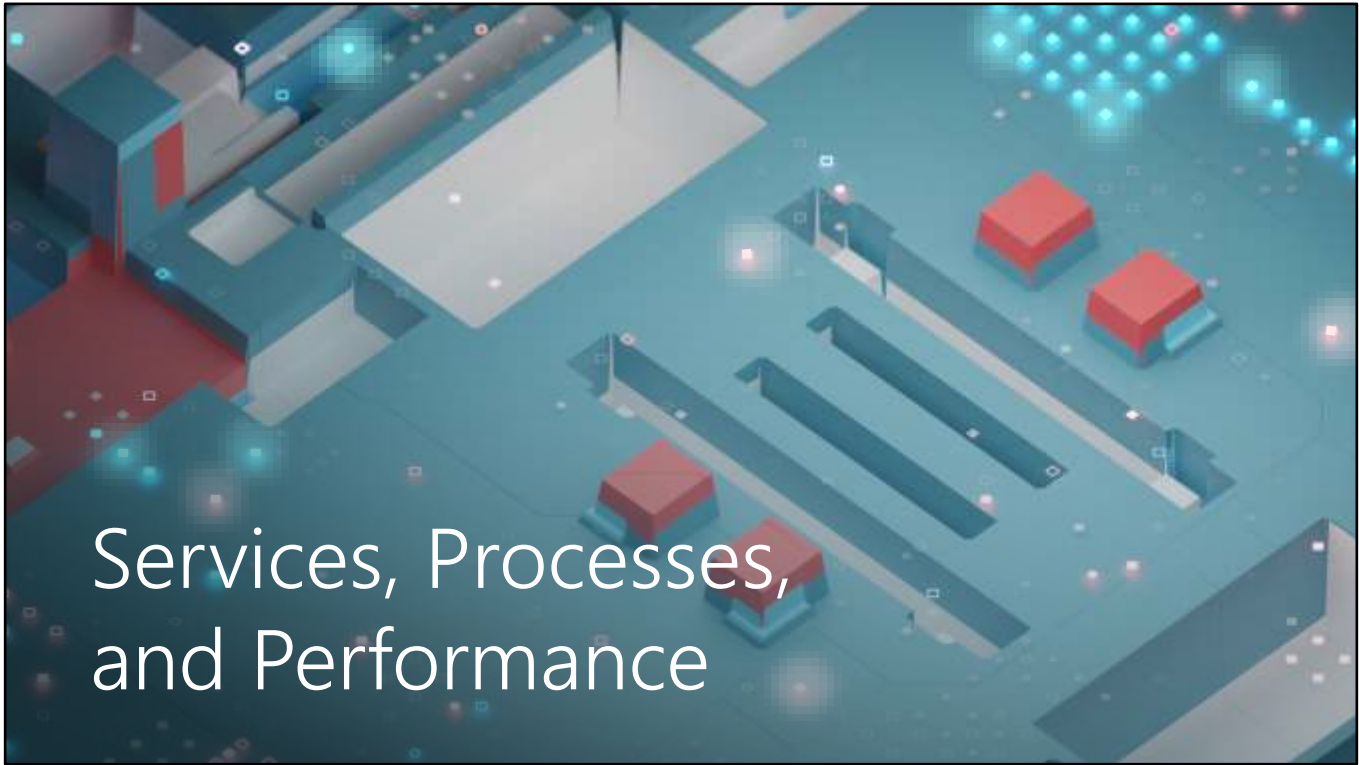
Intro to kernel modules



Kernel module commands



Troubleshooting



Services, Processes, and Performance

©2023 by StormWind LLC. All rights reserved.

<https://t.me/learningnets>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Topics



Intro to processes



Logs



Viewing and killing processes



Priority



Daemons



Facility



Journal

What is a Process?

An application, command, or program that is currently in the following states:

- Running

 - Queued to run or currently running

- Sleeping

 - Waiting on input/idle

- Zombie

 - Parent hasn't killed the child process

Ex:

- nano

- firefox

- bash

Background and Foreground Processes

Certain processes take time to complete and may tie up your shell

Pause a process and restart it in the background

`Ctrl+z` followed by `bg`

Start a new process in the background

`myprocess.sh &`

List existing jobs

`jobs`

Bring background process to foreground

`fg <process>`

top

Lists current processes running and sorts by CPU usage (default)

```
top - 00:58:45 up 5 days, 6:43, 1 user, load average: 0.00, 0.00, 0.00
Tasks: 89 total, 1 running, 88 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni,100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 960.5 total, 311.9 free, 134.1 used, 514.6 buff/cache
MiB Swap: 512.0 total, 512.0 free, 0.0 used. 658.6 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    1 root        20   0 106916  18476  10332 S   0.0   1.9   0:18.49 systemd
    2 root        20   0        0        0        0 S   0.0   0.0   0:00.03 kthreadd
    3 root         0 -20        0        0        0 I   0.0   0.0   0:00.00 rcu_gp
    4 root         0 -20        0        0        0 I   0.0   0.0   0:00.00 rcu_par_gp
    6 root         0 -20        0        0        0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
    9 root         0 -20        0        0        0 I   0.0   0.0   0:00.00 mm_percpu_wq
   10 root        20   0        0        0        0 I   0.0   0.0   0:00.00 rcu_tasks_kthre
   11 root        20   0        0        0        0 I   0.0   0.0   0:00.00 rcu_tasks_rude
   12 root        20   0        0        0        0 I   0.0   0.0   0:00.00 rcu_tasks_trace
```

htop

Alternative version of top

Additional options

F2

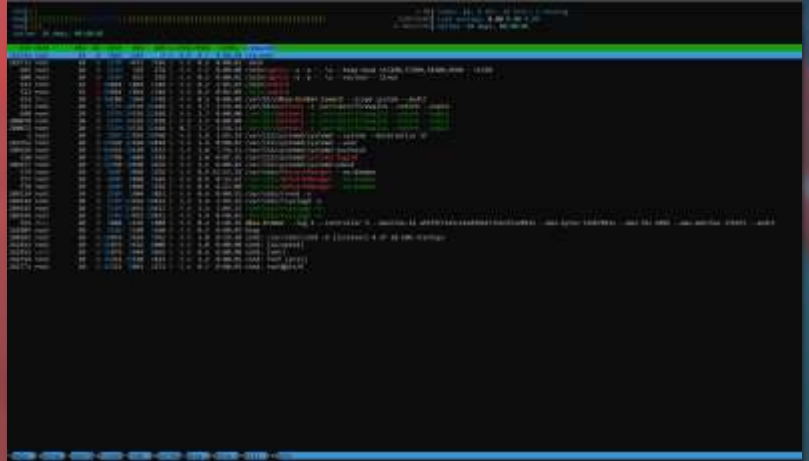
Kill process

Click on option

F9

Sort

F6

A screenshot of the htop process monitoring tool. The interface shows a list of running processes with columns for PID, PPID, USER, CPU, MEM, and COMMAND. The processes are sorted by CPU usage. The top of the screen displays system statistics like uptime, load, and memory usage. The bottom of the screen shows a status bar with various icons and a prompt for user input.

ps

Display snapshot of running processes

PID

Process ID

TTY

Shell process is running in

TIME

CPU time used

CMD

Command used to create process

```
[root@CENTOS ~]# ps
  PID TTY          TIME CMD
 262772 pts/0    00:00:00 bash
 262834 pts/0    00:00:00 ps
```

ps

ps

-e

Shows every process running

-a

All with tty, except session leaders

-u

User

-x

Processes without controlling ttys

```
[root@CENTOS ~]# ps -e
PID TTY          TIME CMD
 1 ?        00:01:45 systemd
 2 ?        00:00:00 kthreadd
 3 ?        00:00:00 rcu_gp
 4 ?        00:00:00 rcu_par_gp
 6 ?        00:00:00 kworker/0:0H-events_highpri
 9 ?        00:00:00 mm_percpu_wq
10 ?        00:00:00 rcu_tasks_kthre
11 ?        00:00:00 rcu_tasks_rude
12 ?        00:00:00 rcu_tasks_trace
13 ?        00:00:19 ksoftirqd/0
14 ?        00:01:02 rcu_preempt
15 ?        00:00:05 migration/0
16 ?        00:00:00 cpuhp/0
18 ?        00:00:00 kdevtmpfs
19 ?        00:00:00 netns
```

```
[root@CENTOS ~]# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  1.8 107572 17824 ?        Ss   Jun17   1:45 /usr/lib/systemd/systemd --system --deserialize 37
root         2  0.0  0.0      0   0 ?        S    Jun17   0:00 [kthreadd]
root         3  0.0  0.0      0   0 ?        Ic   Jun17   0:00 [rcu_gp]
root         4  0.0  0.0      0   0 ?        Ic   Jun17   0:00 [rcu_par_gp]
root         6  0.0  0.0      0   0 ?        Ic   Jun17   0:00 [kworker/0:0H-events_highpri]
root         9  0.0  0.0      0   0 ?        Ic   Jun17   0:00 [mm_percpu_wq]
root        10  0.0  0.0      0   0 ?        I    Jun17   0:00 [rcu_tasks_kthre]
root        11  0.0  0.0      0   0 ?        I    Jun17   0:00 [rcu_tasks_trace]
root        12  0.0  0.0      0   0 ?        I    Jun17   0:00 [rcu_tasks_rude]
root        13  0.0  0.0      0   0 ?        S    Jun17   0:19 [ksoftirqd/0]
root        14  0.0  0.0      0   0 ?        I    Jun17   1:02 [rcu_preempt]
root        15  0.0  0.0      0   0 ?        S    Jun17   0:05 [migration/0]
root        16  0.0  0.0      0   0 ?        S    Jun17   0:00 [cpuhp/0]
root        18  0.0  0.0      0   0 ?        S    Jun17   0:00 [kdevtmpfs]
root        19  0.0  0.0      0   0 ?        Ic   Jun17   0:00 [netns]
root        20  0.0  0.0      0   0 ?        Ic   Jun17   0:00 [inet_frag_wq]
root        21  0.0  0.0      0   0 ?        S    Jun17   0:09 [kauditd]
root        22  0.0  0.0      0   0 ?        S    Jun17   0:03 [khungtaskd]
root        23  0.0  0.0      0   0 ?        S    Jun17   0:00 [oom_reaper]
root        24  0.0  0.0      0   0 ?        Ic   Jun17   0:00 [writeback]
root        25  0.0  0.0      0   0 ?        S    Jun17   0:09 [kcompactd0]
root        26  0.0  0.0      0   0 ?        SN   Jun17   0:00 [kmem]
root        27  0.0  0.0      0   0 ?        SN   Jun17   0:19 [khugepaged]
root        28  0.0  0.0      0   0 ?        Ic   Jun17   0:00 [cgroupd]
root        29  0.0  0.0      0   0 ?        Ic   Jun17   0:00 [kintegrityd]
root        30  0.0  0.0      0   0 ?        Ic   Jun17   0:00 [kblockd]
```

ps

```
ps -u root | grep nano
```

```
[root@CENTOS ~]# ps -u root | grep nano
262928 pts/1    00:00:00 nano
```

pgrep

ps merged with grep

```
[root@CENTOS ~]# pgrep nano
262928
```

kill

kill

Sends signals to processes

15 - SIGTERM - Requests process to kill itself (default)

1 - SIGHUP - Reloads a Process

killall

Kill processes by name instead of PID

pkill

Will kill **ALL** processes with that name

Like killall but more options

```
[root@CENTOS ~]# pgrep nano
262928
[root@CENTOS ~]# kill 262928
```

```
[root@CENTOS ~]# kill -l
 1) SIGHUP      2) SIGINT      3) SIGQUIT      4) SIGILL      5) SIGTRAP
 6) SIGABRT     7) SIGBUS      8) SIGFPE       9) SIGKILL     10) SIGUSR1
11) SIGSEGV     12) SIGUSR2     13) SIGPIPE     14) SIGALRM     15) SIGTERM
16) SIGSTKFLT   17) SIGCHLD    18) SIGCONT     19) SIGSTOP     20) SIGTSTP
21) SIGTTIN     22) SIGTTOU     23) SIGURG      24) SIGXCPU     25) SIGXFSZ
26) SIGVTALRM   27) SIGPROF    28) SIGWINCH    29) SIGIO       30) SIGPWR
31) SIGSYS      34) SIGRTMIN   35) SIGRTMIN+1  36) SIGRTMIN+2  37) SIGRTMIN+3
38) SIGRTMIN+4  39) SIGRTMIN+5  40) SIGRTMIN+6  41) SIGRTMIN+7  42) SIGRTMIN+8
43) SIGRTMIN+9  44) SIGRTMIN+10 45) SIGRTMIN+11 46) SIGRTMIN+12 47) SIGRTMIN+13
48) SIGRTMIN+14 49) SIGRTMIN+15 50) SIGRTMAX-14 51) SIGRTMAX-13 52) SIGRTMAX-12
53) SIGRTMAX-11 54) SIGRTMAX-10 55) SIGRTMAX-9  56) SIGRTMAX-8  57) SIGRTMAX-7
58) SIGRTMAX-6  59) SIGRTMAX-5  60) SIGRTMAX-4  61) SIGRTMAX-3  62) SIGRTMAX-2
63) SIGRTMAX-1  64) SIGRTMAX
```

kill

Some processes will not kill themselves
9 - SIGKILL - Forcibly terminates processes

```
[root@CENTOS ~]# pgrep ping
78688
[root@CENTOS ~]# kill 7688
[root@CENTOS ~]# pgrep ping
78688
[root@CENTOS ~]# kill -9 7688
[1]+  Killed                  ping 8.8.8.8
```

Isof

Lists all open files by all processes

-u

Files opened by username

-c

Files opened by process

-p

Files opened by process ID

nice and renice

nice

Prioritizes CPU usage to certain processes.

