RH – 124 **System Administrator 1**

Chapter 1. Command Line

Chapter 2. Managing Files from the Command Line

Chapter 3. Getting Help

Chapter 4. Creating , Viewing and Editing Text Files

Chapter 5: Managing Local Linux Users and Groups

Chapter 6. ACCESS TO FILES WITH LINUX FILE SYSTEM PERMISSIONS

Chapter 7. Monitoring and Managing Linux Processes

Chapter 8. Controlling Services and Daemon

Chapter 9. Configuring and Securing OpenSSH service

Chapter 10. Analizing and Storing Logs

Chapter 11. Networking

Chapter 12. Archiving ann Copying Files Between Systems

Chapter 13. Installing and Updating Software Packages

Chapter 14. Accesing Linux File Systems

Chapter 15. Virtualized Systems

Instructor: fernando.ruiztapiador@edustance.com

Instructor: montse.alonso@edustance.com

Tenemos una maquina que se llama kiosk-am, que contiene 2 MV's: -desktop4 -server4

student/student

root/redhat

Desde la maquina fisica kios-am:

rht-vmctl status all -- Vemos el estado de las VMs

desktop\_am RUNNING server\_am RUNNING

rht-vmctl view server\_am -- Nos abre el servidor si lo tenemos abierto

rht-vmctl reset server\_am -- Reseteamos la MV

**classrrom**

**- Es la maquina que controla todos los PCs de la clase.**

**- Tiene una tarjeta de red propia que hace de GW hacia internet**

**- IP = 172.25.254.254**

**chapter 1. Accesing the command Line**

**cal**

January 2015

Su Mo Tu We Th Fr Sa

1 2 3

4 5 6 7 8 9 10

11 12 13 14 15 16 17

18 19 20 21 22 23 24

25 26 27 28 29 30 31

cal 4 1966 -- Mes 4 del año 1966

April 1966

Su Mo Tu We Th Fr Sa

1 2

3 4 5 6 7 8 9

10 11 12 13 14 15 16

17 18 19 20 21 22 23

24 25 26 27 28 29 30

cal 4 1966 -- Dia 30 Mes 4 del año 1966. Idem pero nos marca el dia

LANG=es\_ES.utf8 cal - - Calendario en formato español de españa

enero de 2015

lu ma mi ju vi sá do

1 2 3 4

5 6 7 8 9 10 11

12 13 14 15 16 17 18

19 20 21 22 23 24 25

26 27 28 29 30 31

LANG=es\_ES.utf8 -- Dejamos para la sesion actual.

locale - - Da info del local environment del sistema

locale --all |wc -l - - Total idiomas que soporta RH

789

CTRL + SHIFT + U + codigo = Vemos el cóodigo universal

localectl -- locale environment control

to query and change the system locale and keyboard layout settings.

localectl

System Locale: LANG=en\_US.UTF-8

VC Keymap: es

X11 Layout: es

-- Podemos cambiar globalmente a la maquina con:

localectl set-locale LANG=es\_ES.utf8

lscpu - - Vemos las caracteristicas de la CPU

Architecture: x86\_64

CPU op-mode(s): 32-bit, 64-bit

Byte Order: Little Endian

CPU(s): 1

On-line CPU(s) list: 0

Thread(s) per core: 1

Core(s) per socket: 1

Socket(s): 1

NUMA node(s): 1

Vendor ID: GenuineIntel

CPU family: 6

Model: 13

Model name: QEMU Virtual CPU version 1.5.3

Stepping: 3

CPU MHz: 3392.128

BogoMIPS: 6784.25

Hypervisor vendor: KVM

Virtualization type: full

L1d cache: 32K

L1i cache: 32K

L2 cache: 4096K

NUMA node0 CPU(s): 0

ESCRITORIOS

Hay un clone del gnome2.0 que es MATE (argentino)

Los dos grandes ESCRITORIOS son:

Gnome

KDE

Hay dos ESCRITORIOS mas ligeros son:

LXDE (ahora se llama LXQTERMINAL

Esta en favoritos o en Utilities

Lanza un interprete de comandos : Bash

-Mira si es un comando interno

-Mira en los ejecutables

time hay un comando interno y otro externo, no son iguales

externo: /usr/bin/time

whereis time

time: /usr/bin/time /usr/share/man/man1/time.1.gz /usr/share/man/man1p/time.1p.gz /usr/share/man/man2/time.2.gz /usr/share/man/man3p/time.3p.gz /usr/share/man/man7/time.7.gz

**time cal**

January 2015

Su Mo Tu We Th Fr Sa

1 2 3

4 5 6 7 8 9 10

11 12 13 14 15 16 17

18 19 20 21 22 23 24

25 26 27 28 29 30 31

real 0m0.001s

user 0m0.000s

sys 0m0.001s

usr/bin/time cal - - vemos que la salida es distinta!!

January 2015

Su Mo Tu We Th Fr Sa

1 2 3

4 5 6 7 8 9 10

11 12 13 14 15 16 17

18 19 20 21 22 23 24

25 26 27 28 29 30 31

0.00user 0.00system 0:00.00elapsed 92%CPU (0avgtext+0avgdata 1060maxresident)k

0inputs+0outputs (0major+320minor)pagefaults 0swaps

INTERPRETE DE COMANDOS: BASH

Por defecto se usa bash .. que es una evolucion de bsh

Fecha nacimiento de unix= 1 Enero 1970

Sistemas de 32 bits, fecha maxima= 1 Enero 2038 saltará a Enero 1920

sygwin: Utilidad Windows. Hace lo que mobaxterm

Es un interprete de comandos linux, emulado para Windows

mtools: Utilidad RedHat que traduce algunos comandos DOS a comandos Linux

mtools

Supported commands:

mattrib, mbadblocks, mcat, mcd, mclasserase, mcopy, mdel, mdeltree

mdir, mdoctorfat, mdu, mformat, minfo, mlabel, mmd, mmount

mpartition, mrd, mread, mmove, mren, mshowfat, mshortname, mtoolstest

mtype, mwrite, mzip

VIRTUAL CONSOLES

Por defecto hay 6 terminales: 1 gráfica y 5 de texto.

Ctrl + Alt + F1-F2-F3-F4-F5-F6

Ejemplo:

Ctrl + Alt + F6 Abrimos terminal texto 6

tty abrimos una terminal

1. Terminal FISICA= Es lo que podemos tocar fisicamente. TECLADO y MONITOR

2. TERMINAL LOGICA=

tty1 -- Terminal GRAFICO (default)

tty2, tty3, tty4, tty5 y tty6 -- Terminal de TEXTO

Ctrl + Alt + Fx - - Saltamos estando en el entorno GRAFICO

Alt + Fx - - Saltamos estando en el entorno TEXTO

Alt + -> - - Saltamos a la siguiente terminal TEXTO

Alt + <- - - Saltamos a la previaa terminal TEXTO

3. PSEUDO TERMINAL:

tty

/dev/pts/0 - - Pseudo Terminal, nos pueden logear.

Para cambiar de una terminal a otra:

chvt 5 - - Cambiamos a la terminal 5 (no funciona desde la pts)

- - Solo root puede ejecutar chvt

¿Como podemos ir a la terminal 12? : Pues de 3 formas distintas. Siempre como "root"

1) chvt 12

2) ALT + -->

3) ALT + F12

¿Como podemos ir a la terminal 13?

ALT-Grafico + F1 Pues si, existe la tty13

Funciones de Bash:

Ctrl + L - - Limpìa la pantalla sin limpiar la linea de comandos.

Shift + PgUp - - Hace scroll hacia arriba (el buffer es pequeño)

Shift + PgDown - - Hace scroll hacia abajo

SHELL basic

$ comando options arguments

Ej:

ls -a

. .bash\_history .bash\_profile .cache Desktop Downloads .ICEauthority Music Public Templates

.. .bash\_logout .bashrc .config Documents .esd\_auth .local Pictures .ssh Videos

ls --all (hace lo mismo que el anterior)

. .bash\_history .bash\_profile .cache Desktop Downloads .ICEauthority Music Public Templates

.. .bash\_logout .bashrc .config Documents .esd\_auth .local Pictures .ssh Videos

ls -all (ojo, aqui no entiende "all", entiende "all long long")

Equivale a : ls -a -l -l

total 36

drwx------. 14 student student 4096 Jan 27 10:17 .

drwxr-xr-x. 3 root root 20 Dec 9 23:22 ..