Used before starting process

nice -n <value>

Values

-20 = Top Priority

0 = Default Value

+19 = Lowest Priority

-u

Changes all values for user

renice

Changes value of current running process

lscpu

CPU information

Core count

Speed

Virtualization features

```
[root@CENTOS ~]# lscpu | less
```

```
Architecture:           x86_64
CPU op-mode(s):         32-Bit, 64-bit
Address sizes:          40 bits physical, 48 bits virtual
Byte Order:             Little Endian
CPU(s):                 1
On-line CPU(s) list:    0
Vendor ID:              AuthenticAMD
BIOS Vendor ID:         QEMU
Model name:             AMD EPYC 7501 32-Core Processor
BIOS Model name:        pc-q35-4.1
CPU family:             23
Model:                 1
Thread(s) per core:    1
Core(s) per socket:    1
Socket(s):              1
Stepping:               2
BogoMIPS:               3999.99
Flags:                  fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
cmov pat pse36 clflush mmx fxsr sse sse2 syscall nx mmxext fxsr_opt pdpe1gb rdtscp lm
rep_good nopl cpuid extd_apicid tsc_known_freq pni pclmulqdq sse3 fma cx16 sse4_1 sse4_2
x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm
cmp_legacy cr8_legacy abm sse4a misalignsse 3dnowprefetch osvw perfctr_core ssbd lbrb vmmcall
fsgsbase tsc_adjust bmi1 avx2 smep bmi2 rdtseed adx smap clflushopt sha_ni xsaveopt xsavec
xgetbv1 xsavee3 virt_sabd arat arch_capabilities
Hypervisor vendor:      KVM
Virtualization type:    full
L1d cache:              64 KiB (1 instance)
L1i cache:              64 KiB (1 instance)
L2 cache:               512 KiB (1 instance)
L3 cache:               16 MiB (1 instance)
NUMA node(s):           1
NUMA node0 CPU(s):      0
Vulnerability Itlb multihit: Not affected
Vulnerability L1tf:     Not affected
Vulnerability Mds:      Not affected
Vulnerability Meltdown: Not affected
Vulnerability Spec store bypass: Mitigation; Speculative Store Bypass disabled via prctl
Vulnerability Spectre v1: Mitigation; usercopy/swapgs barriers and __user pointer
sanitization
Vulnerability Spectre v2: Mitigation; Retpolines, IBPB conditional, STIBP disabled,
RSB filling
Vulnerability Smbds:     Not affected
Vulnerability Tsx async abort: Not affected
(END)
```

/proc/cpuinfo

Virtual file containing
similar CPU information

```
[root@CENTOS ~]# cat /proc/cpuinfo
processor       : 0
vendor_id      : AuthenticAMD
cpu family     : 23
model          : 1
model name     : AMD EPYC 7501 32-Core Processor
stepping       : 2
microcode      : 0x1000065
cpu MHz        : 1999.998
cache size     : 512 KB
physical id    : 0
siblings       : 1
core id        : 0
cpu cores      : 1
apicid         : 0
initial apicid : 0
fpu            : yes
fpu_exception  : yes
cpuid level    : 13
wp             : yes
flags          : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
pat pse36 clflush mmx fxsr sse sse2 syscall nx mmxext fxsr_opt pdpe1gb rdtscp lm
rep_good nopl cpuid extd_apicid tsc_known_freq pni pclmulqdq ssse3 fma cx16
sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand
hypervisor_lahf_lm cmp_legacy cr8_legacy abm sse4a misalignsse 3dnowprefetch
osvw perfctr_core ssbd ibpb vmcall fsgsbase tsc_adjust bmi1 avx2 smep bmi2
rdseed adx smap clflushopt sha_ni xsaveopt xsavec xgetbv1 xsaves virt_ssbd arat
arch_capabilities
bugs           : fxsave_leak sysret_ss_attrs null_seg spectre_v1 spectre_v2
spec_store_bypass
bogomips       : 3999.99
TLB size       : 1024 4K pages
clflush size   : 64
cache alignment : 64
address sizes   : 40 bits physical, 48 bits virtual
power management:
```

uptime

Displays system uptime,
user count, and system
load

Load average:

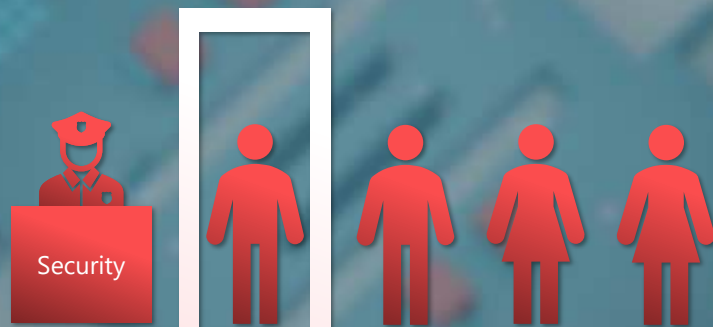
1 Min average

5 Min average

15 Min average

```
[root@CENTOS ~]# uptime
01:25:50 up 19 days, 9:05, 2 users, load average: 0.25, 0.32, 0.14
```

Single Core CPU Load Average



Dual Core CPU Load Average



/proc/meminfo



Virtual file that contains memory information

```
root@Ubuntu:~# cat /proc/meminfo
MemTotal:       994456 kB
MemFree:        81300 kB
MemAvailable:   633460 kB
Buffers:        47160 kB
Cached:         597828 kB
SwapCached:     4776 kB
Active:         426644 kB
Inactive:       318220 kB
Active(anon):   32492 kB
Inactive(anon): 67608 kB
Active(file):   394152 kB
Inactive(file): 250612 kB
Unevictable:    64 kB
Mlocked:        64 kB
SwapTotal:      524284 kB
SwapFree:       114924 kB
Dirty:          204 kB
Writeback:       0 kB
AnonPages:      95252 kB
Mapped:         114996 kB
Shmem:          760 kB
KReclaimable:   62712 kB
Slab:           103540 kB
SReclaimable:   62712 kB
SUnreclaim:     40828 kB
KernelStack:    3772 kB
PageTables:      8824 kB
NFS_Unstable:    0 kB
Bounce:          0 kB
WritebackTmp:    0 kB
CommitLimit:    1021512 kB
Committed_AS:   1956616 kB
VmallocTotal:   34359738367 kB
VmallocUsed:     21824 kB
VmallocChunk:    0 kB
Percpu:         840 kB
HardwareCorrupted: 0 kB
AnonHugePages:   0 kB
ShmemHugePages:  0 kB
ShmemPmdMapped:  0 kB
FileHugePages:   0 kB
FilePmdMapped:   0 kB
HugePages_Total: 0
HugePages_Free:  0
HugePages_Reserved: 0
HugePages_Surp:  0
Hugepagesize:    2048 kB
Hugetlb:          0 kB
DirectMap4k:     171888 kB
DirectMap2M:     876544 kB
DirectMap1G:      0 kB
```

free



Displays essential memory information

available – Available memory including swap

free - Current memory that is available without using swap

```
root@localhost:~# free
              total        used        free      shared  buff/cache   available
Mem:      994456    247208    131376         2140        615872        589752
Swap:      524284    317060    207224
```


dmidecode



Computer hardware details

```
-t processor
```

```
-t bios
```

```
-t memory
```

```
| less
```

What is a daemon?



A process that runs in the background

Examples:

firewalld

sshd

systemd

Most are Indicated with a "d" at the end

systemd



systemd

Manages other daemons

First process started

Unit types:

- Socket

 - Starts process if traffic detected with particular socket

- Service

 - Starts, stops, reloads different daemons

- Target

 - Group of services

 - Boots system to particular state

 - Specific daemons started every time

systemd



Targets

emergency.target

rescue.target

multi-user.target

graphical.target

systemctl



systemctl – manage system daemons

Start

```
systemctl start <service>
```

Stop

```
systemctl stop <service>
```

Restart or reload

```
systemctl restart/reload <service>
```

Start on boot

```
systemctl enable/disable <service> [--now]
```

Status

```
systemctl status <service>
```

Prevent from running whatsoever

```
systemctl mask <service>
```

journal



Daemon that compiles logs into journal



journalctl - View journal

-s

Since date

-U

Until date

--system

--user

journal



Storage locations

Default

/run/log/journal

Change location

/etc/systemd/journald.conf

Storage=auto

1st if exists

/var/log/journal

2nd

/run/log/journal

Storage=persistent

/var/log/journal

Storage=volatile

/run/log/journal

```
[Journal]
#Storage=auto
#Compress=yes
#Seal=yes
#SplitMode=uid
#SyncIntervalSec=5m
#RateLimitIntervalSec=30s
#RateLimitBurst=10000
#SystemMaxUse=
#SystemKeepFree=
#SystemMaxFileSize=
#SystemMaxFiles=100
#RuntimeMaxUse=
#RuntimeKeepFree=
#RuntimeMaxFileSize=
#RuntimeMaxFiles=100
#MaxRetentionSec=
#MaxFileSec=1month
#ForwardToSyslog=no
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
#MaxLevelConsole=info
#MaxLevelWall=emerg
#LineMax=48K
#ReadKMsg=yes
Audit=
```

rsyslog



Takes logs from journal and moves them to specific files or network locations

/var/log

messages

secure

maillog

cron

boot.log

rsyslog



Configuration file is
`/etc/rsyslog.conf`

Log to file by severity

Log to file by facility

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                                /var/log/secure

# Log all the mail messages in one place.
mail.*                                                    -/var/log/maillog

# Log cron stuff
cron.*                                                    /var/log/cron

# Everybody gets emergency messages
*.emerg                                                  :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                           /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                  /var/log/boot.log
```

Syslog Priorities



Define the severity of messages

Level	Priority
0	emergency
1	alert
2	critical
3	error
4	warning
5	notice
6	information
7	debug

Facility



Specifies the subsystem that produced message

auth, authpriv, cron, kern,

lpr, mail, mark, news, syslog,

user, uucp, local0 - local7

Example:

All mail programs log with facility (LOG_MAIL) if logging with syslog

Log Rotation



Configure log rotation in
/etc/logrotate.conf

Rotation frequency

Backlogs

Compressions

```
[root@CENTOS ~]# cat /etc/logrotate.conf
# see "man logrotate" for details

# global options do not affect preceding include directives

# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may be also be configured here.
```

Review



Intro to processes



Logs



Viewing and killing processes



Priority



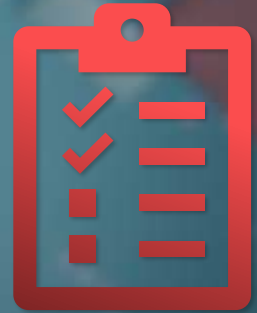
Daemons

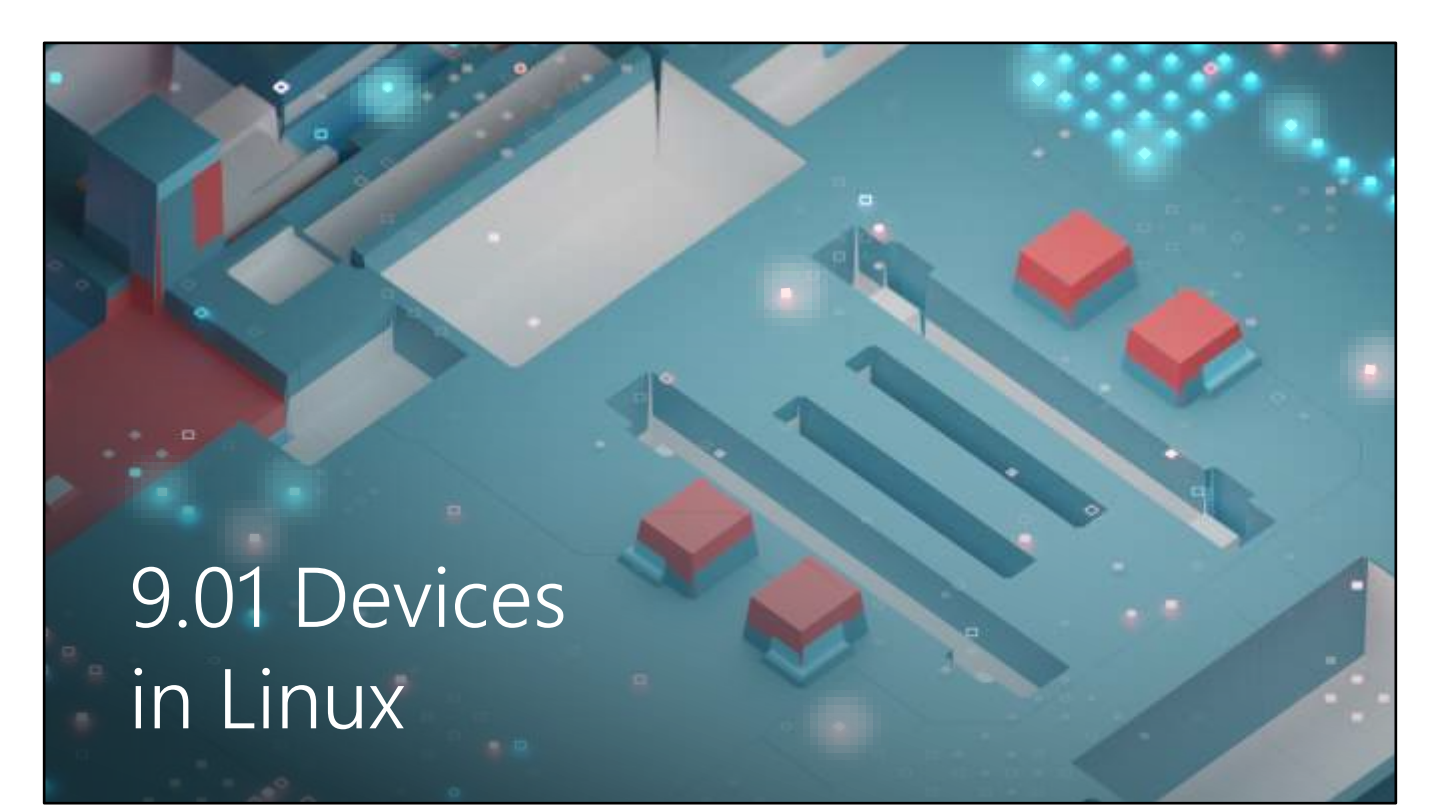


Facility



Journal





9.01 Devices in Linux

Topics

Listing

USB devices

Block devices

PCI buses and devices

SCSI devices

Hardware components

lsusb

Lists USB devices and bus

```
Joshua@Nitro5:~$ lsusb
Bus 002 Device 002: ID 0781:5581 SanDisk Corp. Ultra
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 002: ID 0408:a061 Quanta Computer, Inc. HD User Facing
Bus 001 Device 003: ID 8087:0aaa Intel Corp. Bluetooth 9460/9560 Jefferson Peak (JfP)
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```


lsblk

Lists information for block devices

```
[root@CENTOS ~]# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda          8:0    0 24.5G  0 disk /
└─sda1       8:1    0  5.7G  0 part
sdb          8:16   0   512M  0 disk [SWAP]
```

lspci

Lists PCI buses and PCI devices

```
root@localhost:~# lspci
00:00.0 Host bridge: Intel Corporation 82G33/G31/P35/P31 Express DRAM Controller
00:01.0 VGA compatible controller: Device 1234:1111 (rev 02)
00:02.0 SCSI storage controller: Red Hat, Inc. Virtio SCSI
00:03.0 SCSI storage controller: Red Hat, Inc. Virtio SCSI
00:04.0 Ethernet controller: Red Hat, Inc. Virtio network device
00:1f.0 ISA bridge: Intel Corporation 82801IB (ICH9) LPC Interface Controller (rev 02)
00:1f.2 SATA controller: Intel Corporation 82801IR/IO/IH (ICH9R/DO/DH) 6 port SATA Controller [AHCI mode] (rev 02)
00:1f.3 SMBus: Intel Corporation 82801I (ICH9 Family) SMBus Controller (rev 02)
```

ls SCSI

Lists SCSI devices

```
Joshua@Nitro5:~$ ls SCSI
[4:0:0:0] disk ATA HGST HTS721010A9 A330 /dev/sda
[5:0:0:0] disk USB SanDisk 3.2Gen1 1.00 /dev/sdb
```



dmidecode

Shows system hardware components

```
root@localhost:~# dmidecode
# dmidecode 3.3
Getting SMBIOS data from sysfs.
SMBIOS 2.8 present.
9 structures occupying 398 bytes.
Table at 0x000F5960.

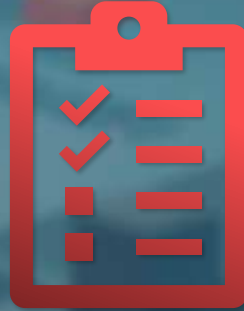
Handle 0x0000, DMI type 0, 24 bytes
BIOS Information
    Vendor: SeaBIOS
    Version: rel-1.12.1-0-ga5cab58e9a3f-prebuilt.qemu.org
    Release Date: 04/01/2014
    Address: 0xE8000
    Runtime Size: 96 kB
    ROM Size: 64 kB
    Characteristics:
        BIOS characteristics not supported
        Targeted content distribution is supported
    BIOS Revision: 0.0

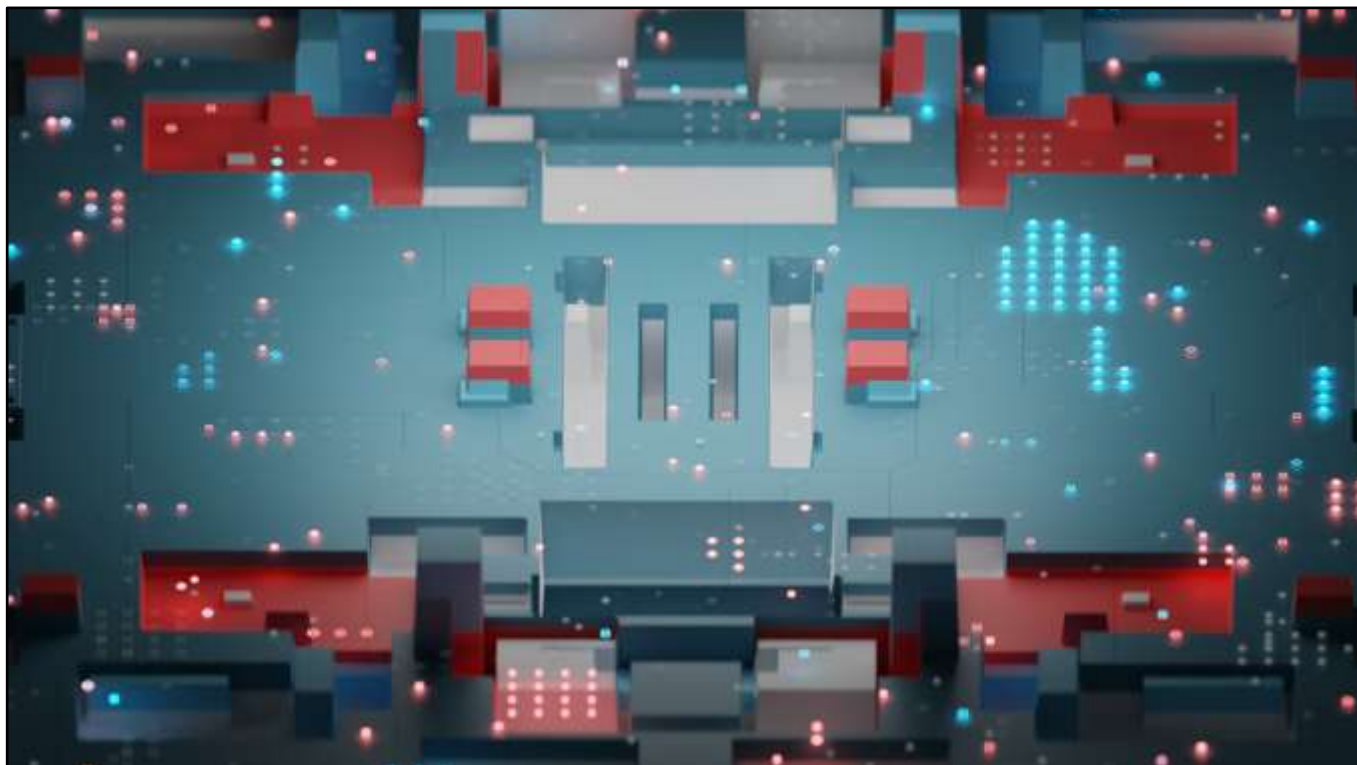
Handle 0x0100, DMI type 1, 27 bytes
System Information
    Manufacturer: QEMU
    Product Name: Standard PC (Q35 + ICH9, 2009)
    Version: pc-q35-4.1
    Serial Number: Not Specified
    UUID: Not Settable
    Wake-up Type: Power Switch
    SKU Number: Not Specified
    Family: Not Specified
```

Review

Listing

- USB devices
- Block devices
- PCI buses and devices
- SCSI devices
- Hardware components

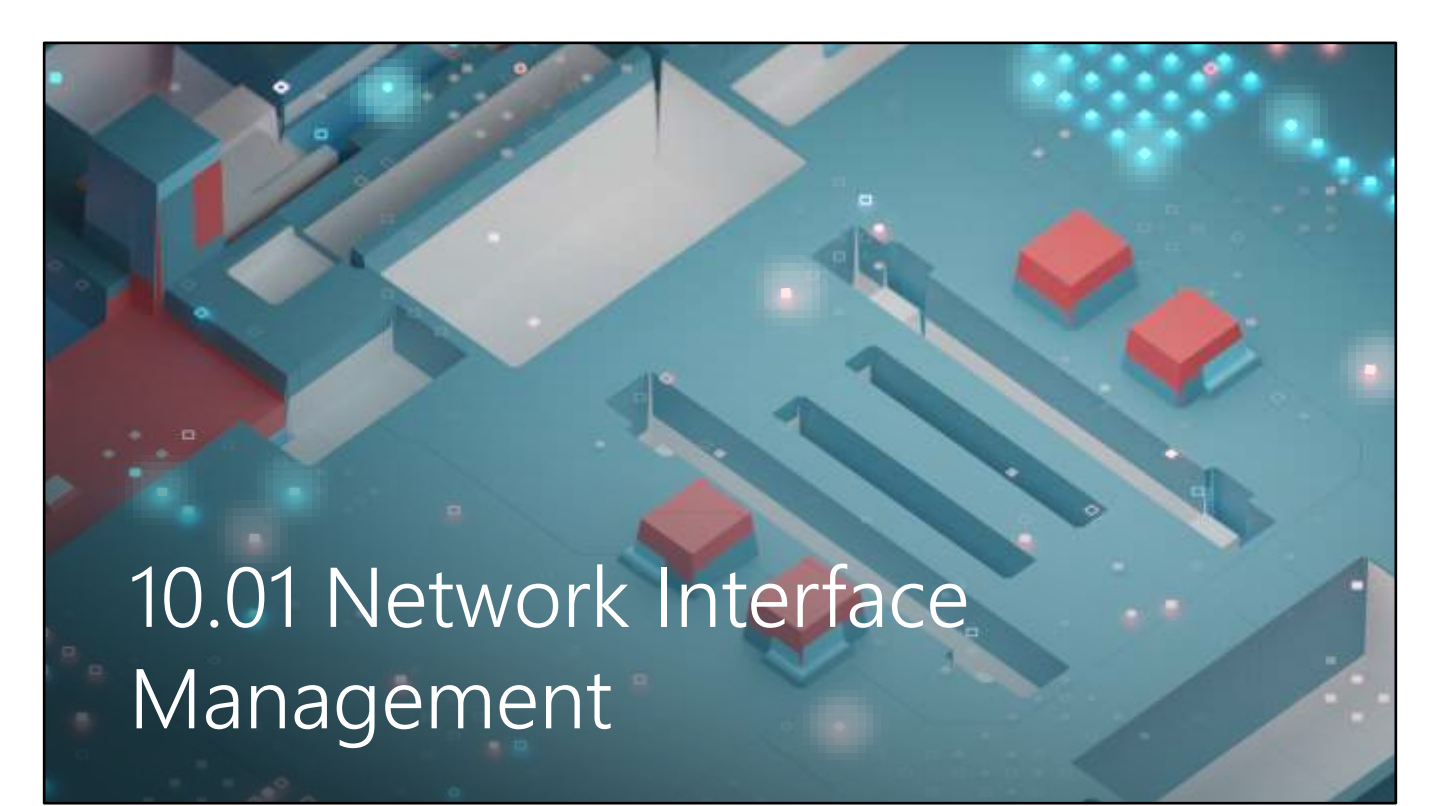




©2023 by StormWind LLC. All rights reserved.

<https://t.me/learningnets>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



10.01 Network Interface Management

Topics

IP information

Changing hostname

Changing IP address

Displaying ARP table

Socket statistics

Displaying routing table

Creating, editing, and deleting
network connections

Network configuration file

Interface Management

ip

a

Shows all interface configurations

link show <interface>

Show specific interface configurations

route

View routing table

```
root@localhost:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue
state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd
    00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc mq state UP group default qlen 1000
    link/ether f2:3c:93:60:aa:23 brd ff:ff:ff:ff:ff:ff
    inet 173.230.138.127/24 brd 173.230.138.255 scope
global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:3c02::f03c:93ff:fe60:aa23/64 scope
global dynamic mngtmpaddr noprefixroute
        valid_lft 60sec preferred_lft 20sec
    inet6 fe80::f03c:93ff:fe60:aa23/64 scope link
        valid_lft forever preferred_lft forever
```

Interface Management

ifconfig

Enabled interfaces

Deprecated

```
root@localhost:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 173.230.138.127 netmask 255.255.255.0
    broadcast 173.230.138.255
    inet6 2600:3c02::f03c:93ff:fe60:aa23 prefixlen 64
    scopeid 0x0<global>
    inet6 fe80::f03c:93ff:fe60:aa23 prefixlen 64
    scopeid 0x20<link>
    ether f2:3c:93:60:aa:23 txqueuelen 1000 (Ethernet)
    RX packets 4007606 bytes 1559581280 (1.5 GB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5634725 bytes 718776348 (718.7 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0
    collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1468 bytes 157225 (157.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1468 bytes 157225 (157.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0
    collisions 0
```

Interface Management

ss - socket statistics

- a = all
- l = listening
- t = TCP
- u = UDP
- x = UNIX domain
- m = socket memory
- s = summary

```
root@localhost:~# ss -t
State      Recv-Q    Send-Q    Local
Address:Port  Peer Address:Port  Process
ESTAB      0          0
173.230.138.127:ssh      64.225.67.175:38938
ESTAB      0          0
173.230.138.127:ssh      107.145.74.3:56696
```

Interface Management

NetworkManager

nmcli

Create, edit, and delete
network connections

```
root@localhost:~# nmcli
eth0: unmanaged
      "Red Hat Virtio"
      ethernet (virtio_net), F2:3C:93:60:AA:23,
hw, mtu 1500
```

```
lo: unmanaged
     "lo"
     loopback (unknown), 00:00:00:00:00:00, sw,
mtu 65536
```

Use "nmcli device show" to get complete information
about known devices and
"nmcli connection show" to get an overview on active
connection profiles.

Consult nmcli(1) and nmcli-examples(7) manual pages
for complete usage details.

Interface Management

hostnamectl

Show or set hostname

```
root@localhost:~# hostname
localhost

root@localhost:~# cat /etc/hostname
localhost

root@localhost:~# hostnamectl
Static hostname: localhost
Icon name: computer-vm
Chassis: vm
Machine ID: 1c33d3d96ddd4e5e951256197c8e1120
Boot ID: 831d07d0eeef4f01b94250dba544a8a2
Virtualization: kvm
Operating System: Ubuntu 22.04 LTS
Kernel: Linux 5.15.0-37-generic
Architecture: x86-64

root@localhost:~# hostnamectl set-hostname
Ubuntu.localdomain
```

Interface Management

arp

Display ARP table

```
root@Ubuntu:~# arp
Address                  HWtype  HWaddress
Flags Mask              Iface    ether    00:00:5e:00:be:ef
C                        eth0
```

Interface Management

route

View routing table

Deprecated

ip route

View routing table

Current

ip route add <range> via <IP>

Modify routing table

```
root@Ubuntu:~# route
Kernel IP routing table
Destination        Gateway            Genmask
Flags Metric Ref    Use Iface
default            gw-li178.linode  0.0.0.0
UG    0          0          0 eth0
173.230.138.0      0.0.0.0           255.255.255.0
U      0          0          0 eth0
```

```
anakin@localhost:~$ ip route
default via 50.116.34.1 dev eth0 proto static
50.116.34.0/24 dev eth0 proto kernel scope
link src 50.116.34.204
```

Interface Management

/etc/sysconfig/network-scripts/ifcfg-eth0

Network configuration file

RHEL/CentOS

```
DEVICE="eth0"  
NAME="eth0"  
ONBOOT="yes"
```

```
# "bootp" and "dhcp" are for dhcp, anything else  
# is for a static configuration. "none" is given  
# by sysconfig.txt so we're using it.  
BOOTPROTO="none"
```

```
# Use hardware-based IPv6 addresses, no privacy extensions.  
IPV6INIT="yes"  
IPV6_ADDR_GEN_MODE="eui64"  
IPV6_PRIVACY="no"
```

```
# Since we want a static configuration, we're specifying DNS  
# addresses in this file for NetworkManager. "No" here tells  
# NM to use them when BOOTPROTO!=dhcp.  
# If NM is disabled the value will be yes  
PEERDNS="no"
```

```
DOMAIN=members.linode.com
```

```
GATEWAY0=50.116.38.1
```

```
# resolvconf doesn't recognize more than 3 nameservers.
```

```
DNS1=173.230.128.5  
DNS2=23.239.18.5  
DNS3=50.116.35.5
```

```
# Sysconfig.txt says that PREFIX takes precedence over  
# NETMASK when both are present. Since both aren't needed,  
# we'll go with PREFIX since it seems to be preferred.
```

```
# IP assignment for eth0  
IPADDR0=50.116.38.249  
PREFIX0=24
```


Managing Forwarding

In some scenarios, you may want to enable IP forwarding on a Linux host

Routing

Firewalling

Load balancing

Proxying

```
sysctl -w net.ipv4.ip_forward=1
```

Enable IP forwarding (non-persistent)

```
echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf
```

Enable IP forwarding (persistent)

```
root@lnxhost# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0

root@lnxhost# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 0

root@lnxhost# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
```