-rw-------. 1 student student 91 Jan 26 13:34 .bash\_history

-rw-r--r--. 1 student student 18 Jan 29 2014 .bash\_logout

-rw-r--r--. 1 student student 193 Jan 29 2014 .bash\_profile

-rw-r--r--. 1 student student 231 Jan 29 2014 .bashrc

drwx------. 10 student student 4096 Jan 26 12:52 .cache

drwxr-xr-x. 15 student student 4096 Jan 26 12:52 .config

drwxr-xr-x. 2 student student 6 Jan 26 12:37 Desktop

drwxr-xr-x. 2 student student 6 Jan 26 12:37 Documents

drwxr-xr-x. 2 student student 6 Jan 26 12:37 Downloads

-rw-------. 1 student student 16 Jan 26 12:37 .esd\_auth

-rw-------. 1 student student 620 Jan 27 10:17 .ICEauthority

drwx------. 3 student student 18 Jan 26 12:37 .local

drwxr-xr-x. 2 student student 6 Jan 26 12:37 Music

drwxr-xr-x. 2 student student 6 Jan 26 12:37 Pictures

drwxr-xr-x. 2 student student 6 Jan 26 12:37 Public

drwx------. 2 student student 28 Dec 9 23:22 .ssh

drwxr-xr-x. 2 student student 6 Jan 26 12:37 Templates

drwxr-xr-x. 2 student student 6 Jan 26 12:37 Videos

**cal --help --help : nos da un RESUMEN de las opciones mas TIPICAS**

Usage:

cal [options] [[[day] month] year]

Options:

-1, --one show only current month (default)

-3, --three show previous, current and next month

-s, --sunday Sunday as first day of week

-m, --monday Monday as first day of week

-j, --julian output Julian dates

-y, --year show whole current year

-V, --version display version information and exit

-h, --help display this help text and exit

Cuando ponga [date] ... Los 3 puintos es que adminten mas de 1 opcion

**Accesing the Command Line Usign Desktop**

Por defecto nos arranca GNOME

Alt + TAB -- Cambiamos de tarea

Si ponemos el raton en la "esquina superior izda" - - salen las tareas y al derecha los 4 Workspaces por defecto:

Executing Commands Using the Bash Shell

date +%R - - Ver solo la HORA

12:13

**date +%x - - Ver solo la FECHA**

01/27/2015

Hay 2 grandes familias de UNIX:

- System V (linux Red Hat)

- BSD (la version de linux es FreeBSD, que es la que usa Apple)

locate \*.jpg - - Buscar ficheros

/usr/lib64/pygtk/2.0/demos/images/background.jpg

/usr/share/backgrounds/corporate\_engraved\_1800x1440.jpg

/usr/share/backgrounds/corporate\_engraved\_2048x1536.jpg

file --Escanea el principio del fichero y nos dice que tipo es

file -z fichero.gz --Intenta ver lo que hay dentro del fichero comprimido

fichero.avi --Nos da la resolucion y el codec

head

head -n 1 /etc/passwd --muestra la 1 primera linea

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

tail

tail -n 1 /etc/passwd --muestra la 1 ultima linea

tail -f /var/log/messages -- Logs del sistema

systemctl status bluetooth.service -- Servicio bluetoth: nos dice el status

bluetooth.service - Bluetooth service

Loaded: loaded (/usr/lib/systemd/system/bluetooth.service; enabled)

Active: active (running) since Tue 2015-01-27 10:17:18 CET; 2h 19min ago

Main PID: 2474 (bluetoothd)

CGroup: /system.slice/bluetooth.service

└─2474 /usr/sbin/bluetoothd -n

Jan 27 10:17:18 server4.example.com systemd[1]: Starting Bluetooth service...

Jan 27 10:17:18 server4.example.com bluetoothd[2474]: bluetoothd[2474]: Bluetooth daemon 4.101

Jan 27 10:17:18 server4.example.com bluetoothd[2474]: Bluetooth daemon 4.101

Jan 27 10:17:18 server4.example.com systemd[1]: Started Bluetooth service.

Jan 27 10:17:18 server4.example.com bluetoothd[2474]: bluetoothd[2474]: Starting SDP server

Jan 27 10:17:18 server4.example.com bluetoothd[2474]: Starting SDP server

Jan 27 10:17:18 server4.example.com bluetoothd[2474]: bluetoothd[2474]: Parsing /etc/bluetooth/input.conf faile...tory

Jan 27 10:17:18 server4.example.com bluetoothd[2474]: Parsing /etc/bluetooth/input.conf failed: No such file or...tory

Jan 27 10:17:18 server4.example.com bluetoothd[2474]: bluetoothd[2474]: Bluetooth Management interface initialized

Jan 27 10:17:18 server4.example.com bluetoothd[2474]: Bluetooth Management interface initialized

Hint: Some lines were ellipsized, use -l to show in full.

wc

-c, --bytes print the byte counts

-m, --chars print the character counts

-l, --lines print the newline counts

--files0-from=F read input from the files specified by

NUL-terminated names in file F;

If F is - then read names from standard input

-L, --max-line-length print the length of the longest line

-w, --words print the word counts

TABULADOR

"El Tabulador es nuestro amigo".

Tabula tanto comandos como ficheros del directorio actual (si hay un espacio en blanco)

system +TAB

ls +TAB -- Nos dice los ficheros del directorio actual

ls File +TAB -- Nos dice los ficheros que empiezan por File

useradd -- +TAB -- Me da las opciones del comando useradd

nmcli +TAB - - Nos dice las opciones del comando "nmcli"

connection device general help networking radio

nmcli es nuevo en RH7 !!

-Ahora en RH7, es obligatorio el uso del Network Manager Client

-dockers: Es el equivalente a las zonas de Solaris. Es paravirtualizacion.

Ej. Se aprovecha el kernel de la maquina anfitrion para las MVs

history

! 10 -- Ejecuta el comando 10 del historico

history -d 112 --Borra la linea del historico 112

! he --Ejecuta el ultimo comando que empezaba por "he"

head -n 1 /etc/passwd

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

HISTCONTROL=ignoreboth -- Haciendo esto, los comandos que empieze por BLANCOS

-- no los memoriza en el historico de comandos

set |grep HIST -- Variables del HISTORY

HISTCONTROL=ignoreboth

HISTFILE=/root/.bash\_history

HISTFILESIZE=1000

HISTSIZE=1000

alt + . -- Autocompleta con el ultimo parametro de cada linea de comando

history 10

47 HISTCONTROL=ignoreboth

48 history

49 head -n 1 /etc/passwd

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

51 set |greo \_HIST

52 set |grep \_HIST

53 set |grep HIST

54 history 10

ls /etc/passwd pulsando ALT + . (punto)

ESC + AltGraph + # -- Es util cuando:

-- Empezamos a teclear un comando un muy largo y no queremos perderlo

-- Lo que hace es que nos pone una almohadilla (#) al principio de linea

LAB: Accessing the Command Line

1 passwd

2 date

3 date +%r

4 file /usr/bin/clean-binary-files

5 wc /usr/bin/clean-binary-files

6 ll /usr/bin/clean-binary-files

7 head /usr/bin/clean-binary-files

8 tail /usr/bin/clean-binary-files

9 tail -n 20 /usr/bin/clean-binary-files

10 date

11 history

**chapter 2. Managing Files from the Command Line**

The file system hierarchy - FSH 29-1-15

Estandares:

POSIX= Portable Operating System uniX (norma IEEE)

LSB = Linux Standard Base (basado en POSIX)

-El primer Linux fue en el 1991 (Linux Torwald)

- Todo cuelga del directorio /. Tipos de ficheros:

Estaticos

Dinamicos: Los files cambian porque el nucleo los cam

Compartidos

DIRECTORIOS:

/ Aqui solo hay directorios

**/boot Es lo que lee primero el sistema cuando se arranca**

Están los ficheros necesarios para el boot process

Aqui está el kernel y el GRUB

Muy recomendado que sea una particion separada

No permite estar en LVM ni raid

**/home Contenido de todos los users del sistema. Podemos cifrarlo pero se pierde un 30%**

/root home de root

/bin Aqui estan los comandos de TODOS los usuarios

**/sbin Aqui estan los comandos SOLO de root**

/dev Aqui estan los devices. Terminales, raton, CDROM, discos

Incluidos devices virtuales: /dev/null /dev/random

**/etc Ficheros de configuracion hasta RHEL6**

Solo contiene ficheros de TEXTO. Lo bueno es que podemos hacer find's, grep

**/lib Contiene las librarys (bibliotecas)**

**Programas binarios que son llamados desde otros binarios Ej: libreria PAM**

**/lib64 Solo para RHEL7. RHEL7: solo trabaja en 64bits**

recordar: 32bits: solo gesiona 4GB de RAM

Es la que usa por defecto RHEL7 Iphone: desde 1-feb-15 , todos tienen que migrar a 64bts

**/media medios remobibles. CDROM, USB hasta RHEL6**

/run Dynamic no-persistente aplication runtime

**/run/media Desde RHEL7, se automontan aqui**

/mnt Para montar un resource (samba, usb, dir, etc..) de forma manual

/opt Contiene paquetes opcionales. Paquetes de TERCEROS. Ej: Oracle

**/proc Direcotorio virtual, Esta todo en RAM**

Este directorio lo gestiona directamente el KERNEL

Casi todos tienen tamaño 0

Se van refrescando dinamicamente

**/srv Aqui debemos poner TODOS LOS SERVERS que EXPORTAMOS hacia fuera**

Ej: Apache, Samba, NFS

En el futuro habra que cambiar de /var/www/ .... hacia /srv

**/sys Tambien son ficheros virtuales en RAM**

Lo mismo que /proc pero mas documentados, mas ordenados

/tmp Archivos temporales

**Hay un cron que se ejecuta a diario, que si encuentra ficheros de >10 dias los borra**

**/var/tmp ficheros de >30 dias los borra**

/usr jerarquia secundaria de los datos de usuario

Contiene programas y librerias instalados

**Usuarios:**

/bin Aqui mira 3º

/usr/bin Aqui mira 2º

/usr/local/bin Aqui mira 1º

**En RHEL 7 solo hay 2 directorios:**

**/bin --> /usr/bin es un link Aqui mira 2º**

**/usr/local/bin Aqui mira 1º**

**root:**

**/sbin --> /usr/sbin es un link Aqui mira 2º**

**/usr/local/sbin Aqui mira 1º**

/var Archivos variables con el tiempo

**Locating Files by Name**

-Absolute paths and relative paths

-El path completo no puede contener mas de 4095 chars

-Un fichero no puede tener más de 255 chars

**touch**  **Sirve para actualizar la fecha-hora actual de un fichero que YA existe**

Si no existe ==> Lo crea **Cambia los meta-datos**

ll -R listado Recursivo viendo lo que hay dentro de cada directorio

El comando tree, nos muestra mejor esta info

Managing Files Using Command-Line Tools

cp copiar

cp -r dir1 dir2 dir3 dir4 **: Copia dir1** dir2 dir3 dentro de dir4

-r = recursivo

mv Mover a otro directorio o renombrar

mkdir Crear **mkdir -p dir1/dir2/dir3 : Crea varios directorios a la vez**

rmdir Solo borra directorios vacios

rm -rf dir Borra un directorio y su contenido SIN PREGUNTAR... OJO!!