Review

IP information

Changing hostname

Changing IP address

Displaying ARP table

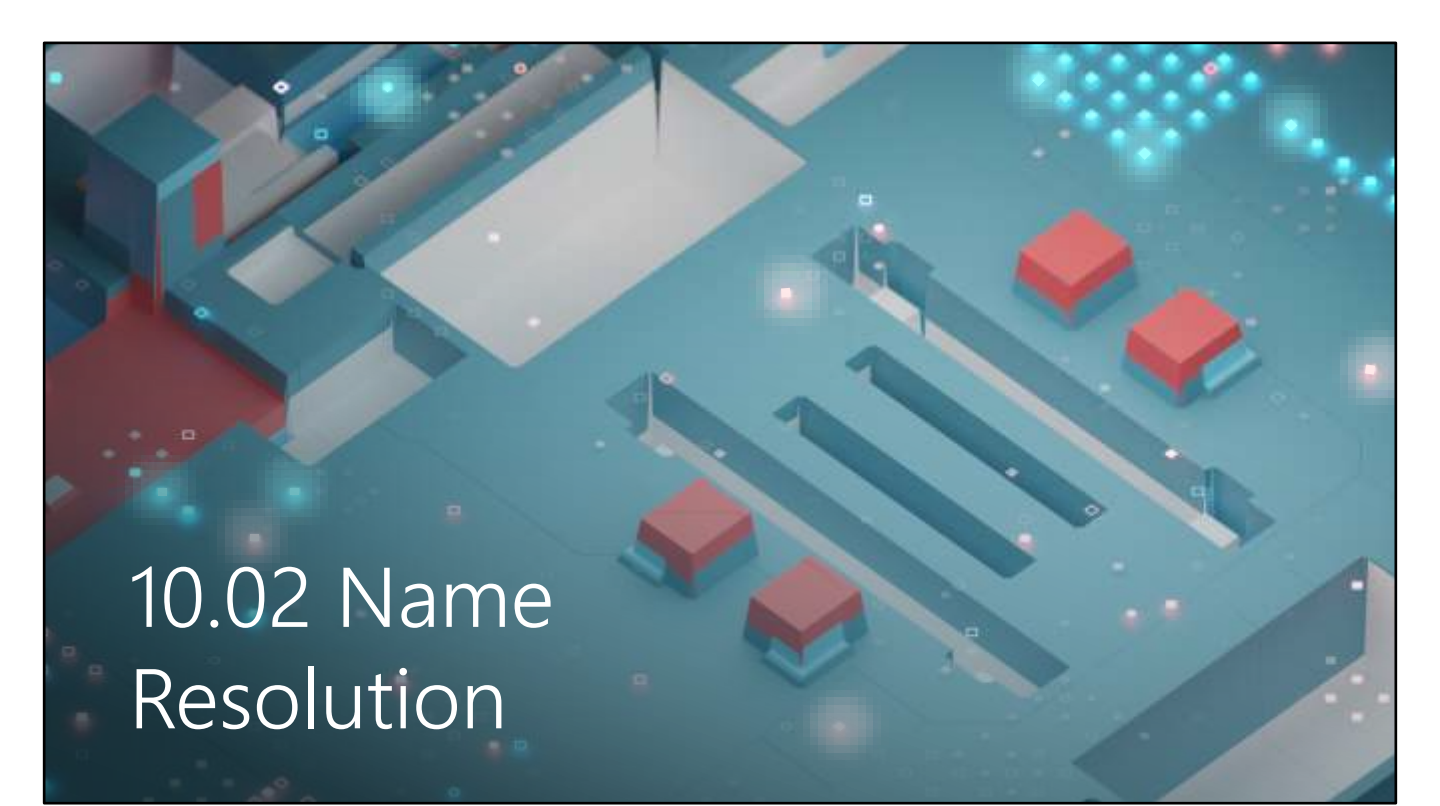
Socket statistics

Displaying routing table

Creating, editing, and deleting network connections

Network configuration file



An isometric illustration of a cityscape with various buildings in shades of blue, red, and white. The scene is filled with glowing blue and red particles, giving it a futuristic or digital feel. The text '10.02 Name Resolution' is overlaid on the left side in a white, sans-serif font.

10.02 Name Resolution

Topics



DNS Name Resolution

Name Resolution

```
root@Ubuntu:~# cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages
# installed, try:
# `info libc "Name Service Switch"' for information about this
# file.

passwd:      files systemd
group:       files systemd
shadow:      files
gshadow:     files

hosts:       files mdns4_minimal [NOTFOUND=return] dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

nsswitch

Used by GNU C library

Which name server to use

Where it's located

Name Resolution

```
root@Ubuntu:~# cat /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-
resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search members.linode.com
```

/etc/resolv.conf

File to edit DNS servers and
resolving order

Name Resolution

```
root@Ubuntu:~# resolvectl
Global
  Protocols: -LLMNR -mDNS -DNSOverTLS
  DNSSEC=no/unsupported
  resolv.conf mode: stub

Link 2 (eth0)
  Current Scopes: DNS
    Protocols: +DefaultRoute +LLMNR -mDNS -
  DNSOverTLS DNSSEC=no/unsupported
  Current DNS Server: 173.230.128.5
    DNS Servers: 173.230.128.5 23.239.18.5
  66.228.59.5
    DNS Domain: members.linode.com
```

resolvectl

Name Resolution

```
root@Ubuntu:~# dig @8.8.8.8 stormwindstudios

; <<>> DiG 9.18.1-lubuntu1.1-Ubuntu <<>> stormwindstudios@8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 18772
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;stormwindstudios\@8.8.8.8.      IN      A

;; AUTHORITY SECTION:
.                1884     IN      SOA      a.root-servers.net.
nstld.verisign-grs.com. 2022070500 1800 900 604800 86400

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Jul 05 15:03:57 UTC 2022
;; MSG SIZE rcvd: 128
```

dig

Check DNS servers' entries

\$ dig @<server> <host>

host = server trying to
resolve

server = DNS server for
request


```
anakin@localhost:~$ dig stormwindstudios.com
```

```
; <<>> DiG 9.18.1-lubuntu1.1-Ubuntu <<>> stormwindstudios.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 35077
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;stormwindstudios.com.          IN      A

;; ANSWER SECTION:
stormwindstudios.com.  107     IN      A      165.227.62.161

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Jul 12 14:52:15 UTC 2022
;; MSG SIZE rcvd: 65
```

```
anakin@localhost:~$ dig stormwindstudios.com

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> stormwindstudios.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 35077
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;stormwindstudios.com.          IN      A

;; ANSWER SECTION:
stormwindstudios.com.  107     IN      A      165.227.62.161

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Jul 12 14:52:15 UTC 2022
;; MSG SIZE rcvd: 65
```

```
anakin@localhost:~$ dig stormwindstudios.com

; <<>> DiG 9.18.1-lubuntu1.1-Ubuntu <<>> stormwindstudios.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 35077
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;stormwindstudios.com.          IN      A

;; ANSWER SECTION:
stormwindstudios.com.  107     IN      A      165.227.62.161

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Jul 12 14:52:15 UTC 2022
;; MSG SIZE rcvd: 65
```

```
anakin@localhost:~$ dig stormwindstudios.com

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> stormwindstudios.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 35077
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;stormwindstudios.com.          IN      A

;; ANSWER SECTION:
stormwindstudios.com.  107     IN      A      165.227.62.161

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Jul 12 14:52:15 UTC 2022
;; MSG SIZE rcvd: 65
```

```
root@Ubuntu:~# dig stormwindstudios@8.8.8.8

; <<>> DiG 9.18.1-lubuntu1.1-Ubuntu <<>> stormwindstudios@8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 18772
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 65494
;; QUESTION SECTION:
;stormwindstudios\@8.8.8.8.      IN      A

;; AUTHORITY SECTION:
.                1884     IN      SOA      a.root-servers.net. nstld.verisign-grs.com. 2022070500 1800 900 604800 86400

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Jul 05 15:03:57 UTC 2022
;; MSG SIZE rcvd: 128
```

```
anakin@localhost:~$ dig stormwindstudios.com

; <<>> DiG 9.18.1-lubuntu1.1-Ubuntu <<>> stormwindstudios.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 35077
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;stormwindstudios.com.          IN      A

;; ANSWER SECTION:
stormwindstudios.com.  107     IN      A      165.227.62.161

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Jul 12 14:52:15 UTC 2022
;; MSG SIZE rcvd: 65
```

Name Resolution



nslookup
Query DNS record

```
root@Ubuntu:~# nslookup apple.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   apple.com
Address: 17.253.144.10
```

Name Resolution



host

Provides IP of host & owner

```
root@Ubuntu:~# host apple.com
apple.com has address 17.253.144.10
apple.com mail is handled by 10 mal-aaemail-dr-lapp03.apple.com.
apple.com mail is handled by 10 mal-aaemail-dr-lapp02.apple.com.
apple.com mail is handled by 10 mal-aaemail-dr-lapp01.apple.com.
apple.com mail is handled by 10 rn-mailsvcp-ppex-lapp45.apple.com.
apple.com mail is handled by 10 rn-mailsvcp-ppex-lapp44.apple.com.
apple.com mail is handled by 10 rn-mailsvcp-ppex-lapp35.apple.com.
apple.com mail is handled by 10 rn-mailsvcp-ppex-lapp34.apple.com.
apple.com mail is handled by 10 rn-mailsvcp-ppex-lapp24.apple.com.
apple.com mail is handled by 10 rn-mailsvcp-ppex-lapp15.apple.com.
apple.com mail is handled by 10 rn-mailsvcp-ppex-lapp14.apple.com.
```


Name Resolution



whois

Provides IP-organization ownership
Abuse contact

```
root@Ubuntu:~# whois stormwindstudios.com
Domain Name: STORMWINDSTUDIOS.COM
Registry Domain ID: 1545024355_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2022-03-03T14:58:08Z
Creation Date: 2009-03-02T20:15:31Z
Registry Expiry Date: 2023-03-02T20:15:31Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited
```

Review



DNS Name Resolution





Network Monitoring

©2023 by StormWind LLC. All rights reserved.

<https://t.me/learningnets>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Topics



Network troubleshooting



Network monitoring



ping

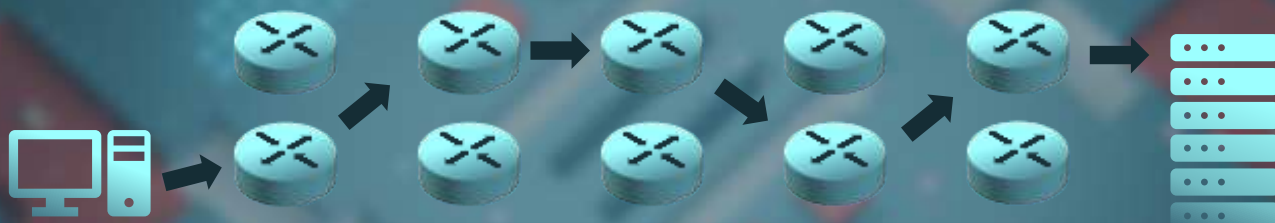
```
root@Ubuntu:~# ping 8.8.8.8 -c 5
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=2.41 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=0.554 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=0.549 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=0.574 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=58 time=1.59 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4051ms
rtt min/avg/max/mdev = 0.549/1.135/2.407/0.751 ms
```



traceroute

Traces path to destination



```
root@Ubuntu:~# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 gw=112282.linode.com (139.177.200.1)  0.186 ms  0.171 ms  0.163 ms
 2 10.204.64.28 (10.204.64.28)  0.280 ms  1.459 ms  10.204.64.27 (10.204.64.27)  0.282 ms
 3 10.204.32.128 (10.204.32.128)  1.449 ms  10.204.32.126 (10.204.32.126)  0.946 ms  10.204.32.128 (10.204.32.128)  1.439 ms
 4 10.204.32.65 (10.204.32.65)  0.630 ms  0.624 ms  10.204.32.67 (10.204.32.67)  0.602 ms
 5 206.71.12.25 (206.71.12.25)  0.735 ms  1.827 ms  1.819 ms
 6 108.170.249.65 (108.170.249.65)  0.608 ms  206.71.12.25 (206.71.12.25)  0.516 ms  108.170.249.97 (108.170.249.97)  1.678 ms
 7 108.170.249.97 (108.170.249.97)  1.659 ms  216.239.47.35 (216.239.47.35)  1.328 ms  108.170.249.65 (108.170.249.65)  0.571 ms
 8 dns.google (8.8.8.8)  0.449 ms  1.638 ms  1.570 ms
```

Traceroute

1

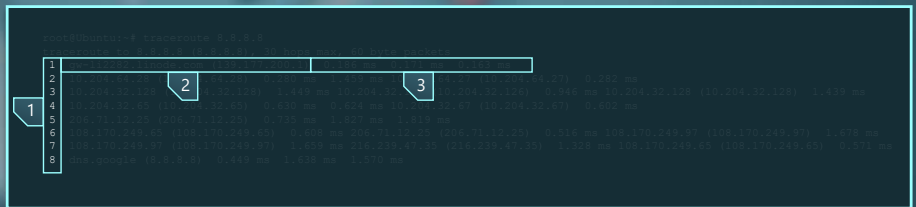
Number of Hops

2

Hop device information

3

Time roundtrip to this hop
3 probes are default





mtr

Live ping + traceroute

```
My traceroute  [v0.95]
Ubuntu.localdomain (173.230.138.127) -> 8.8.8.8 (8.8.8.8)
2022-07-05T15:26:55+0000
Keys:  Help   Display mode  Restart statistics  Order of fields  quit

  Host
  1. gw-112282.linode.com
  2. 10.204.64.28
  3. 10.204.32.132
  4. 10.204.32.71
  5. ae0-100.gw3.atl1.us.linode.com
  6. 206.71.12.25
  7. 108.170.249.97
  8. 142.251.60.221
  9. dns.google

Packets
Loss%  Snt  Last  Avg  Best  Wst  StDev
0.0%   8   0.1  0.2  0.1  0.2  0.0
0.0%   8   0.3  0.5  0.3  1.4  0.4
0.0%   8   2.4  4.5  0.6 14.2  5.9
0.0%   8  14.9  3.9  0.3 14.9  6.4
0.0%   8   0.4  8.6  0.4 33.4 15.1
0.0%   8   0.7  1.0  0.6  1.8  0.5
0.0%   7   1.6  1.8  1.5  2.7  0.4
0.0%   7   1.7  1.0  0.6  1.8  0.5
0.0%   7   1.7  0.7  0.6  1.7  0.4
```


Network Monitoring



tcpdump

Monitor network traffic

-D

Lists interfaces tcpdump can be run on

-c

Stop after set occurrences

Filtering

By protocol

By IP