-f = force

***Idea:***

**LANG=es\_ES.UTF8** rmdir dir

rmdir: fallo al borrar «dir»: El directorio no está vacío **- - > Nos habla en castellano !!**

***Matching File Names using Path Name Expansion***

**Comodines (globbing)::**

**~ Pulsando AltGr + 4**

**AltGr + Ñ**

**touch file{1..9} Creamos 9 ficheros . No hace falta un for**

**[ ] SOLO 1 CHAR**

ll file[12] Entre corchetes solo 1 char

-rw-rw-r--. 1 student student 0 Jan 28 11:10 file1

-rw-rw-r--. 1 student student 0 Jan 28 11:10 file2`

ll file[12][12]

-rw-rw-r--. 1 student student 0 Jan 28 11:11 file11

-rw-rw-r--. 1 student student 0 Jan 28 11:11 file12

**^ NEGACION**

ll file[^2]

-rw-rw-r--. 1 student student 0 Jan 28 11:10 file1

-rw-rw-r--. 1 student student 0 Jan 28 11:10 file3

-rw-rw-r--. 1 student student 0 Jan 28 11:10 file4

-rw-rw-r--. 1 student student 0 Jan 28 11:10 file5

**[[:digit:]] Solo numeros 0-9**

**[[:alpha:]] Solo Caracteres alfabeticos**

[[:alnum:]] Solo Alfanumericos

[[:lower:]] chars lowers

[[:upper:]] chars UPPERS

[[:punct:]] Any char imprimible que no sea space o alfanumerico

[[:space:]] Espacios en blanco o tabuladores

**{ } Permite RANGOS : Permite varios CHARS**

touch file{1..100} Crear 100 ficheros

**Command substitution**

echo `date +%A`

Wednesday

***Consejo: Poner las variables entre llaves { }***

echo "Hola $USER, son las $(date +%R)"

Hola student, son las 12:12

mejor:

echo "Hola ${USER}, son las $(date +%R)"

Las comillas simples ( ' ) no expanden los metachars:

echo 'Hola ${USER}, son las $(date +%R)'

Hola ${USER}, son las $(date +%R)

Podemos crear variables en una shell:

station=$(hostname)

echo $station

server4.example.com

\ (barra invertida) -- No expande el metachar que va a continuacion

echo "Hola \${USER}, son las $(date +%R)"

Hola ${USER}, son las 12:17

echo "Hola que tal estais, esta linea es muy larga\ -- Elimina el metachar ENTER

> y creo una segunda linea pero realmente no lo es porque quita el ENTER"

Hola que tal estais, esta linea es muy largay creo una segunda linea pero realmente no lo es porque quita el ENTER

Chapter 3. Getting Helping in REH HAT Enterprise Linux

man

section 1 comandos de usuario puede ejecutar (cualquier user)

/bin

/usr/bin

/usr/local/bin

section 8 comandos que solo root puede ejecutar

/sbin

/usr/sbin

/usr/local/sbin

section 5 Ficheros de configuracion

/etc

man 5 fstab

FSTAB(5)

RTFM = Read The Fuck Manual: Nos los podemos ver en google jejeje

bro = solo ejemplos, brother!

section 7 Convenciones, standars, miscellanuis

man 7 ascii

ASCII(7) Linux Programmer's Manual ASCII(7)

NAME

ascii - ASCII character set encoded in octal, decimal, and hexadecimal

DESCRIPTION

ASCII is the American Standard Code for Information Interchange. It is a 7-bit code. Many 8-bit codes (such as ISO 8859-1, the Linux default

character set) contain ASCII as their lower half. The international counterpart of ASCII is known as ISO 646.

The following table contains the 128 ASCII characters.

C program '\X' escapes are noted.

Oct Dec Hex Char Oct Dec Hex Char

────────────────────────────────────────────────────────────────────────

000 0 00 NUL '\0' 100 64 40 @

001 1 01 SOH (start of heading) 101 65 41 A

002 2 02 STX (start of text) 102 66 42 B

003 3 03 ETX (end of text) 103 67 43 C

004 4 04 EOT (end of transmission) 104 68 44 D

005 5 05 ENQ (enquiry) 105 69 45 E

006 6 06 ACK (acknowledge) 106 70 46 F

007 7 07 BEL '\a' (bell) 107 71 47 G

man -f ls - - Da una descripcion corta del comando

ls (1) - list directory contents

ls (1p) - list directory contents

man -f fdisk

fdisk (8) - manipulate disk partition table

man -f apropos

apropos (1) - search the manual page names and descriptions

apropos -- Busca cadenas

whatis -- Busca palabras completas

man -k nombre -- Equivale al apropos

whatis bluetooth -- Nos dice los comando donde aparece el texto bluetooth

bluetooth-sendto (1) - GTK application for transferring files over Bluetooth

bluetooth-wizard (1) - GTK wizard for setting up devices with the Linux Bluetooth stack

bluetoothd (8) - Bluetooth daemon

ciptool (1) - Bluetooth Common ISDN Access Profile (CIP)

hciconfig (8) - configure Bluetooth devices

hcitool (1) - configure Bluetooth connections

whatis ls

ls (1) - list directory contents

ls (1p) - list directory contents

passwd -l username -- lock user

passwd -u username -- unlock user

man Es como navegar por un fichero

info Es como navegar por un por una web

pinfo Es como navegar por un por una web, mas visual en colores

p=previo <--

n=next -->

q=salir

locate -- Localizar fichero en la jerarquia de directorios que contengan una cadena segun una BBDD

-- Hace lo mismo que el find pero utiliza una BBDD

-- Tiene que estar actualizada la BBDD

updatebd -- Actualiza la BBDD que usa el locate

cat /etc/updatedb.conf -- Aqui ponemos lo que no queremos que CONSIDERE el locate

PRUNE\_BIND\_MOUNTS = "yes"

PRUNEFS = "9p afs anon\_inodefs auto autofs bdev binfmt\_misc cgroup cifs coda configfs cpuset debugfs devpts ecryptfs exofs fuse fuse.sshfs fusectl gfs gfs2 hugetlbfs inotifyfs iso9660 jffs2 lustre mqueue ncpfs nfs nfs4 nfsd pipefs proc ramfs rootfs rpc\_pipefs securityfs selinuxfs sfs sockfs sysfs tmpfs ubifs udf usbfs"

PRUNENAMES = ".git .hg .svn"

PRUNEPATHS = "/afs /media /mnt /net /sfs /tmp /udev /var/cache/ccache /var/lib/yum/yumdb /var/spool/cups /var/spool/squid /var/tmp"

ll /etc/updatedb.conf

-rw-r--r--. 1 root root 508 Jan 26 2014 /etc/updatedb.conf

find

find -- Busca ficheros en tiempo real

DOCUMENTACION QUE HAY EN RHEL7

du -sh /usr/share/doc/

85M /usr/share/doc/

¿Que docus hay del ZIP?

rpm -ql zip q=query

/usr/bin/zip

/usr/bin/zipcloak

/usr/bin/zipnote

/usr/bin/zipsplit

/usr/share/doc/zip-3.0

/usr/share/doc/zip-3.0/CHANGES

/usr/share/doc/zip-3.0/LICENSE

/usr/share/doc/zip-3.0/README

/usr/share/doc/zip-3.0/README.CR

/usr/share/doc/zip-3.0/TODO

/usr/share/doc/zip-3.0/WHATSNEW

/usr/share/doc/zip-3.0/WHERE

/usr/share/doc/zip-3.0/algorith.txt

/usr/share/man/man1/zip.1.gz

/usr/share/man/man1/zipcloak.1.gz

/usr/share/man/man1/zipnote.1.gz

/usr/share/man/man1/zipsplit.1.gz

ll /usr/share/doc/ |wc -l

893 - - Hay 893 directorios en la docuemtnacion

rpm -qa | wc -l a=all

1208 -- Hay 1208 paquetes total instalados

-El KERNEL tiene un gran paquete de documentacion llamado: kernel.doc

Getting Help From Red Hat

https://access.redhat.com/

Los mas usados:

Suscription

Downloads

Support Casses

Hay 2 tipos de cuentas:

Profesional Si podemos bajarnos ISO

Personal No nos podemos bajar ISO

Permite acceder a la docu , a las tools (gran parte)

Migration Planning Guide -- Ideal para migrar de RHEL 6 a RHEL 7.... o RHEL5 a RHEL6

Performance Tunning Guide -- Interesante para mejorar la eficiencia del sistema

SECURITY

- SELinux User's Admin Guide

Nueva herramienta en RHEL7:

redhat-support-tool

Welcome to the Red Hat Support Tool.

Command (? for help):

redhat-support-tool kb 781733 -- Miro el articulo 781733 kb=knolowge case

Please enter your RHN user ID: andres66

Save the user ID in /home/student/.redhat-support-tool/redhat-support-tool.conf (y/n): y

Please enter the password for andres66:

Save the password for andres66 in /home/student/.redhat-support-tool/redhat-support-tool.conf (y/n): y

Title

===============================================================================

Determine how much memory is being used on the system

URL: None

sosreport - - Collect and package diagnostic and support data

- - Paquetes, Memoria, procesis

- Ejecutar como root

- Severidad 4: la mas baja, se responde en 2 dias laborales

- Suelen pedir un sosreport

- En RHEL se pueden meter Incidencias ilimitadas

- Genera un fichero comprimido

sosreport (version 3.0)

This command will collect diagnostic and configuration information from

this Red Hat Enterprise Linux system and installed applications.