```
root@Ubuntu:~# tcpdump -c6 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:29:07.562660 IP 50-116-38-249.ip.linodeusercontent.com > 173-230-138-127.ip.linodeusercontent.com: ICMP echo request, id 9, seq 1, length 64
15:29:07.562689 IP 173-230-138-127.ip.linodeusercontent.com > 50-116-38-249.ip.linodeusercontent.com: ICMP echo reply, id 9, seq 1, length 64
15:29:08.564637 IP 50-116-38-249.ip.linodeusercontent.com > 173-230-138-127.ip.linodeusercontent.com: ICMP echo request, id 9, seq 2, length 64
15:29:08.564659 IP 173-230-138-127.ip.linodeusercontent.com > 50-116-38-249.ip.linodeusercontent.com: ICMP echo reply, id 9, seq 2, length 64
15:29:09.588631 IP 50-116-38-249.ip.linodeusercontent.com > 173-230-138-127.ip.linodeusercontent.com: ICMP echo request, id 9, seq 3, length 64
15:29:09.588655 IP 173-230-138-127.ip.linodeusercontent.com > 50-116-38-249.ip.linodeusercontent.com: ICMP echo reply, id 9, seq 3, length 64
6 packets captured
6 packets received by filter
0 packets dropped by kernel
```



netstat

Displays current port and network activity on device

Deprecated (replaced by ss)

Options

-a

Lists which ports are actively listening

-b

which applications are used to open connection

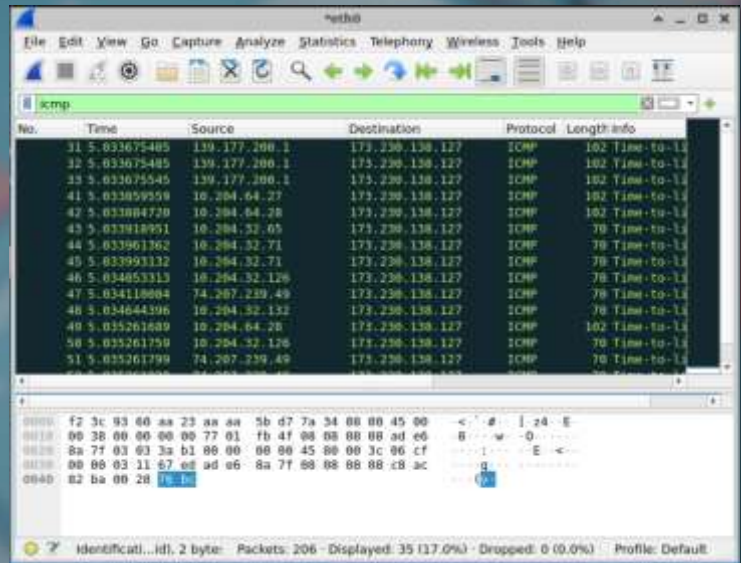
```
root@Ubuntu:~# netstat | less
```

```
Active Internet connections (w/o servers)Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 173-230-138-127.ip:ssh 162.243.170.111:50420   TIME_WAIT
tcp        0      0 173-230-138-127.ip:ssh 107-145-074-003.r:56696 ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]       DGRAM     20770        /run/user/0/systemd/notify
unix  3      [ ]       DGRAM     18048        /run/systemd/notify
unix  2      [ ]       DGRAM     18064        /run/systemd/journal/syslog
unix  15     [ ]       DGRAM     18073        /run/systemd/journal/dev-log
unix  9      [ ]       DGRAM     18075        /run/systemd/journal/socket
unix  3      [ ]       STREAM    CONNECTED    779685
unix  3      [ ]       STREAM    CONNECTED    779269 /run/user/0/bus
unix  3      [ ]       STREAM    CONNECTED    779048 /run/user/0/bus
unix  2      [ ]       DGRAM     2571549
unix  3      [ ]       STREAM    CONNECTED    779620 /run/user/0/bus
unix  3      [ ]       STREAM    CONNECTED    2599393
unix  3      [ ]       STREAM    CONNECTED    779550 /run/user/0/at-spi/bus
unix  3      [ ]       STREAM    CONNECTED    779819
unix  3      [ ]       STREAM    CONNECTED    2571886
unix  3      [ ]       STREAM    CONNECTED    2573324
unix  3      [ ]       STREAM    CONNECTED    779801
unix  3      [ ]       STREAM    CONNECTED    779660 8/tmp/.X11-unix/X0
unix  3      [ ]       STREAM    CONNECTED    779429 /run/user/0/bus
unix  3      [ ]       STREAM    CONNECTED    779278 /run/dbus/system_bus_socket
unix  3      [ ]       STREAM    CONNECTED    779235
unix  3      [ ]       STREAM    CONNECTED    779001
unix  2      [ ]       DGRAM     20678
unix  3      [ ]       STREAM    CONNECTED    2583482
unix  3      [ ]       STREAM    CONNECTED    779083
:
```



Wireshark/Tshark



Review

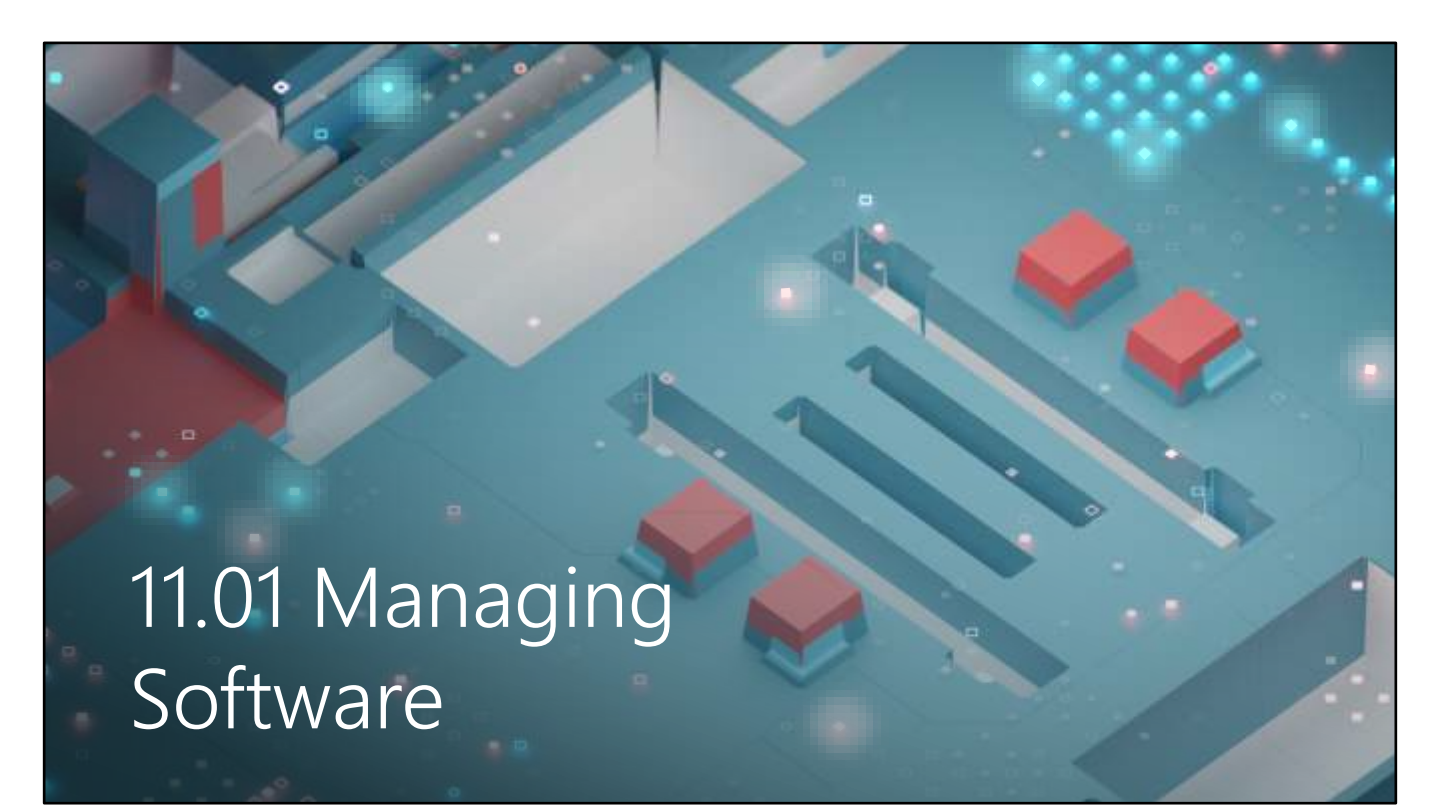


Network troubleshooting



Network monitoring





11.01 Managing Software

©2023 by StormWind LLC. All rights reserved.

<https://t.me/learningnets>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debian & Ubuntu

Low-level

dpkg

Only installs main package (no dependencies)

Advanced package manager

apt

Installs package and its dependencies

apt

Configuration files

/etc/apt/sources.list.d
/etc/apt.conf

Search

`apt search <package>`

Installation

`apt install <package>`

```
root@localhost:~# apt install docker
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  wmdocker
The following NEW packages will be installed:
  docker wmdocker
0 upgraded, 2 newly installed, 0 to remove and 4 not
upgraded.
Need to get 14.3 kB of archives.
After this operation, 58.4 kB of additional disk space
will be used.
Do you want to continue? [Y/n]
```

Debian & Ubuntu

apt

- apt list --upgradable**
Searches for upgradable software
- apt update && apt upgrade**
Upgrades all available software
- apt full-upgrade**
Upgrades and removes vestigial software dependencies

1

```
root@localhost:~# apt list --upgradable
Listing... Done
apparmor/jammy-updates 3.0.4-2ubuntu2.1 amd64
[upgradable from: 3.0.4-2ubuntu2]
libapparmor1/jammy-updates 3.0.4-2ubuntu2.1 amd64
[upgradable from: 3.0.4-2ubuntu2]
python3-libapparmor/jammy-updates 3.0.4-2ubuntu2.1
amd64 [upgradable from: 3.0.4-2ubuntu2]
ubuntu-advantage-tools/jammy-updates 27.9-22.04.1
amd64 [upgradable from: 27.8-22.04.1]
```

2

```
root@localhost:~# apt update && apt upgrade
Hit:1 http://mirrors.linode.com/ubuntu jammy InRelease
Get:2 http://mirrors.linode.com/ubuntu jammy-updates InRelease [109 kB]
Get:3 http://mirrors.linode.com/ubuntu jammy-backports InRelease [99.8 kB]
Get:4 http://mirrors.linode.com/ubuntu jammy-updates/main amd64 Packages [330 kB]
Get:5 http://mirrors.linode.com/ubuntu jammy-updates/restricted amd64 Packages [215 kB]
Get:6 http://mirrors.linode.com/ubuntu jammy-updates/universe amd64 Packages [134 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 999 kB in 1s (1,594 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
4 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  apparmor libapparmor1 python3-libapparmor ubuntu-advantage-tools
4 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,507 kB of archives.
After this operation, 21.5 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```


Debian & Ubuntu

apt

Remove package

apt remove <package>

Does not remove dependencies

Remove package and dependencies

apt purge <package>

Remove unneeded packages

apt autoremove

```
root@localhost:~# apt remove docker
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no
longer required:
  wmdocker
Use 'apt autoremove' to remove it.
The following packages will be REMOVED:
  docker
0 upgraded, 0 newly installed, 1 to remove and 4 not upgraded.
After this operation, 9,216 B disk space will be freed.
Do you want to continue? [Y/n]
```

```
root@localhost:~# apt autoremove
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
```

Debian & Ubuntu

Software information

apt show <package>

Version

Size

Dependencies

```
root@localhost:~# apt show docker
Package: docker
Version: 1.5-2
Priority: optional
Section: universe/x11
Origin: Ubuntu
Maintainer: Ubuntu Developers <ubuntu-devel-
discuss@lists.ubuntu.com>
Original-Maintainer: Paul Tagliamonte <paultag@debian.org>
Bugs: https://bugs.launchpad.net/ubuntu/+filebug
Installed-Size: 9,216 B
Depends: wmdocker
Download-Size: 1,316 B
APT-Manual-Installed: yes
APT-Sources: http://mirrors.linode.com/ubuntu jammy/universe
amd64 Packages
Description: transitional package
 This is a transitional package for system tray docking
 application.
 It can safely be removed.
```

CentOS, RHEL, Fedora

yum

Prior to
CentOS 8
RHEL 8
Fedora 22
.rpm
/etc/yum.conf
/etc/yum.repos.d

dnf

Newer version of yum
CentOS 8 & later
RHEL 8 & later
Fedora 22 & later
.rpm
/etc/dnf/dnf.conf

*Yum and DNF have the same syntax

rpm

Manages local packages

```
rpm -ivh <package.rpm>  
rpm -evh <package>
```

Useful for querying

```
rpm -qf <config file>  
rpm -V <package>
```

Doesn't manage dependencies

dnf

Finding packages

```
dnf search <term>  
dnf list installed
```

Installing packages

```
dnf install <package>
```

dnf

```
[root@CENTOS ~]# dnf install docker
Last metadata expiration check: 1:05:03 ago on Sat 02 Jul 2022 12:06:43 AM UTC.
Dependencies resolved.
=====Package
Architecture      Version           Repository        Size
=====Installing:
podman-docker      noarch            2:4.1.1-1.el9    appstream        41 k
Installing dependencies:
common            x86_64            2:2.1.2-2.el9    appstream        55 k
container-selinux noarch            3:2.188.0-1.el9  appstream        48 k
containers-common x86_64            2:1-39.el9       appstream        114 k
criu              x86_64            3.17-2.el9       appstream        544 k
criu-libs        x86_64            3.17-2.el9       appstream        33 k
crun             x86_64            1.4.5-2.el9       appstream        187 k
fuse-common      x86_64            3.10.2-5.el9     baseos           9.0 k
fuse-overlayfs   x86_64            1.8.2-1.el9       appstream        72 k
fuse3            x86_64            3.10.2-5.el9     appstream        54 k
fuse3-libs       x86_64            3.10.2-5.el9     appstream        93 k
libnet           x86_64            1.2-6.el9         appstream        59 k
libslirp        x86_64            4.4.0-4.el9       appstream        69 k
netavark         x86_64            2:1.0.1-39.el9   appstream        2.0 M
podman           x86_64            2:4.1.1-1.el9    appstream        12 M
podman-catatonit x86_64            2:4.1.1-1.el9    appstream        351 k
protobuf-c       x86_64            1.3.3-12.el9     baseos           36 k
shadow-utils-subid x86_64            2:4.9-4.el9      baseos           88 k
slirp4netns      x86_64            1.2.0-2.el9       appstream        47 k
yajl             x86_64            2.1.0-20.el9     appstream        38 k
Installing weak dependencies:
aardvark-dns     x86_64            2:1.0.1-39.el9   appstream        1.0 M
tar              x86_64            2:1.34-3.el9     baseos           890 k

Transaction Summary
=====Install 22
Packages

Total download size: 18 M
Installed size: 65 M
Is this ok [y/N]:
```

dnf

Upgrading packages

dnf check-update

Looks for updates

dnf upgrade

Upgrades all packages

dnf upgrade <package>

Upgrades specific
package

```
Obsoleting Packages
grub2-tools.x86_64                1:2.06-32.el9      baseos
  grub2-tools.x86_64              1:2.06-25.el9      @baseos
grub2-tools-efi.x86_64            1:2.06-32.el9      baseos
  grub2-tools.x86_64              1:2.06-25.el9      @baseos
grub2-tools-extra.x86_64          1:2.06-32.el9      baseos
  grub2-tools.x86_64              1:2.06-25.el9      @baseos
grub2-tools-minimal.x86_64        1:2.06-32.el9      baseos
  grub2-tools.x86_64              1:2.06-25.el9      @baseos
[root@CENTOS ~]#
```

```
harfbuzz                625 k      x86_64      2.7.4-5.el9
baseos
kernel-core              35 M        x86_64      5.14.0-119.el9
baseos
kernel-modules           22 M        x86_64      5.14.0-119.el9
baseos
libpng                   117 k       x86_64      2:1.6.37-12.el9
baseos
python3-gobject-base-noarch 161 k       noarch      3.40.1-6.el9
baseos
```

Transaction Summary

=====

Install 10 Packages

Upgrade 140 Packages

Total download size: 398 M

Is this ok [y/N]:

dnf

Removing packages

```
dnf remove <package>  
    Only removes package  
dnf autoremove  
    Remove unneeded dependencies  
dnf autoremove <package>  
    Removes package and dependencies  
dnf remove --duplicates  
    Remove duplicate packages  
dnf history  
    View history of prior dnf commands  
dnf history undo [last | number]  
    Undo last dnf command or specific entry  
    from history
```


OpenSuse

Zypper

Installing packages

zypper install <package>

Updating packages

zypper update

Updates all packages

zypper update <package>

Updates specific package

Deleting packages

zypper remove <package>

```
zypper install docker
Retrieving repository 'Update repository of openSUSE Backports' metadata
.....[done]Building repository 'Update repository
of openSUSE Backports' cache
.....[done]Retrieving repository 'Non-OSS
Repository' metadata
.....[done]Building
repository 'Non-OSS Repository' cache
.....[done]Retrieving
repository 'Main Repository' metadata
.....[done]Building
repository 'Main Repository' cache
.....[done]Retrievin
g repository 'Update repository with updates from SUSE Linux Enterprise 15' metadata
.....[done]Building repository 'Update repository with updates from
SUSE Linux Enterprise 15' cache .....[done]Retrieving repository
'Main Update Repository' metadata
.....[done]Building repository
'Main Update Repository' cache
.....[done]Retrieving
repository 'Update Repository (Non-Oss)' metadata
.....[done]Building repository
'Update Repository (Non-Oss)' cache
.....[done]Loading repository
data...
Reading installed packages...
Resolving package dependencies...

The following 3 recommended packages were automatically selected:
  criu git-core lvm2

The following 24 NEW packages are going to be installed:
  apparmor-parser apparmor-parser-lang catatonit containerd criu docker docker-bash-
completion git-core iptables
  libip6tc2 libjansson4 liblvm2cmd2_03 libnet9 libnetfilter_conntrack3 libnftnlk0
libnftables1 libnftnl11
  libprotobuf-c1 libshaildetectcoll1 lvm2 python3-ipaddr python3-protobuf runc
xtables-plugins

24 new packages to install.
Overall download size: 55.1 MiB. Already cached: 0 B. After the operation, additional
261.9 MiB will be used.
Continue? [y/n/v/...? shows all options] (y):
```

Sandboxed application managers

Non-distro specific
Everything is built in
No separate dependencies
Applications are separate from another

snapt

snapt install <package>

snapt refresh <package>

Reinstall packages

snapt list

List all snapt applications

snapt revert <package>

snapt remove <package>

```
root@localhost:~# snapt list
Name      Version  Rev    Tracking    Publisher    Notes
blender   3.2.0    2474   latest/stable  blenderfoundation/  classic
core18     20220428  2409   latest/stable  canonical/         base
snapt      2.56     16010  latest/stable  canonical/         snapt
```

flatpak

```
flatpak search <package>
```

```
flatpak install <package>
```

```
flatpak update <package>
```

```
flatpak uninstall <package>
```

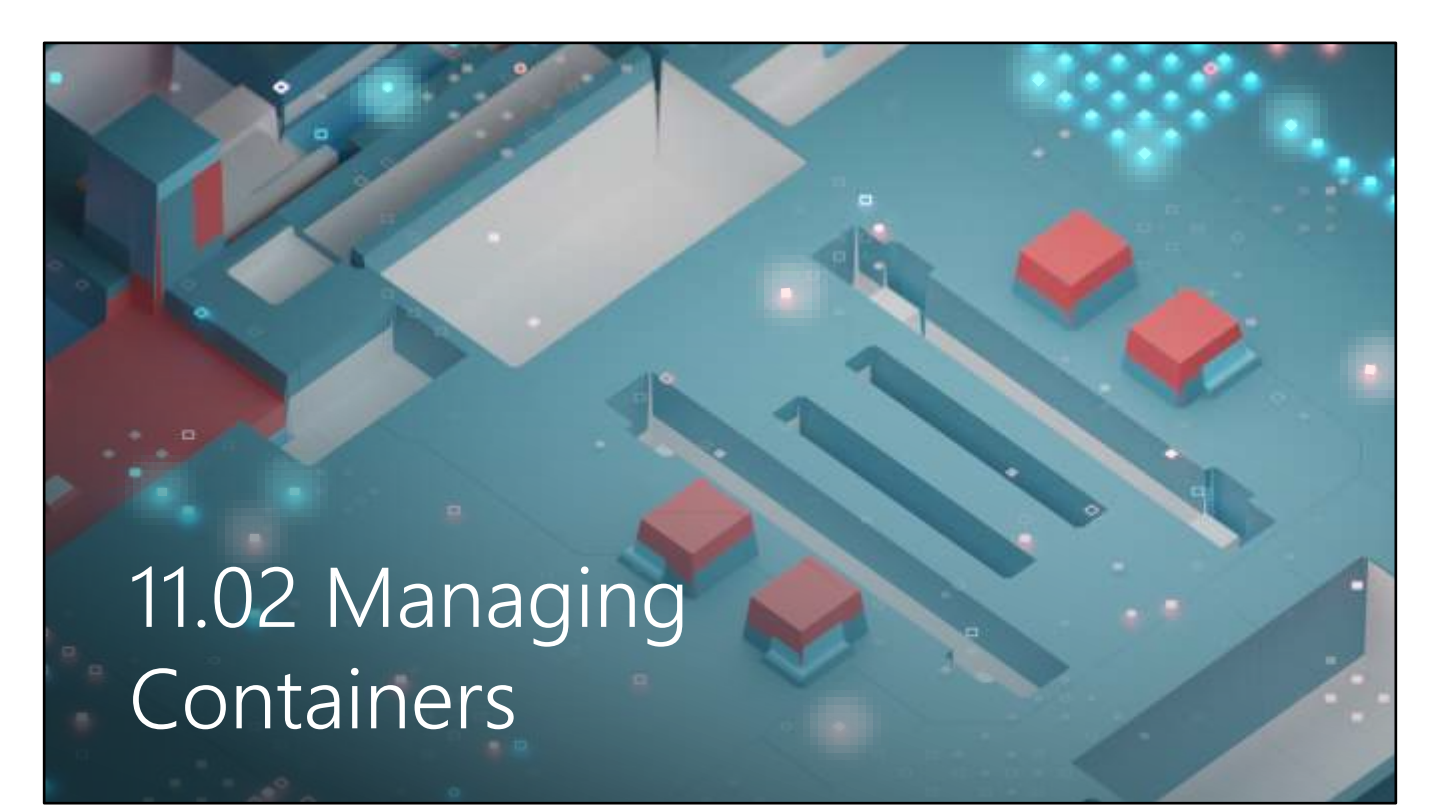
AppImage Lab

Go to appimage.org

Download the example software

Make it executable and run





11.02 Managing Containers

Containerization

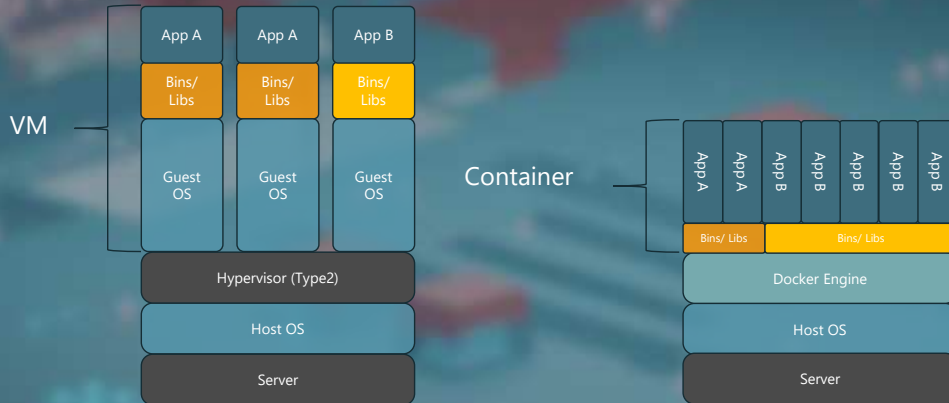
Containers provide a consistent environment in which to run applications

- Segmented
- Shared kernel (lower overhead)
- Bare-bones filesystem with dependencies

Containerization Platforms

- Docker
- podman

Virtualization vs. Containerization



Docker – Pulling Images and Running Containers

Pulling is downloading a container image from a registry

```
docker pull ubuntu
docker pull ubuntu:20.04
```

Listing pulled images

```
docker images
```

Run container from an image

```
docker run -it ubuntu
docker run -d ubuntu
```

```
root@localhost:~# docker pull ubuntu
Trying to pull docker.io/library/ubuntu:latest...
Getting image source signatures
Copying blob 3428fab9 done
Copying blob 9fab3df2a done
...
```

```
root@localhost:~# docker run -d ubuntu
30ecd53813a59f4e69bfa82b5f774b06a9bbdba1
```

Docker – Viewing and Stopping Containers

List containers

`docker ps` (running only)
`docker ps -a` (running and otherwise)

View containers' configs

`docker inspect ubuntu`

Stop a container

`docker stop <container>`

```
root@localhost:~# docker ps

CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS
9b6247364a03   busybox   bash      2 minutes ago   Up

root@localhost:~# docker stop 9b6247364a03
9b6247364a03

root@localhost:~# docker ps -a

CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS
9b6247364a03   busybox   bash      3 minutes ago   Exited
```

Docker – Removing and Pruning Images

Remove a specific container

```
docker rm <container>
```

Prune unused images

```
docker image prune
```

Remove specific image

```
docker rmi <image>
```

```
root@localhost:~# docker ps -a
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS
9b6247364a03	busybox	bash	3 minutes ago	Exited

```
root@localhost:~# docker rm 9b6247364a03  
9b6247364a039bfa82b5f774b06a9bbdbal
```

```
root@localhost:~# docker ps -a
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS

Docker – Port Forwarding and Copying Files

Copying files from container

```
docker cp <container>:/container_path/ /host_path/
```

Port forwarding

```
docker run -p <host>:<container> <image>
```

```
root@localhost:~# docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED
9b6247364a03	busybox	bash	3 minutes ago

```
root@localhost:~# docker cp 9b6247364a03:/test.jpg .
```

```
root@localhost:~# ls
test.jpg
```

podman – Pulling Images and Running Containers

Pulling is downloading a container image from a registry

```
podman pull ubuntu  
podman pull ubuntu:20.04
```

Listing pulled images

```
podman images
```

Run container from an image

```
podman run -it ubuntu  
podman run -d ubuntu
```

```
root@localhost:~# podman pull ubuntu  
Trying to pull docker.io/library/ubuntu:latest...  
Getting image source signatures  
Copying blob 3428fab9 done  
Copying blob 9fab3df2a done  
...
```

```
root@localhost:~# podman run -d ubuntu  
30ecd53813a59f4e69bfa82b5f774b06a9bbdba1
```

podman – Viewing and Stopping Containers

List containers

podman ps (running only)
podman ps -a (running and otherwise)

View containers' configs

podman inspect ubuntu

Stop a container

podman stop <container>

```
root@localhost:~# podman ps

CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS
9b6247364a03   busybox   bash     2 minutes ago   Up

root@localhost:~# podman stop 9b6247364a03
9b6247364a03

root@localhost:~# podman ps -a

CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS
9b6247364a03   busybox   bash     3 minutes ago   Exited
```

podman – Removing and Pruning Images

Remove a specific container

```
podman rm <container>
```

Prune unused images

```
podman image prune
```

Remove specific image

```
podman rmi <image>
```

```
root@localhost:~# podman ps -a
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS
9b6247364a03	busybox	bash	3 minutes ago	Exited

```
root@localhost:~# podman rm 9b6247364a03  
9b6247364a039bfa82b5f774b06a9bbdb1
```

```
root@localhost:~# podman ps -a
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS

podman – Port Forwarding and Copying Files

Copying files from container