An archive containing the collected information will be generated in

/var/tmp and may be provided to a Red Hat support representative.

Any information provided to Red Hat will be treated in accordance with

the published support policies at:

https://access.redhat.com/support/

The generated archive may contain data considered sensitive and its

content should be reviewed by the originating organization before being

passed to any third party.

No changes will be made to system configuration.

Press ENTER to continue, or CTRL-C to quit.

Chapter 4. Creating , Viewing and Editing Text Files

entrada standar 0 TECLADO

salida standar 1 PANTALLA

salida error 2 PANTALLA

echo hola > fichero 2>&1 Estandar y Errores --> al mismo fichero

echo hola 2>&1 > fichero Errores --> a la estandar (pantall)

CONCATENAR FICHEROS:

cat file1 file2 file3

diff Saca diferencia en ficheros de texto

vimdiff Idem pero las displaya con el editor vim

Constructing pipelines

- Permite que la stdout de un proceso ---> lo envia ---> a la stdin de otro proceso

- La salida de errores (stderr)

Comando tee

- Permite duplicar la salida estandard (stdin) a otro sitio mas

ls | tee fichero.txt -- a parte de pantalla va a otro fichero

- Tecnicas de lineas de comandos:

http://www.commandlinefu.com/commands/browse -Pag web util

- Podemos enviar correos por linea de comandos

ll | mail -s "asunto" andres.guijarro@gmail.com

- Podemos poner en casa en el arranque este comando:

curl ifconfig.me - - Nos dice la IP PUBLICA desde que salimos a internet desde casa

195.235.163.201

-- curl : es como un wget

-- Es la IP dinamica que nos ponen en el router para salir

curl ifconfig.me/all

ip\_addr: 195.235.163.201

remote\_host:

user\_agent: curl/7.29.0

port: 13968

lang:

connection: keep-alive

keep\_alive:

encoding:

mime: \*/\*

charset:

via: 1.1 localhost:3128 (squid/2.7.STABLE9)

forwarded: 10.2.4.254

- Nos manda un mail:

echo "La IP de salida de Getafe es la $(curl -s ifconfig.me)" | mail -s "IP de Getafe" andres.guijarro@gmail.com

Editing Text Files from the Shell Prompt

vi es un alias del vim (alias vi='vim')

vim

emacs

joe

nano

gedit

Cosas del vim:

ZZ --Salir guardando!!

ZQ --Salir sin guardar!!

Ctrol+Z --Duerme un proceso

dw -- Borra una word

de -- Hace lo mismo que dw (delete word) pero conserva los blancos

d$ -- Borra hasta el final de la linea

u -- para deshacer el último mandato

U -- para deshacer una línea entera.

CTRL-R -- Para deshacer lo deshecho

yy

4p pegame 4 veces lo que está en el portapapeles

Ctrl+Shift+R Rehacer

:set number -- Veo los numeros de lineas

:set list - - Veo los chars no-imprimibles

:77 -- Vete a la linea 77

grep -n Music file --Dime en que fila esta el literal "Music"

7:Music

vim +7 file -- Y ahora editame el fichero y vete a la linea 7

vimrc : Buscar en google para configurar el vim

http://amix.dk/vim/vimrc.html

http://vim-adventures.com/ -- juegos

Chapter 5: Managing Local Linux Users and Groups

30-1-14

-Cada proceso en ejecucion pertenece o se ejecuta con un USUARIO concreto

-El acceso a los ficheros y directorios estan restringidos por USUARIOS

-Cuando un proceso se ejecuta ==> SE HEREDAN LOS PERMISOS DEL USUARIO al que pertenece el fichero

USUARIOS

uid = identificador de usuario

id -- comando que Muestra quien soy yo

id | tr " " "\n" -- Traduce los " " por saltos de linea

uid=1000(student)

gid=1000(student)

groups=1000(student),10(wheel) context=unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023

--Contexto de SELINUX

id root | tr " " "\n"

uid=0(root)

gid=0(root)

groups=0(root)

cat /etc/passwd --Fchero de USUARIOS

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

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin

adm:x:3:4:adm:/var/adm:/sbin/nologin

lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

sync:x:5:0:sync:/sbin:/bin/sync

shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

halt:x:7:0:halt:/sbin:/sbin/halt

mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

operator:x:11:0:operator:/root:/sbin/nologin

games:x:12:100:games:/usr/games:/sbin/nologin

ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin

nobody:x:99:99:Nobody:/:/sbin/nologin

dbus:x:81:81:System message bus:/:/sbin/nologin

polkitd:x:999:998:User for polkitd:/:/sbin/nologin

avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin

avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin

rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin

rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin

id < 1000 --Usuarios ESPECIALES del sistema, que no tienen SHELL . No van a hacer LOGIN nunca

/etc/shadow --Fichero de PASSWD

GRUPOS

Fichero /etc/group

grep student /etc/group

wheel:x:10:student --En el grupo wheel esta el usuario "student"

student:x:1000: --En el grupo student

Grupo wheel: Es un grupo especial, tiene privilegios de root

- Siempre siempre debe haber un grupo PRIMARIO

- Grupo SECUNDARIO, puede haber por usuario o no

- El Administrador de SELINUX puede controlar QUE PUEDE y que NO PUEDE HACER root

- El Administrador de SELINUX está por encima de ROOT.

- SELINUX tiene ya 10 años

Gaining Superuser Access

- Se recomienda NO ENTRAR NUNCA como root.

- Siempre entrar como usuario normal (student) y subir a root.

Switching users whith su

su [ - ] <username>

1) SI estando como student hago su root: Utiliza las mismas variables de entorno que el usuario del que vengo:

[student@server4 ~]$ echo $PATH

/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/home/student/.local/bin:/home/student/bin

[student@server4 ~]$ su root

Password:

[root@server4 student]# echo $PATH

/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/home/student/.local/bin:/home/student/bin

[root@server4 student]#

2) SI estando como student hago su - root: ejecuta el profile del usurio root:

[root@server4 student]# echo $PATH

/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/home/student/.local/bin:/home/student/bin

[student@server4 ~]$ su - root

Password:

Last login: Fri Jan 30 10:12:07 CET 2015 on pts/1

[root@server4 ~]# echo $PATH

/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin

su - - c ls -c = ejecuta lo que venga a continuacion (como root): ls

Password:

anaconda-ks.cfg Desktop Documents Downloads Music Pictures Public Templates Videos

Comando sudo

-Vale para heredar la propiedades de root

[student@server4 ~]$ fdisk -l /dev/vda

fdisk: cannot open /dev/vda: Permission denied -- No puedo ejecutar fdisk como student !!

[student@server4 ~]$ sudo !! !! = es el ultimo comando (ahora le pongo sudo delante)

sudo fdisk -l /dev/vda

[sudo] password for student: -- Le pide la passwd de "student"

Disk /dev/vda: 10.7 GB, 10737418240 bytes, 20971520 sectors

Units = sectors of 1 \* 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk label type: dos

Disk identifier: 0x00013f3e

Device Boot Start End Blocks Id System

/dev/vda1 \* 2048 20970332 10484142+ 83 Linux

Fichero /etc/sudoers -- Fichero de configuracion del SUDO

## Sudoers allows particular users to run various commands as

## the root user, without needing the root password.

- Nunca edidarlo DIRECTRAMENTE

visudo --Editor especifico del SUDOERS

-- Al salir grabando chequea la sintaxis

-- Siempre como root

## Allow root to run any commands anywhere

root ALL=(ALL) ALL

usuario-sudo maquina's=(ejecuta como el usuario xxxx) Que comandos

student ALL=(ALL) NOPASSWD: /sbin/fdisk -l /dev/vda -- ahora ya no pedirá passwd a student cuando

-- ejecute el comando

Managing Local User Accounts

user + TAB --Salen los comandos para trabajar con usuarios.

useradd -- Añadir usuarios

usermod -- Modificar usuarios

userdel -- Borrar usuarios

userformat

userhelper

userinfo

usermount

usernetctl

userpasswd

users

newusers - update and create new users in batch --Crea usuarios masivamente segun fichero de texto

cat /etc/login.defs | grep -v ^# -- Parametros default al crear 1 passd de usuario

MAIL\_DIR /var/spool/mail

PASS\_MAX\_DAYS 99999

PASS\_MIN\_DAYS 0

PASS\_MIN\_LEN 5

PASS\_WARN\_AGE 7

UID\_MIN 1000

UID\_MAX 60000

SYS\_UID\_MIN 201

SYS\_UID\_MAX 999

GID\_MIN 1000

GID\_MAX 60000

SYS\_GID\_MIN 201

SYS\_GID\_MAX 999

CREATE\_HOME yes

UMASK 077

USERGROUPS\_ENAB yes

ENCRYPT\_METHOD SHA512

cat /etc/default/useradd | grep -v ^# -- Default para ALTAS de usuarios

GROUP=100

HOME=/home

INACTIVE=-1

EXPIRE=

SHELL=/bin/bash

SKEL=/etc/skel

CREATE\_MAIL\_SPOOL=yes

ll -a /etc/skel/ --Estos ficheros OCULTOS se copian al $HOME

-- cuando creamos un USUARIO nuevo

total 24

drwxr-xr-x. 4 root root 88 Dec 9 23:38 .

drwxr-xr-x. 133 root root 8192 Jan 30 10:44 ..