```
podman cp <container>:/container_path /host_path
```

Port forwarding

```
podman run -p <host>:<container> <image>
```

```
root@localhost:~# podman ps
CONTAINER ID   IMAGE     COMMAND   CREATED
9b6247364a03   busybox   bash     3 minutes ago
root@localhost:~# podman cp 9b6247364a03:/test.jpg .
root@localhost:~# ls
test.jpg
```


Docker and Kubernetes

Docker

Containerization platform

Used to build, deploy, and run containers

Not terribly scalable on its own

Kubernetes

Orchestration of containers (including Docker containers) across many hosts

Provides scalability and high availability for containerized applications

Service meshes provide load balancing, security, and monitoring for Kubernetes environments



Security Practices

©2023 by StormWind LLC. All rights reserved.

<https://t.me/learning013ts>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Topics



Firewalls

Stateless
Stateful
Zones



Hardening



SSH



PKI



Hashing



Authentication

Stateless Firewall

Packet filtering

MAC address

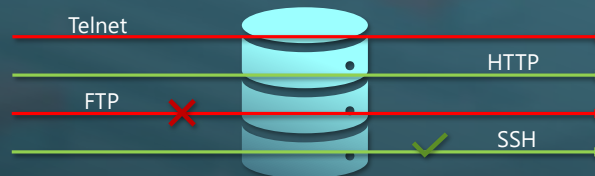
IP address

Port number

Protocol

Implicit deny

Implicit allow



Stateful Firewall

Maintains state

Where did the request originate from?

Is this a new or ongoing connection?



Firewall zones



Digital Certificates

Also known as public key certificates

Contents

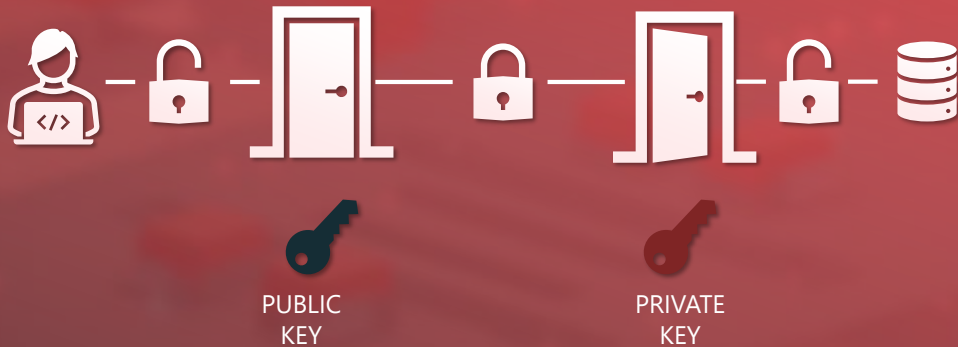
- Public key
- Owner identity
- Additional information
- Digital signatures attesting to authenticity

Not to be confused with digital signatures

- Signature proves authenticity of a message
- Certificate proves identity of a user or system



Managing Public Key Infrastructure (PKI) Certificates



Certification Authority

TRUSTED third party

Issues Certificates

- Creates and signs them

- Publishes current certificates

Issues Certificate Revocation Lists (CRLs)

- List of invalid (revoked) certificates

- Online Certificate Status Protocol (OCSP)

Maintains archives of status information

May retain copy of data encryption private key, for purposes of key recovery

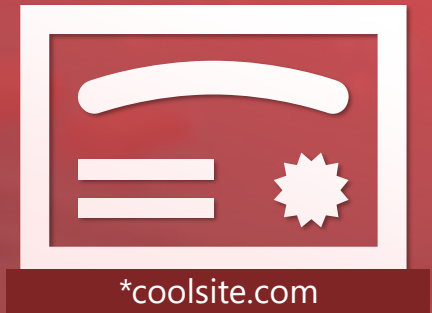
- Government requirement

Managing Public Key Infrastructure (PKI) Certificates

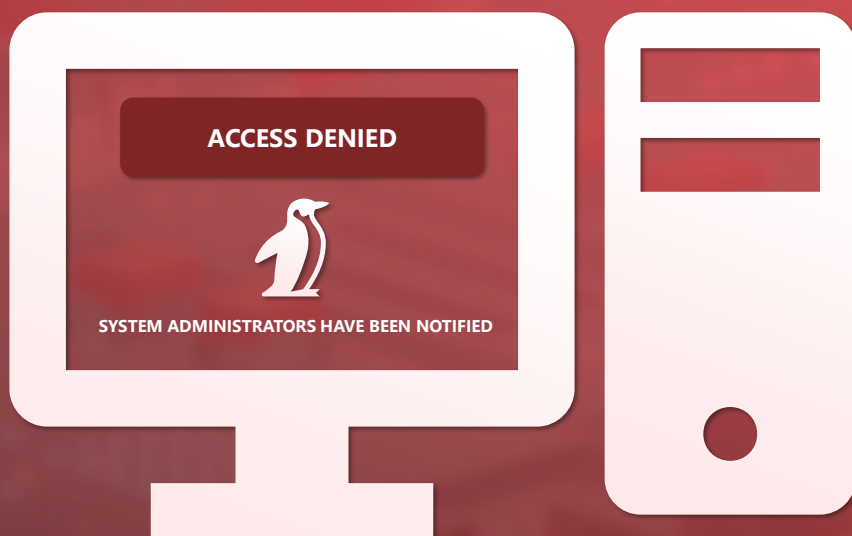
Wildcard Certificate

Used for Multiple Domains

*







Single Sign-on (SSO)

Allows you to sign in once and not repeatedly for multiple applications by combining login screens into one.



Microsoft

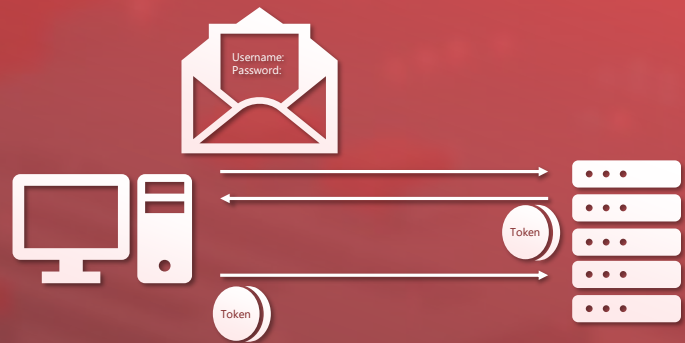
Office 365



Tokens

Authentication information stored in a cryptographic string

Used instead of entering username and password for authentication



Multifactor Authentication

Improves security by adding authentication factors such as:

Something you have

Phone

Keycard

Something you know

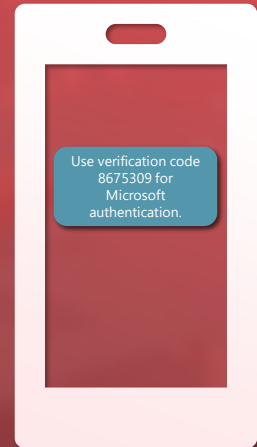
Security question

Password

Something you are

Fingerprint

FaceID



Pluggable Authentication Modules (PAM)

Various Modules that handle authentication tasks of applications

Administrator can set authentication parameters for applications

`/etc/pam.conf`

`/etc/pam.d/`

If directory exists, `/etc/pam.conf` will be ignored

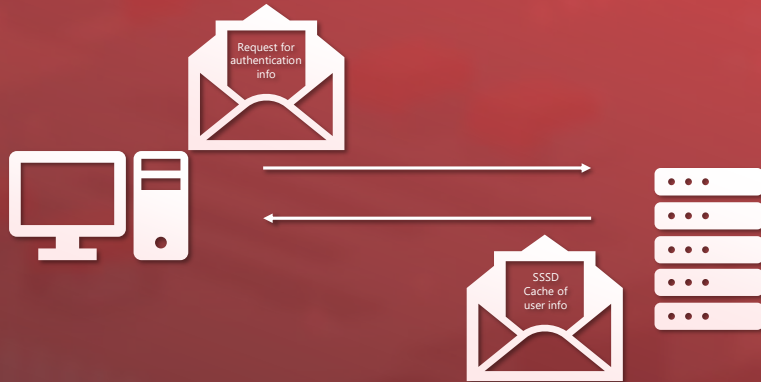
```
anakin@localhost:~$ ls /etc/pam.d/  
chfn      chsh      common-auth      common-session      cron      newusers  passwd  runuser  sshd  sudo  su-l  
chpasswd  common-account  common-password  common-session-noninteractive  login  other  polkit-1  runuser-1  su  sudo-i  vmtoclsd
```


System Security Services Daemon (SSSD)

Access remote directories and authentication mechanisms

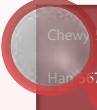
LDAP

Active Directory



Lightweight Directory Access Protocol (LDAP)

Used to organize and request information in a hierarchical directory



Chewy 549-146-5464	Moff 546-283-2316
Han 357-863-4259	Vader 246-516-4732
Lando 321-578-6214	Palpatine 164-565-4140
Leia 257-315-6489	Jabba 356-981-0254
Luke 257-315-6489	Fett 321-568-9891

Security Scanning

Regularly scan for vulnerabilities and malware

Viruses

Ransomware

Rootkits

Programs

Lynis

chkrootkit

rkhunter

```
[+] Boot and services
-----
- Service Manager: [ systemd ]
- Checking presence GRUB2: [ FOUND ]
- Checking for password protection: [ NONE ]
- Check running services (systemctl): [ DONE ]
  Result: found 20 running services
- Check enabled services at boot (systemctl): [ DONE ]
  Result: found 43 enabled services
- Check startup files (permissions): [ OK ]
- Running 'systemd-analyze security'
  - ModemManager.service: [ MEDIUM ]
  - apport.service: [ UNSAFE ]
  - cloud-init-hotplugd.service: [ UNSAFE ]
  - cron.service: [ UNSAFE ]
  - dbus.service: [ UNSAFE ]
  - dm-event.service: [ UNSAFE ]
  - dmesg.service: [ UNSAFE ]
  - emergency.service: [ UNSAFE ]
  - getty@tty1.service: [ UNSAFE ]
  - haveged.service: [ PROTECTED ]
```

Secure Boot (UEFI)

Only signed software is loaded during boot

Prevents unsigned (potentially malicious) code from being run

Mitigates risk of low-level malware such as rootkits

SSH

Secure shell

Enables encrypted remote access

```
C:\Users\anakin> ssh  
root@50.116.34.204
```

Encrypted Tunnel



SSH

SSH configuration files

`/etc/ssh/sshd_config`

Server configuration file

`/etc/ssh/ssh_config`

Global client configuration file

`~/.ssh/config`

User-specific client configuration file

`~/.ssh/known_hosts`

`~/.ssh/authorized_keys`

SSH

Configuration files

ssh-keygen

Generates keypairs

ssh-copy-id

Copy public key to remote machine

ssh-add

Adds private key to authentication agent

```
[root@CENTOS ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:KxOe6WsunN7UyNuzigvumBS6Ew9vqkl+9ldzHf1ne74 root@CENTOS.localdomain
The key's randomart image is:
+---[RSA 3072]-----+
|
|
|
| . o o . S . . o . |
|+ o =.+... . . |
|oB.+ o*... o |
|B=.*.*o+ . |
|O*+.*o E. |
+-----[SHA256]-----+
```

SSH Tunneling

X11 forwarding

Run GUI Applications remotely
Enable or disable in sshd_config

```
X11Forwarding yes  
#X11DisplayOffset 10  
#X11UseLocalhost yes
```



Review



Firewalls

Stateless
Stateful
Zones



Hardening



SSH



PKI



Hashing



Authentication





13.1 Bash Scripting

Topics



Shell script elements



Common script utilities



Environment variables

Shell Script Elements

Shell parameter expansion

Globbing with *

Matches zero or more characters

ls *.png

```
root@Ubuntu:/home# ls
file1.txt  file3.txt  investing.sh  OSI      quinjet.sh  sourcescript.sh  trip2.jpeg  trip4.jpeg  vacation2.png  vacation4.png
file2.txt  filexample  loops.sh     OSI_Model  savings.sh  tripl.jpeg      trip3.jpeg  vacation1.png  vacation3.png
root@Ubuntu:/home# ls *.png
vacation1.png  vacation2.png  vacation3.png  vacation4.png
```

Shell Script Elements

Brace expansions with { }
Generates list of strings

```
root@Ubuntu:/home# echo {1,2,3,4,5}
1 2 3 4 5
root@Ubuntu:/home# echo {1..5}
1 2 3 4 5
root@Ubuntu:/home# echo {a..z}
a b c d e f g h i j k l m n o p q r s t u v w x y z
root@Ubuntu:/home# echo {z..a}
z y x w v u t s r q p o n m l k j i h g f e d c b a
root@Ubuntu:/home# touch brace{1..5}.txt
root@Ubuntu:/home# ls brace*
brace1.txt brace2.txt brace3.txt brace4.txt brace5.txt
```

Shell Script Elements

Arithmetic Comparisons

Place expression in square brackets

[num1 <option> num2]

-eq

equal

-gt

greater than

-ge

greater than or equal to

-lt

less than

-le

less than or equal to

-ne

not equal

Shell Script Elements

Other Comparisons

Place expression in square brackets

[**var1** <option> **var2**]

=

Equal

!=

Not equal

-n

Greater than 0

-z

0

-e

File exists

-f

File exists and is a regular file

-d

File exists and is a directory

Shell Script Elements

Variables

Substitute value of something
for another

Syntax

```
<variable>="output"  
${<variable>}
```

```
#!/bin/bash  
  
E="this is an Example of a simple Variable"  
  
echo $E
```


read

Can ask user what variable should be:

```
#!/bin/bash  
  
echo "New Username?"  
  
read username  
  
useradd $username
```

Shell Script Elements

Regular Expressions

Text patterns used with grep, vim, awk, and sed to filter and parse data efficiently

Shell Script Elements

Pipes (|) chain multiple commands together

`CommandOne | CommandTwo`

Output of CommandOne is input to CommandTwo

Shell Script Elements

Boolean operators

`||`

OR

`a || b`

b is run if a is not successful

`&&`

AND

`a && b`

b is run if a is successful

Shell Script Elements

stdout – Standard (non-error) output

Redirect stdout to file

>

Overwrites file

>>

Appends file

```
root@Ubuntu:~/ex# ls
root@Ubuntu:~/ex# date > example.txt
root@Ubuntu:~/ex# ls
example.txt
root@Ubuntu:~/ex# cat example.txt
Tue Jul  5 04:05:33 PM UTC 2022
root@Ubuntu:~/ex# date >> example.txt
root@Ubuntu:~/ex# cat example.txt
Tue Jul  5 04:05:33 PM UTC 2022
Tue Jul  5 04:05:52 PM UTC 2022
```

Shell Script Elements

Here documents

Command << **Token**
Text
Token

```
cat << _theend_  
  
7 - Application  
6 - Presentation  
5 - Session  
4 - Transport  
3 - Network  
2 - Data Link  
1 - Physical  
  
_theend_
```

Common Script Utilities

awk

Powerful text editing and analysis tool

awk '{print}' <filename>

Print full file like cat

\$<field number>

Prints column

Column separated by space

\$NF will print last field

awk -F ':' '{print \$1,\$6}' /etc/passwd

-F defines delimiter

```
root@Ubuntu:~# awk '{print}' Employees.txt
John Ceo John@wesellstuff.com
Jacob VP Jacob@wesellstuff.com
Jingleheimer Manager
Jingleheimer@wesellstuff.com
Schmidt Engineer Schmidt@wesellstuff.com
```

```
root@Ubuntu:~# awk '{print $1,$2}'
Employees.txt
John Ceo
Jacob VP
Jingleheimer Manager
Schmidt Engineer
```

Common Script Utilities

sed

Stream editor (edit files line-by-line)

Outputs only to console by default

sed -i 's/old/new/' <file>

Replace first "old" on each line

sed -i 's/old/new/g' <file>

Replace every "old" in file

```
root@Ubuntu:~# cat sedexample.sh
this
is
a example
of
sed changing things lets change orange to red

root@Ubuntu:~# sed -i 's/orange/red/' sedexample.sh

root@Ubuntu:~# cat sedexample.sh
this
is
a example
of
sed changing things lets change red to red

root@Ubuntu:~# sed -i 's/red/orange/g' sedexample.sh

root@Ubuntu:~# cat sedexample.sh
this
is
a example
of
sed changing things lets change orange to orange
```


Common Script Utilities

find - search for file and directories throughout system

-name

Search by file name

-empty

Find empty files/directories

-perm

Search by permissions

-mtime

Modified less than (-days) or more than (+days)
ago

-exec command {} \;

Run **command** on each result

```
root@Ubuntu:~# find ./ -type f -name  
"*.txt" -exec grep 'PASSWORD' {} \;  
PASSWORD LIST:  
MASTER PASSWORD: P@SSW0rd
```

Common Script Utilities

xargs

Output from CommandOne is passed though CommandTwo

Default command2 is **echo**

```
root@Ubuntu:~/ex# ls
example.txt
root@Ubuntu:~/ex# echo "files pictures
videos" | xargs mkdir
root@Ubuntu:~/ex# ls -l
total 16
-rw-r--r-- 1 root root 64 Jul 5 16:05
example.txt
drwxr-xr-x 2 root root 4096 Jul 5 18:00
files
drwxr-xr-x 2 root root 4096 Jul 5 18:00
pictures
drwxr-xr-x 2 root root 4096 Jul 5 18:00
videos
```

Common Script Utilities

grep

Regular expression filtering

Best practice single quotes

```
root@Ubuntu:~/ex# grep 'example | cool'  
example.txt  
Let's show output of searching for  
example | cool
```

Common Script Utilities

egrep

Extended expression filtering

+ ? |

```
root@Ubuntu:~/mess# ls
100.txt 15.txt 20.txt 26.txt 31.txt 37.txt 42.txt 48.txt
53.txt 59.txt 64.txt 6.txt 75.txt 80.txt 86.txt 91.txt
97.txt   trip3.jpeg
10.txt  16.txt 21.txt 27.txt 32.txt 38.txt 43.txt 49.txt
54.txt  5.txt  65.txt 70.txt 76.txt 81.txt 87.txt 92.txt
98.txt   trip4.jpeg
11.txt  17.txt 22.txt 28.txt 33.txt 39.txt 44.txt 4.txt
55.txt  60.txt 66.txt 71.txt 77.txt 82.txt 88.txt 93.txt
99.txt   vacation1.png
12.txt  18.txt 23.txt 29.txt 34.txt 3.txt  45.txt 50.txt
56.txt  61.txt 67.txt 72.txt 78.txt 83.txt 89.txt 94.txt
9.txt    vacation2.png
13.txt  19.txt 24.txt 2.txt  35.txt 40.txt 46.txt 51.txt
57.txt  62.txt 68.txt 73.txt 79.txt 84.txt 8.txt  95.txt
trip1.jpeg vacation3.png
14.txt  1.txt  25.txt 30.txt 36.txt 41.txt 47.txt 52.txt
58.txt  63.txt 69.txt 74.txt 7.txt  85.txt 90.txt 96.txt
trip2.jpeg vacation4.png
root@Ubuntu:~/mess# ls | egrep "jpeg|png"
trip1.jpeg
trip2.jpeg
trip3.jpeg
trip4.jpeg
vacation1.png
vacation2.png
vacation3.png
vacation4.png
```

Common Script Utilities

tee

Copy output to files