-rw-r--r--. 1 root root 18 Jan 29 2014 .bash\_logout

-rw-r--r--. 1 root root 193 Jan 29 2014 .bash\_profile

-rw-r--r--. 1 root root 231 Jan 29 2014 .bashrc

drwxr-xr-x. 2 root root 56 Dec 9 23:38 .config

drwxr-xr-x. 4 root root 37 Dec 9 23:26 .mozilla

vipw --Para editar el fichero /etc/passwd.

vigr --Para editor el fichero /etc/group

-Estos 2 comandos hace copia de seguriidad de ambos ficheros cuando tocamos

etc/passwd-

/etc/group-

Borrar un usuario:

userdel -R usuario -R = Borra el $HOME del usuario

find / -nouser -- Encontrar ficheros que no tengan el UID en /etc/passwd

find: ‘/proc/3862/task/3862/fd/6’: No such file or directory

find: ‘/proc/3862/task/3862/fdinfo/6’: No such file or directory

find: ‘/proc/3862/fd/6’: No such file or directory

find: ‘/proc/3862/fdinfo/6’: No such file or directory

-Si quiero borrar esos ficheros que no tengan usuarios:

find / -nouser -exec rm -rf {} \; -- El \ significa: el ";" no es de la bash .. es del find !!!

Managing Local Group Accounts

groupadd groupname -- Añade grupos desde /etc/login.defs

groupadd -g GID -- Añado Grupo directamente poniendo el GID

groupadd -g 3000 shakespeare --Creo el grupo suplementario "shakespeare" y le pongo GID=3000

usermod -aG wheel elvis -- Añade el user "elvis" al grupo wheel

- Se recomienda que se use un rango distintos para los gurpos

- Por ejemplo > 5000

- Si borramos un grupo y tiene usuarios: Se quedar el GID primario como numero.

Managing User Passwords

- Por defecto la passwd de 1 usuario nunca caduca

- Se movieron del /etc/passwd al /etc/shadow

¿Como funciona el sistema de passwd?

-Cuando el sistema se loguea: El systema regenera el passwd del usuario y ver si coincide con lo que hay en /etc/passwd

tail /etc/shadow --Los campos van separados por ":"

Campos del /etc/shadow:

1 Usuario

2 algoritmo

3 lastchange - Fecha desde 1-1-1970 epoch

4 Nª dias inciales en los que no puede cambiar la passs -m (min)

5 Nº dias que dura la passwd -M (max) chage

6 Nª dias de aviso de que tiene que cambiar la passwd -W (warning)

7 Nº dias de gracia para cambiar la passwd -I (Inactive)

8 Fecha directa en la que expira la passwd -E (Expire)

9 Se deja en blanco para uso futuro

chage -d username -- Fuerzo a que un usuario cambie su passwd cuando entre a su cuenta

-Cuando se bloquea un user, en el campo 8==> se deja un 0

tail -1 /etc/shadow | tr ":" "\n"

elvis

6

DCO603zy

vJZfbs4hxvBIYu1UOwOte1rcYtVoSSUDfl3FehBZXYG5HRPK.tEWvbqmGy/XBPLgIbXn4ZmlKrS/m8Ltk8W4q0

16465

0

99999

7

6 = Algoritmo SHA-512

DCO603zy = salt: Nº aleatorio

JZfbs4hxvBIYu1UOwOte1rcYtVoSSUDfl3FehBZXYG5HRPK.tEWvbqmGy/XBPLgIbXn4ZmlKrS/m8Ltk8W4q0:16465:0:99999:7:::

= Passwd cifrada = passwd con SHA-512 + salt

Si existe el fichero /etc/nologin ==> Cuando se crea ese fichero:: ningun usuario puede entrar al sistema

==> Cuando se hace reboot: se borra este fichero

/sbin/nologin -- Esta es una shell especiail para usuarios que no queremos que metan comandos

-- Ejemplo: apache, bin, daemon, ftp...

http://xkcd.com/ --> Web de humor

Heramienta grafica de gestion de Usuarios

No esta instalada por defecto

yum install system-config-users

Chapter 6.ACCESS TO FILES WITH LINUX FILE SYSTEM PERMISSIONS

2-2-15

Profesor: David

-Vamos a establecer los permisos sobre ficheros

-Interpretar los efectos de seguridad segun los settings de los permisos

- Vamos a trabajar con el UID y GID

FILES

DIRECTORY

r (read)

-Ver contenido del fichero

-Ver ficheros dentro del directorio (listado corto)

w (write)

-Modificar contenido del fichero

NO: borrar el fichero

-Modificar el contenido del directorio

-NO modificar el contenido del directorio

x (exec)

- Ejecutar el fichero

-Movernos dentro del directorio (cd) (listado largo)

U G O

rwx rwx rwx .

rwx rwx rwx +

. = El fichero está en un contexto de SELINUX

+ = El fichero tiene ACLs

stat -- Nos da los metadatos de los ficheros

stat /tmp/student

File: ‘/tmp/student’

Size: 0 Blocks: 0 IO Block: 4096 regular empty file

Device: fd01h/64769d Inode: 17065068 Links: 1

Access: (0664/-rw-rw-r--) Uid: ( 1000/ student) Gid: ( 1000/ student)

Context: unconfined\_u:object\_r:user\_tmp\_t:s0

Access: 2015-02-02 10:00:39.992072382 +0100

Modify: 2015-02-02 10:00:39.992072382 +0100

Change: 2015-02-02 10:00:39.992072382 +0100

Birth: - -- Esto es nuevo en RHEL7

- Los permisos en GNOME estan muy limidados

- Los entornos gráficos consumen un 40% de los recursos

-RHEL7 tiene Gnome3

Comando chmod

- Cambiar los permisos de un fichero

- Los PERMISOS en Linux se llaman MODOS

METODO SYMBOLICO

chmod Who What Which file | directory

Who = u, g, o, a (user, group, others, all)

what = +, -, = (add, remove, asignar)

which = r, w, x (read, write, executable)

Ej:

chmod o+rwx es lo mismo que chmod o=

METODO NUMERICO

chmod ### file | directory

-Cada digito representa un nivel de acceso

-r=4 w=2 x=1

Comando chown

- Cambiar el PROPIETARIO (OWNER) de un fichero

- El user solo lo puede cambiar root y el dueño del fichero

- Cambiar el grupo de un fichero lo puede hacer cualquiera siempre y cuando, el usuario que lo posee

chown [OPTION]... [OWNER][:[GROUP]] FILE...

or:

chown [OPTION]... --reference=RFILE FILE...

chown -R student file - recursivo

chown -R student:grupo file - recursivo y cambio usuario: grupo

chown -R student.grupo file - recursivo y cambio usuario: grupo

chown -R :group file - recursivo SOLO el grupo

Comando chgrp

- Cambiar el GRUPO

chgrp

Managing Default Permissions and file Access

Permisos especiales:

- Cuando se ejecuta un proceso se ejecuta con unos permisos.

- Ese proceso tiene un user/group de ejecucion

bit especial

Files

Directorio

suid

u+s

proceso perteneza al propietario del fichero

No hay efecto

sgid

g+s

proceso pertenezca al grupo del fichero

ficheros dentro del directorio pertenecen con grupo del directorio

sticky

o+t

no tiene efecto

solo root y el proietario del fichero pueden borrar el fichero

Lo tipico es verlo en /tmp

suid: Sobre un fichero

Se establece con

u+s

u-s

Ej:

passwd -- Requiere acceso a un fichero especial /etc/shadow

Cuando student cambie su passwd, se estará ejecutando como si fuera "root"

guid

Cuando el usuario student' crea un fichero ==> pertenece al grupo del directorio

Se establece con

g+s

g-s

sticky

ll -d /tmp

drwxrwxrwt. 12 root root 4096 Feb 2 10:38 /tmp

Se establece con:

o+t

o-t

Numericamente se puede cambiar con chmod en el primer DIGITO

chmod 2770 directory

MASCARA DE PERMISOS

Permisos maximos que se pueden establecer en un fichero: 666 rw- rw- rw-

Permisos maximos que se pueden establecer en un directorio: 777 rwx rwx rwx

umask

Nos dice la mascara de permisos del usuario actual

¿Como se calcula la los permisos de un fichero?

Permisos maximos

- Mascara

-----------------------------------

default mask "user": 002

default mask "root": 022

Ejemplo:

touch file ¿que permisos tiene el fichero file?

666 permisos maximos

- 002 mascara

---------------

664 Permisos default al crear 1 fichero

-rw-rw-r--. 1 student student 0 Feb 2 11:01 file

touch dir ¿que permisos tiene el directorio dir?

777 permisos maximos

- 002 mascara

---------------

775 Permisos default al crear 1 directorio

drwxrwxr-x. 2 student student 6 Feb 2 11:01 dir

1. /etc/profile

- Se ejecuta cada ver que si inicia sesion de un usuario

2. /etc/bashrc (leido cuando ejecutamos una shell bash)

- Contiene solo FUNCIONES y ALIAS

- Se ejecuta cada vez que se abre un terminal

- Mascaras por defecto se establece en este fichero que solo puede modificar root:

- History

A nivel de usuario:

.bash\_profile -- Se abre cada ver que hacemos login

.bashc -- Se abre en cada consola virtual que abramos

-- Aqui puedo cambiar la mascara de un usuario

Chapter 7. Monitoring and Managing Linux Processes

Proceso: Es una instancia en ejecucion de un programa ejecutable lanzado

Consta de:

- Espacio de direcciones (memoria reservada)

- Seguridad: credenciales y privilegios

- Uno o mas hilos de ejecucion del codigo del programa

- Estado del proceso

- Se carga un entorno de trabajo del proceso que incluye:

variables local y global

current sheduling context

Recursos del sistema reservados (ej: file descriptors o puerto de red)

Estado de un proceso:

RUNNING R (el proceso está o ejecutando en 1 CPU o wating to run)

SLEEPING S S = Se puede interrumpir

D = No puede inturrumpirse

K = Permite ser KILLED

STOPPED T El proceso ha sido parado (suspendido)

T El proceso esta siendo depurado (Traced)

ZOMBIE Z Un proceso hijo manda una señal al padre de que existe

X Cuando el proceso padre se limpia, los procesos hijos son liberados

Procesos hijos. Finalizan de 2 formas:

- Normal

- Zombe No ocupa memoria ni disco.. pero aparece en la lista de procesos

Comando ps

UID Usuario con que se ha ejecutado el proces

PID Process Id

Uso de CPU

Uso de Memoria

Ubicacion del proceso

Estado del proceso

ps aux -- Nos muestra todos los procesos del sistema con todos los usuarios

USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND

root 1 0.0 0.3 52328 6496 ? Ss 09:56 0:01 /usr/lib/systemd/systemd --switched-root --system --deserialize 21

root 2 0.0 0.0 0 0 ? S 09:56 0:00 [kthreadd]

root 3 0.0 0.0 0 0 ? S 09:56 0:00 [ksoftirqd/0]

root 5 0.0 0.0 0 0 ? S< 09:56 0:00 [kworker/0:0H]

root 6 0.0 0.0 0 0 ? S 09:56 0:00 [kworker/u2:0]

root 7 0.0 0.0 0 0 ? S 09:56 0:00 [migration/0]

...

ps -feo comm,pid,%cpu -e=all,

COMMAND PID %CPU

bash 31350 0.0

\\_ ps 597 0.0

CONTROLLING JOBS

jobs: Suele ser un proceso pero no siempre

-Es 1 o mas procesos asginados por un entorno que podemos controlar

Ambitos de trabajo de un job:

-Foreground

Son los que lanza el usuario

Toma el control de una terminal y espera señales de esa terminal

-Background

se ejecutan en 2º plano.

Puedo seguir usando la terminal

Ejemplo:

[root@server4 ~]# firefox

(process:1061): GLib-CRITICAL \*\*: g\_slice\_set\_config: assertion `sys\_page\_size == 0' failed

CTROL + Z - - Ahora lo he puesto STOPPED y firefox no responde !!

[root@server4 ~]# firefox & -- Lo lanzo en background

-- He generado un JOB

jobs -- Muestra la lista de trabajos disponibles

Proceso top

Tambien existe htop 3-2-15

H: Hilos de ejecucion

User real el que ha lanzado manual

user efectivo es el UID con el que se está ejecutando

sort:

L Load (carga)

T: Hilos

M: Memoria

P: CPU

R: Renice

W: Write configuracion top

Filtros:

b: resalta los procesos en negrita

u: user

Help for Interactive Commands - procps-ng version 3.3.9

Window 1:Def: Cumulative mode Off. System: Delay 3.0 secs; Secure mode Off.

Z,B,E,e Global: 'Z' colors; 'B' bold; 'E'/'e' summary/task memory scale

l,t,m Toggle Summary: 'l' load avg; 't' task/cpu stats; 'm' memory info

0,1,2,3,I Toggle: '0' zeros; '1/2/3' cpus or numa node views; 'I' Irix mode

f,F,X Fields: 'f'/'F' add/remove/order/sort; 'X' increase fixed-width

L,&,<,> . Locate: 'L'/'&' find/again; Move sort column: '<'/'>' left/right

R,H,V,J . Toggle: 'R' Sort; 'H' Threads; 'V' Forest view; 'J' Num justify

c,i,S,j . Toggle: 'c' Cmd name/line; 'i' Idle; 'S' Time; 'j' Str justify

x,y . Toggle highlights: 'x' sort field; 'y' running tasks

z,b . Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y')

u,U,o,O . Filter by: 'u'/'U' effective/any user; 'o'/'O' other criteria

n,#,^O . Set: 'n'/'#' max tasks displayed; Show: Ctrl+'O' other filter(s)

C,... . Toggle scroll coordinates msg for: up,down,left,right,home,end

k,r Manipulate tasks: 'k' kill; 'r' renice

d or s Set update interval

W,Y Write configuration file 'W'; Inspect other output 'Y'

q Quit

( commands shown with '.' require a visible task display window )

Chapter 8. Controlling Services and Daemon

systemd : Es el nuevo Daemon que controla los servicios del sistema

- Ya no hay proceso INIT, ahora es systemd PID=1

- Tiene una carga de servicios divididos en UNIDADES:

Montaje

Servicios de Red

Sockets

. . .

- Entre las UNIDADES hay una dependencia interna de estos SERVICIOS.

- Mientras estos servicios arrancan, systemd arranca otros servicios paralelamente

- Las dependencias si van serializadas.

- Ya no existen runlevels, ahora son targets

- Con un disco SSD, RedHat puede arrancar en pocos segundos.

¿Como arrancamos/paramos servicios?

Systemd ofrece 2 herramientas :

1) systemctl

2) systemd

systemctl -t help -- Muestra los TIPOS de unidades

Available unit types:

service -- Lo veremos (\*)

socket -- Lo veremos

target -- Lo veremos

device

mount

automount

snapshot

timer

swap

path

slice

scope

Sintaxis:

systemctl [OPTIONS...] {COMMAND} ...

systemctl Operacion NombreServicio

systemctl (a pelo) -- Muestra TODAS las unidades

UNIT LOAD ACTIVE SUB DESCRIPTION

proc-sys-fs-binfmt\_misc.automount loaded active waiting Arbitrary Executable File Formats File System Automount Point

sys-devices-pci0000:00-0000:00:03.0-virtio0-net-eth0.device loaded active plugged Virtio network device

sys-devices-pci0000:00-0000:00:04.0-virtio1-block-vda-vda1.device loaded active plugged /sys/devices/pci0000:00/0000:00:04.0/virtio1/block/vda/vda1

sys-devices-pci0000:00-0000:00:04.0-virtio1-block-vda.device loaded active plugged /sys/devices/pci0000:00/0000:00:04.0/virtio1/block/vda

sys-devices-pci0000:00-0000:00:05.0-virtio2-block-vdb.device loaded active plugged

....

systemctl status sshd.service

sshd.service - OpenSSH server daemon

Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled) -----> Cuando se arranque la maquina: el service se arrancará

Active: active (running) since Tue 2015-02-03 09:21:49 CET; 56min ago

Process: 1143 ExecStartPre=/usr/sbin/sshd-keygen (code=exited, status=0/SUCCESS) --Prog previo

Main PID: 1149 (sshd)

CGroup: /system.slice/sshd.service

└─1149 /usr/sbin/sshd -D

Feb 03 09:21:49 localhost systemd[1]: Started OpenSSH server daemon. --Es un tail del log

Feb 03 09:21:50 localhost sshd[1149]: Server listening on 0.0.0.0 port 22.

Feb 03 09:21:50 localhost sshd[1149]: Server listening on :: port 22.

Feb 03 09:26:13 server4.example.com sshd[1539]: Accepted password for student from 172.25.4.250 port 42563 ssh2

Feb 03 09:33:09 server4.example.com sshd[1715]: Accepted password for student from 172.25.4.250 port 42570 ssh2

Feb 03 09:58:23 server4.example.com sshd[2117]: Accepted password for student from 172.25.4.250 port 42629 ssh2

Otros casos de servicio active:

active (exit)

active (wainting) -- El servicio esta activo, pero el demonio no está en ejecucion, esta a la espera (ej. el TFTP)

active (running)

systemctl stop sshd.service

Active: inactive (dead) since Tue 2015-02-03 10:24:01 CET; 4s ago

systemctl -t service -- Muestra UNIDADES tipo Service

systemctl -type service

systemctl status rngd.service -l -- Muestra en formato "long"

rngd.service - Hardware RNG Entropy Gatherer Daemon

Loaded: loaded (/usr/lib/systemd/system/rngd.service; enabled)

Active: failed (Result: exit-code) since Tue 2015-02-03 09:21:35 CET; 1h 6min ago

Process: 505 ExecStart=/sbin/rngd -f (code=exited, status=1/FAILURE)

Main PID: 505 (code=exited, status=1/FAILURE)

CGroup: /system.slice/rngd.service

Feb 03 09:21:34 localhost systemd[1]: Started Hardware RNG Entropy Gatherer Daemon.

Feb 03 09:21:35 localhost rngd[505]: Unable to open file: /dev/tpm0

Feb 03 09:21:35 localhost rngd[505]: can't open any entropy source

Feb 03 09:21:35 localhost rngd[505]: Maybe RNG device modules are not loaded

Feb 03 09:21:35 localhost systemd[1]: rngd.service: main process exited, code=exited, status=1/FAILURE

Feb 03 09:21:35 localhost systemd[1]: Unit rngd.service entered failed state.

systemctl is-active sshd -- ¿Está activo el SSH?

inactive

systemctl is-enabled sshd -- ¿Arrancará cuando se inicie la maquina?

enabled

systemctl list-units -t service -all -- Unidades de tipo SERVICIO

systemctl list-unit-files -t service -- Dime unidades tipo servicio en formato mas legible

UNIT FILE STATE

abrt-ccpp.service enabled

abrt-oops.service enabled

abrt-pstoreoops.service disabled

abrt-vmcore.service enabled

abrt-xorg.service enabled

abrtd.service enabled

accounts-daemon.service enabled

alsa-restore.service static

alsa-state.service static

alsa-store.service static

anaconda-direct.service static

systemctl --failed -t service -- Dime los servicios que han fallado

UNIT LOAD ACTIVE SUB DESCRIPTION

ovirt-guest-agent.service loaded failed failed oVirt Guest Agent

rc-local.service loaded failed failed /etc/rc.d/rc.local Compatibility

rhnsd.service loaded failed failed LSB: Starts the Spacewalk Daemon

rngd.service loaded failed failed Hardware RNG Entropy Gatherer Daemon

LOAD = Reflects whether the unit definition was properly loaded.