```
root@Ubuntu:~# cat OSI_Model.txt | grep 7 | tee Layer7.txt
Application.txt
7 - Application
root@Ubuntu:~# cat Layer7.txt
7 - Application
root@Ubuntu:~# cat Application.txt
7 - Application
```

Common Script Utilities

wc

Count words, lines and characters in files

- c** Byte count
- m** Character count
- l** Line count
- w** Word count

```
root@Ubuntu:~# cat woodchuck.txt
How much wood would a woodchuck chuck if a woodchuck could chuck
wood.
root@Ubuntu:~# wc woodchuck.txt
1 13 71 woodchuck.txt
```

Common Script Utilities

```
root@Ubuntu:~# cut -d : -f 1,6 /etc/passwd |  
tail -10  
tom:/home/tom  
Hank:/home/Hank  
rtkit:/proc  
avahi:/run/avahi-daemon  
saned:/var/lib/saned  
colord:/var/lib/colord  
pulse:/run/pulse  
dnsmasq:/var/lib/misc  
_flatpak:/nonexistent  
frank:/home/frank
```

cut remove fields out of
output
-d specifies delimiter

```
root@Ubuntu:~# awk -F : '$3 > 999 {print $1}'  
/etc/passwd | sort -d  
engineer  
frank  
guest  
Hank  
josh  
nobody  
patrick  
tom
```

sort sorts output
-n numeric
-d dictionary

Common Script Utilities

```
root@Ubuntu:~# head -n 4 OSI_Model.txt
7 - Application
6 - Presentation
5 - Session
4 - Transport
```

head prints top line(s)
of file

```
head -n 4 <file>
```

```
root@Ubuntu:~# tail -n 3 OSI_Model.txt
3 - Network
2 - Data Link
1 - Physical
```

tail prints bottom
line(s) of file

```
tail -n 3 <file>
```


Environment Variables

```
root@Ubuntu:~# env
SHELL=/bin/bash
PWD=/root
LOGNAME=root
XDG_SESSION_TYPE=tty
MOTD_SHOWN=pam
HOME=/root
LANG=en_US.UTF-8
```

Environment variables

Exported variable

Any sub-shells can use variable,
including scripts

System created

User can create their own

env displays environment variables

Environment Variables

```
root@Ubuntu:~# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

\$PATH

Directories system will search for when running commands

Environment Variables

```
root@Ubuntu:~# echo $SHELL  
/bin/bash
```

\$SHELL
Current shell being used

Environment Variables

```
root@Ubuntu:~# useradd mary
root@Ubuntu:~# echo $?
0
root@Ubuntu:~# useradd Hank
useradd: user 'Hank' already exists
root@Ubuntu:~# echo $?
9
```

After a command runs it generates an exit code

echo \$? will show exit code

0 – Command was executed successfully

1 – General error

Anything else is application-specific

Shell Script Elements

```
#!/bin/bash

#ASKS USER NEW USERNAME
echo "What is the new Username"
read Username

#CREATES USERNAME
useradd $Username

#provide message
if [ $? -eq 0 ];
then
    echo "User created successfully"
fi

#SET USER PASSWORD
passwd $Username
```

```
root@Ubuntu:~/ex# bash ./createuser.txt
What is the new Username
nathan
User created successfully
New password:
Retype new password:
passwd: password updated successfully
```

Conditionals

if

Verify condition is true

Must be closed by a **fi**

Shell Script Elements

```
#!/bin/bash

echo "Authentication required"

read answer

if test "$answer" == "Point Break"
then
    echo " Welcome, Point Break"
else
    echo " Access Denied"
fi
```

```
root@Ubuntu:~/ex# bash ./quinjet.sh
Authentication required
Thor
Access Denied
root@Ubuntu:~/ex# bash ./quinjet.sh
Authentication required
Strongest Avenger
Access Denied
root@Ubuntu:~/ex# bash ./quinjet.sh
Authentication required
Point Break
Welcome, Point Break
```

Conditionals

test

Compare values

else

If answer is different, then run

Shell Script Elements

```
#!/bin/bash

echo "Authentication required"

read answer

case $answer in
    "Point Break")      echo "Welcome, Point Break" ;;
    "Strongest Avenger") echo "You are not the Hulk"
                        sleep 1
                        echo "Access Denied" ;;
    *)                  echo "Access Denied" ;;
esac
```

```
root@Ubuntu:~/ex# bash ./quinjet.sh
Authentication required
Thor
Access Denied
root@Ubuntu:~/ex# bash ./quinjet.sh
Authentication required
Strongest Avenger
You are not the Hulk
Access Denied
root@Ubuntu:~/ex# bash ./quinjet.sh
Authentication required
Point Break
Welcome, Point Break
```

Conditionals

case - multiple input options

;;

Separates options

***)**

Catch-call

esac

Closes case

Shell Script Elements

```
root@Ubuntu:~/ex# echo $USER
root
root@Ubuntu:~/ex# cat sourcescript.sh
#!/bin/bash

USER=engineering

echo $USER

root@Ubuntu:~/ex# source sourcescript.sh
engineering
root@Ubuntu:~/ex# echo $USER
engineering
```

source

Executes scripts and adds variables to user's current shell

Shell Script Elements

```
#!/bin/bash

#amount in savings
savings=500

#month count
m=1

#adding $500 a month into savings until Reaching $6,000

while [ $savings -le 6000 ]
do
    echo "Month$m =" "$savings"
    m=$(( $m+1 ))
    savings=$(( savings+500 ))
done
```

```
root@Ubuntu:~/ex# bash ./savings.sh
Month1 = 500
Month2 = 1000
Month3 = 1500
Month4 = 2000
Month5 = 2500
Month6 = 3000
Month7 = 3500
Month8 = 4000
Month9 = 4500
Month10 = 5000
Month11 = 5500
Month12 = 6000
```

Loops

while runs command while condition is true

Shell Script Elements

```
#!/bin/bash

#amount investing per year (ROTH LIMIT)
i=6000

#age
echo "How old are you?"
read age

#Retirement age
echo "When do you want to retire?"
read retire

#interest rate
echo "What is the interest rate average?"
Ex:
9% = 09
10% = 10"
read rate

echo "Note: this calculation is if 6000 investment is
added at end of year."

sleep 2

#investment
until [ $age -gt $retire ]
do
    echo "$age years old you will have $i invested
    i=$(echo 6000+$i*1.$rate | bc )
    age=$(( $age+1 ))
done
```

Loops

until runs command while
condition is not true

```

root@Ubuntu:~/ex# bash ./investing.sh
How old are you?
24
When do you want to retire?
65
What is the interest rate average?
Ex:
9% = 09
10% = 10
07
Note: if 6000 investment is added at end of year.
24 years old you will have 6000 invested
25 years old you will have 12420.00 invested
26 years old you will have 19289.40 invested
27 years old you will have 26639.65 invested
28 years old you will have 34504.42 invested
29 years old you will have 42919.72 invested
30 years old you will have 51924.10 invested
31 years old you will have 61558.78 invested
32 years old you will have 71867.89 invested
33 years old you will have 82898.64 invested
34 years old you will have 94701.54 invested
35 years old you will have 107330.64 invested
36 years old you will have 120843.78 invested
37 years old you will have 135302.84 invested
38 years old you will have 150774.03 invested
39 years old you will have 167328.21 invested
40 years old you will have 185041.18 invested
41 years old you will have 203994.06 invested
42 years old you will have 224273.64 invested
43 years old you will have 245972.79 invested
44 years old you will have 269190.88 invested
45 years old you will have 294034.24 invested
46 years old you will have 320616.63 invested
47 years old you will have 349059.79 invested
48 years old you will have 379493.97 invested
49 years old you will have 412058.54 invested
50 years old you will have 446902.63 invested
51 years old you will have 484185.81 invested

```

```

52 years old you will have 524078.81 invested
53 years old you will have 566764.32 invested
54 years old you will have 612437.82 invested
55 years old you will have 661308.46 invested
56 years old you will have 713600.05 invested
57 years old you will have 769552.05 invested
58 years old you will have 829420.69 invested
59 years old you will have 893480.13 invested
60 years old you will have 962023.73 invested
61 years old you will have 1035365.39 invested
62 years old you will have 1113840.96 invested
63 years old you will have 1197809.82 invested
64 years old you will have 1287656.50 invested
65 years old you will have 1383792.45 invested

```

Shell Script Elements

```
#!/bin/bash

for n in {1..10};
do
    echo $n
done
```

```
anakin@localhost:~$ bash ./script.sh
1
2
3
4
5
6
7
8
9
10
```

Loops

for repeats command(s) for every item on the list

Review



Shell script elements

Common script utilities

Environment variables



Scheduling Jobs, Working with Git, & Orchestration Tools

©2023 by StormWind LLC. All rights reserved.

<https://t.me/learningnets>

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Topics



Scheduling jobs



Intro to Git



Git commands



Branches



Infrastructure as Code

Scheduling Jobs

at

Schedule command at specified time

crontab file

Schedule commands on a regular basis

```
[root@CENTOS Deathstar]# cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR
sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name  command to be executed
```


What is Git?

Free version control

Manage projects

Tracks changes

Collaboration

Merges changes

Feature branches

Update specific sections of code



What is Git?

git config

--global user.name
--global user.email

git init

Instantiates Git in the directory

git commit

-m

Adds message to commit

-a

Commits all updated files in directory

```
[root@CENTOS ~]# git config --global user.name "Anakin"
[root@CENTOS ~]# git config --global user.email "Podracing@tatooine.com"
```

```
[root@CENTOS Deathstar]# git init
hint: Using 'master' as the name for the initial branch. This default branch name
hint: is subject to change. To configure the initial branch name to use in all
hint: of your new repositories, which will suppress this warning, call:
hint:     git config --global init.defaultBranch <name>
hint:
hint: Names commonly chosen instead of 'master' are 'main', 'trunk' and
hint: 'development'. The just-created branch can be renamed via this command:
hint:     git branch -m <name>
Initialized empty Git repository in /root/Deathstar/.git/
```

```
[root@CENTOS Deathstar]# git commit -m "First Commit" -a
[master (root-commit) 31f7b86] First Commit
1 file changed, 0 insertions(+), 0 deletions(-)
create mode 100644 Plans
```

Core Git Commands

git remote add

Add repository information to device

git clone

Copy repository from a server to device

git push

Push repository from harddrive into server that is hosting repository

git pull

Taking repository from server and moving to device

git commit

Staging = choose which files you want committed

Saves Changes in repository

-m message

git add

Adds changes to the staging area.

git checkout

Get prior last commit information

Even after changes and deletes

GitHub is hosting of repository

```
[root@CENTOS ~]# git remote add origin https://github.com/Anakin/DeathStar.git
```

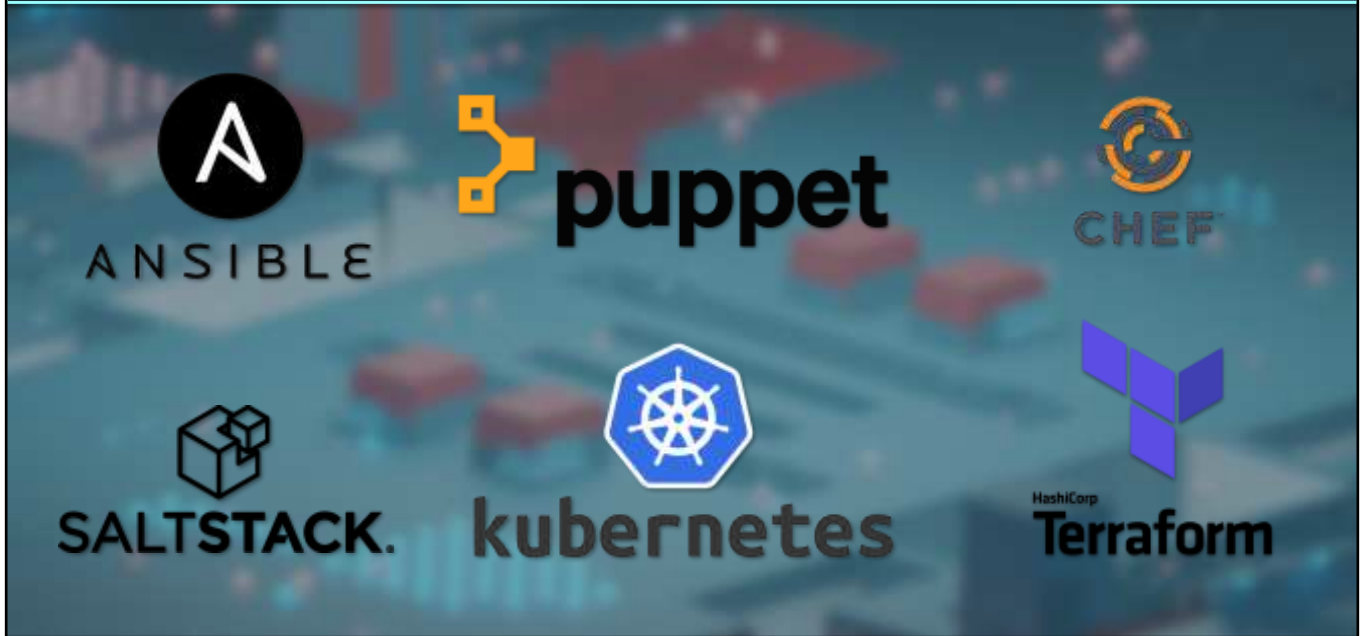


Branches

Work and save separate sections of code



Infrastructure as Code (IaC)



Ansible

Ansible uses YAML files called **playbooks** to define how servers should be configured

The Ansible application connects to servers via SSH and configures them as specified in playbooks

Example:

```
---
- name: Simple Ansible playbook
  hosts: myserver.com
  tasks:
    - name: Create file called '/tmp/file' with the text 'hi'
      copy:
        content: hi
        dest: /tmp/file
```

Terraform

Terraform uses human-readable text files to define how cloud infrastructure should be created

Providers allow Terraform to interact with specific cloud vendors (e.g., AWS)

Resources dictate what Terraform should create in the cloud environment

Example:

```
provider "aws" {  
  region = "us-west-2"  
}  
  
resource "aws_instance" "web" {  
  ami           = "ami-25187859"  
  instance_type = "t3.nano"  
}
```

Review



Scheduling jobs



Intro to Git



Git commands



Branches



Infrastructure as Code