ACTIVE = The high-level unit activation state, i.e. generalization of SUB.

SUB = The low-level unit activation state, values depend on unit type.

4 loaded units listed. Pass --all to see loaded but inactive units, too.

To show all installed unit files use 'systemctl list-unit-files'.

Practica:

systemctl list-units -t socket -all -- lista unidades tipo SOCKET

UNIT LOAD ACTIVE SUB DESCRIPTION

avahi-daemon.socket loaded active running Avahi mDNS/DNS-SD Stack Activation Socket

cups.socket loaded active listening CUPS Printing Service Sockets

dbus.socket loaded active running D-Bus System Message Bus Socket

dm-event.socket loaded active listening Device-mapper event daemon FIFOs

iscsid.socket loaded active listening Open-iSCSI iscsid Socket

iscsiuio.socket loaded active listening Open-iSCSI iscsiuio Socket

lvm2-lvmetad.socket loaded active running LVM2 metadata daemon socket

rpcbind.socket loaded active running RPCbind Server Activation Socket

syslog.socket loaded inactive dead Syslog Socket

systemd-initctl.socket loaded active listening /dev/initctl Compatibility Named Pipe

systemd-journald.socket loaded active running Journal Socket

systemd-shutdownd.socket loaded active listening Delayed Shutdown Socket

systemd-udevd-control.socket loaded active running udev Control Socket

systemd-udevd-kernel.socket loaded active running udev Kernel Socket

LOAD = Reflects whether the unit definition was properly loaded.

ACTIVE = The high-level unit activation state, i.e. generalization of SUB.

SUB = The low-level unit activation state, values depend on unit type.

14 loaded units listed.

To show all installed unit files use 'systemctl list-unit-files'.

- Hay ciertas dependencias entre SERVICIOS y SOCKETS

systemctl status chronyd -- Vemos que es un demonio que depende del servicio NTP

chronyd.service - NTP client/server

Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled)

Active: active (running) since Tue 2015-02-03 09:21:36 CET; 1h 15min ago

Process: 537 ExecStartPost=/usr/libexec/chrony-helper add-dhclient-servers (code=exited, status=0/SUCCESS)

Process: 484 ExecStart=/usr/sbin/chronyd -u chrony $OPTIONS (code=exited, status=0/SUCCESS)

Main PID: 511 (chronyd)

CGroup: /system.slice/chronyd.service

└─511 /usr/sbin/chronyd -u chrony

Feb 03 09:21:34 localhost chronyd[511]: chronyd version 1.29.1 starting

Feb 03 09:21:35 localhost chronyd[511]: Linux kernel major=3 minor=10 patch=0

Feb 03 09:21:35 localhost chronyd[511]: hz=100 shift\_hz=7 freq\_scale=1.00000000 nominal\_tick=10000 slew\_delta\_tick=833 max\_tick\_bias=1000 shift\_pll=2

Feb 03 09:21:36 localhost systemd[1]: Started NTP client/server.

ps -p 511 -p=process

PID TTY TIME CMD

511 ? 00:00:00 chronyd

Ejemplo:

less /usr/lib/systemd/system/chronyd.service --Podemos ver el script de servicio

[Unit]

Description=NTP client/server

After=ntpdate.service sntp.service ntpd.service --Ejecutarlo despues de estos servicios: ntp..

Conflicts=ntpd.service

[Service]

Type=forking -- Puede hacer fork

EnvironmentFile=-/etc/sysconfig/chronyd

ExecStart=/usr/sbin/chronyd -u chrony $OPTIONS

ExecStartPost=/usr/libexec/chrony-helper add-dhclient-servers -Post del servicio

[Install]

WantedBy=multi-user.target -- Debe eser en el target: multi-user (antes eran runlevel)

- systemd puede cargar servicioso de System V, pero primero se ejecutan los script de systemd

systemctl stop cups.service

Warning: Stopping cups.service, but it can still be activated by: --Ojo avisa que puede ser activado por estas unidades:

cups.path paths

cups.socket sockets

¿COMO VEO LAS DEPENDENCIAS?

systemctl list-dependencies sshd.service

sshd.service

├─system.slice

└─basic.target

├─alsa-restore.service

├─alsa-state.service

├─firewalld.service

. . . . . .

ENMASCARAMIENTO DE LOS SERVICIOS:

- Con systemctl podemos enmascarar servicios

- En RHEL7 hay mucha dependencia con Firewall-d

systemctl mask network

ln -s '/dev/null' '/etc/systemd/system/network.service' -- Crea un link simbolico

-Ahora si intento arrancar el servicio , no me va a dejar

systemctl start network -- Ya NO deja: da Failed !!

Failed to issue method call: Unit network.service is masked.

- Esta idea de enmascarar el servicio de red network, para que no volvamos a RHEL5-6, porque en RHEL7 network-manager nos da mas versatilidad

systemctl unmask network --Borra el link symb y se recupera el servicio

rm '/etc/systemd/system/network.service'

systemctl status network

network.service - LSB: Bring up/down networking

Loaded: loaded (/etc/rc.d/init.d/network)

Active: active (exited) since Tue 2015-02-03 09:21:48 CET; 1h 47min ago

Feb 03 09:21:47 localhost systemd[1]: Starting LSB: Bring up/down networking...

Feb 03 09:21:47 localhost network[866]: Bringing up loopback interface: Could not load file '/etc/sysconfig/network-scripts/ifcfg-lo'

Feb 03 09:21:47 localhost network[866]: Could not load file '/etc/sysconfig/network-scripts/ifcfg-lo'

Feb 03 09:21:48 localhost network[866]: Could not load file '/etc/sysconfig/network-scripts/ifcfg-lo'

Feb 03 09:21:48 localhost network[866]: Could not load file '/etc/sysconfig/network-scripts/ifcfg-lo'

Feb 03 09:21:48 localhost network[866]: [ OK ]

Feb 03 09:21:48 localhost network[866]: Bringing up interface eth0: [ OK ]

Feb 03 09:21:48 localhost systemd[1]: Started LSB: Bring up/down networking.

¿COMO CONTROLAMOS LOS SERVICIOS DURANTE EL ARRANQUE?

systemctl disable sshd.service

rm '/etc/systemd/system/multi-user.target.wants/sshd.service' --Borra el link symbolico

systemctl status sshd.service

sshd.service - OpenSSH server daemon

Loaded: loaded (/usr/lib/systemd/system/sshd.service; disabled) -- Ya no se carga (Load) en el arranque

Active: active (running) since Tue 2015-02-03 10:50:01 CET; 21min ago

Main PID: 3165 (sshd)

CGroup: /system.slice/sshd.service

└─3165 /usr/sbin/sshd -D

Feb 03 10:50:01 server4.example.com systemd[1]: Starting OpenSSH server daemon...

Feb 03 10:50:01 server4.example.com systemd[1]: Started OpenSSH server daemon.

Feb 03 10:50:01 server4.example.com sshd[3165]: Server listening on 0.0.0.0 port 22.

Feb 03 10:50:01 server4.example.com sshd[3165]: Server listening on :: port 22.

Feb 03 10:52:13 server4.example.com systemd[1]: Reloading OpenSSH server daemon.

Feb 03 10:52:13 server4.example.com sshd[3165]: Received SIGHUP; restarting.

Feb 03 10:52:13 server4.example.com sshd[3165]: Server listening on 0.0.0.0 port 22.

Feb 03 10:52:13 server4.example.com sshd[3165]: Server listening on :: port 22.

Feb 03 10:52:13 server4.example.com systemd[1]: Reloaded OpenSSH server daemon.

¿COMO VEMOS LOS TARGETS?

ll /etc/systemd/system

total 12

drwxr-xr-x. 2 root root 54 Dec 9 23:27 basic.target.wants

drwxr-xr-x. 2 root root 30 Dec 9 23:31 bluetooth.target.wants

lrwxrwxrwx. 1 root root 41 Dec 9 23:31 dbus-org.bluez.service -> /usr/lib/systemd/system/bluetooth.service

lrwxrwxrwx. 1 root root 41 Dec 9 23:27 dbus-org.fedoraproject.FirewallD1.service -> /usr/lib/systemd/system/firewalld.service

lrwxrwxrwx. 1 root root 44 May 7 2014 dbus-org.freedesktop.Avahi.service -> /usr/lib/systemd/system/avahi-daemon.service

lrwxrwxrwx. 1 root root 44 Dec 9 23:34 dbus-org.freedesktop.ModemManager1.service -> /usr/lib/systemd/system/ModemManager.service

lrwxrwxrwx. 1 root root 46 May 7 2014 dbus-org.freedesktop.NetworkManager.service -> /usr/lib/systemd/system/NetworkManager.service

lrwxrwxrwx. 1 root root 57 May 7 2014 dbus-org.freedesktop.nm-dispatcher.service -> /usr/lib/systemd/system/NetworkManager-dispatcher.service

lrwxrwxrwx. 1 root root 40 Dec 9 23:38 default.target -> /usr/lib/systemd/system/graphical.target

drwxr-xr-x. 2 root root 85 May 7 2014 default.target.wants

lrwxrwxrwx. 1 root root 35 Dec 9 23:32 display-manager.service -> /usr/lib/systemd/system/gdm.service

drwxr-xr-x. 2 root root 31 May 7 2014 getty.target.wants

drwxr-xr-x. 2 root root 63 Dec 9 23:38 graphical.target.wants

drwxr-xr-x. 2 root root 4096 Feb 3 11:10 multi-user.target.wants

drwxr-xr-x. 2 root root 29 May 7 2014 nfs.target.wants

drwxr-xr-x. 2 root root 25 Dec 9 23:30 printer.target.wants

drwxr-xr-x. 2 root root 4096 Dec 9 23:30 sockets.target.wants

drwxr-xr-x. 2 root root 35 Dec 9 23:34 spice-vdagentd.target.wants

drwxr-xr-x. 2 root root 4096 Dec 9 23:28 sysinit.target.wants

drwxr-xr-x. 2 root root 83 Dec 9 23:30 system-update.target.wants

lrwxrwxrwx. 1 root root 9 May 7 2014 tmp.mount -> /dev/null

Chapter 9. Configuring and Securing OpenSSH service

- SSH original desarrollado por AT&T

-Hay 2 tipos de cifrados:

SIMETRICO

debilidad: "Como se transfiere la clave"

ASIMETRICO

Claves privadas y publicas

- Las comunicaciones se establecen por usuario y por maquina.

-

Establecer conexiones SSH:

1)

[student@server4 ~]$ ssh desktop4 1-- sin nada: ssh maquina

The authenticity of host 'desktop4 (172.25.4.10)' can't be established.

ECDSA key fingerprint is e0:e3:6c:90:c8:ee:88:15:d2:0a:93:e0:bf:58:e7:c5.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'desktop4,172.25.4.10' (ECDSA) to the list of known hosts.

student@desktop4's password:

Last login: Tue Feb 3 09:25:38 2015 from 172.25.4.250

[student@desktop4 ~]$ w -d -- who: UTIL para ver quien se ha conectado por SSH

12:23:27 up 3:02, 3 users, load average: 0.00, 0.01, 0.05 -d = dead

USER TTY LOGIN@ IDLE JCPU PCPU WHAT

student pts/1 12:22 7.00s 0.02s 0.01s w (veo que estoy dentro)

2)

[student@server4 ~]$ ssh student@desktop4 2-- con usuario

student@desktop4's password:

Last login: Tue Feb 3 12:22:58 2015 from server4.example.com

3)

[student@server4 ~]$ ssh student@desktop4 hostname 3-- Ejecutando un comando remoto

student@desktop4's password:

desktop4.example.com

[student@server4 ~]$

4)

[student@server4 ~]$ ssh student@desktop4 'hostname |grep --color desktop'

si ponemos + parametros ==> entre comillas

student@desktop4's password:

desktop4.example.com

[student@server4 ~]$ ssh student@desktop4

student@desktop4's password:

Last failed login: Tue Feb 3 12:28:26 CET 2015 from server4.example.com on ssh:notty

There were 2 failed login attempts since the last successful login. -- Intentos fallidos desde el ultimo login

Last login: Tue Feb 3 12:24:11 2015 from server4.example.com -- Ultimo login

[student@desktop4 ~]$ w -f (who -f) -f = from

12:29:38 up 3:08, 3 users, load average: 0.00, 0.03, 0.05

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

student pts/0 172.25.4.250 09:25 2:59m 0.03s 0.03s -bash

student pts/1 server4.example. 12:28 2.00s 0.01s 0.00s w -f -Nos dice desde donde FROM

CALVES PUBLICAS y CLAVES PRIVADAS

[student@server4 .ssh]$ ssh desktop4

The authenticity of host 'desktop4 (172.25.4.10)' can't be established.

ECDSA key fingerprint is e0:e3:6c:90:c8:ee:88:15:d2:0a:93:e0:bf:58:e7:c5. -- ¿es esta la clave publica (huella) que envia desktop4?

Are you sure you want to continue connecting (yes/no)?

¿como compuebo la huella?

[student@desktop4 ssh]$ ssh-keygen -lf /etc/ssh/ssh\_host\_ecdsa\_key.pub

256 e0:e3:6c:90:c8:ee:88:15:d2:0a:93:e0:bf:58:e7:c5 (ECDSA)

[student@server4 .ssh]$ ssh desktop4

student@desktop4's password:

Last login: Tue Feb 3 12:28:30 2015 from server4.example.com

- Ahora ya nos ha incorporado esa clave publica en el fichero /home/student/.ssh/known\_hosts

Practica 2)

[root@desktop4 ssh]# rm -f /etc/ssh/\*host\*key\*

[root@desktop4 ssh]# systemctl restart sshd

[root@desktop4 ssh]# ll

total 268

-rw-------. 1 root root 242153 Mar 19 2014 moduli

-rw-r--r--. 1 root root 2123 Mar 19 2014 ssh\_config

-rw-r--r--. 1 root root 4439 Dec 9 23:38 sshd\_config

-rw-r-----. 1 root ssh\_keys 227 Feb 3 12:43 ssh\_host\_ecdsa\_key

-rw-r--r--. 1 root root 162 Feb 3 12:43 ssh\_host\_ecdsa\_key.pub

-rw-r-----. 1 root ssh\_keys 1675 Feb 3 12:43 ssh\_host\_rsa\_key

-rw-r--r--. 1 root root 382 Feb 3 12:43 ssh\_host\_rsa\_key.pub

[student@server4 .ssh]$ ssh desktop4 -- Ha cambiado la huella desktop4.. OJO!

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-middle attack)!

It is also possible that a host key has just been changed.

The fingerprint for the ECDSA key sent by the remote host is

35:c3:ae:5a:1b:60:fa:74:e1:4d:3c:aa:b1:17:99:d7.

Please contact your system administrator.

Add correct host key in /home/student/.ssh/known\_hosts to get rid of this message.

Offending ECDSA key in /home/student/.ssh/known\_hosts:1

ECDSA host key for desktop4 has changed and you have requested strict checking.

Host key verification failed.

¿Como lo arreglamos?

- Se desaconseja modificar el fichero /home/student/.ssh/known\_hosts !!

Mejor hacer:

[student@server4 .ssh]$ ssh-keygen -R desktop4 -- Regenero el know host

# Host desktop4 found: line 1 type ECDSA

/home/student/.ssh/known\_hosts updated.

Original contents retained as /home/student/.ssh/known\_hosts.old

Ahora ya si , nos podemos conectar:

[student@server4 .ssh]$ ssh desktop4

The authenticity of host 'desktop4 (172.25.4.10)' can't be established.

ECDSA key fingerprint is 35:c3:ae:5a:1b:60:fa:74:e1:4d:3c:aa:b1:17:99:d7.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'desktop4,172.25.4.10' (ECDSA) to the list of known hosts.

student@desktop4's password:

Last login: Tue Feb 3 12:41:31 2015 from server4.example.com

[student@server4 .ssh]$ ssh -vvv desktop4 --Por si queremos depurar el SSH

OpenSSH\_6.4, OpenSSL 1.0.1e-fips 11 Feb 2013

debug1: Reading configuration data /etc/ssh/ssh\_config

debug1: /etc/ssh/ssh\_config line 51: Applying options for \*

debug2: ssh\_connect: needpriv 0

debug1: Connecting to desktop4 [172.25.4.10] port 22.

vim /etc/ssh/ssh\_config

# StrictHostKeyChecking ask -- Si ponemos "no" : aceptara todas las huellas sin preguntar !!! nunca hacerlo

man 5 ssh\_config

GlobalKnownHostsFile -- Ponemos en 1 fichero SOLO ACCESIBLE por root

-- las claves unicas de los servidores a los cuales los usaurios se van a conectar

SSH con CLAVES PUBLICAS y PRIVADAS

1º) Necesitamos que nuestro cliente entregue las claves publicas y privadas

- Generamos el par de claves publica y privada

[student@server4 .ssh]$ ssh-keygen -- Generamos el par de claves

Generating public/private rsa key pair. -- rsa=algoritmo cifrado

Enter file in which to save the key (/home/student/.ssh/id\_rsa): -- Directorio por defecto

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/student/.ssh/id\_rsa.

Your public key has been saved in /home/student/.ssh/id\_rsa.pub.

The key fingerprint is:

9a:55:8f:1f:10:36:b1:71:7e:cf:1e:1e:98:d9:77:05 student@server4.example.com

The key's randomart image is:

+--[ RSA 2048]----+

| \*.. E |

| . B . |

| + . . .|

| . + .=o.|

| S . o+ +=|

| + . ...=|

| o . ..|

| |

| |

+-----------------+

[student@server4 .ssh]$ ll

total 20

-rw-------. 1 student student 1651 Dec 9 23:22 authorized\_keys

-rw-------. 1 student student 1679 Feb 3 13:08 id\_rsa -- Clave Privada , permisos 600

-rw-r--r--. 1 student student 409 Feb 3 13:08 id\_rsa.pub -- Clave publica

-rw-------. 1 student student 182 Feb 3 12:49 known\_hosts

-rw-r--r--. 1 student student 182 Feb 3 12:41 known\_hosts.old

MECANISMOS PARA ENVIAR LA CLAVE PUBLICA

- Lo ideal es llevarlo con un pendrive USB

student@server4 .ssh]$ ssh-copy-id desktop4 -- Enviamos el id\_rsa.pub a donde me quiero conectar

Number of key(s) added: 1 -- al fichero /home/student/.ssh/authorized\_key de desktop4

Now try logging into the machine, with: "ssh 'desktop4'"

and check to make sure that only the key(s) you wanted were added.

[student@server4 .ssh]$ ssh -vv desktop4 -- Deputacion del ssh

OpenSSH\_6.4, OpenSSL 1.0.1e-fips 11 Feb 2013

debug1: Reading configuration data /etc/ssh/ssh\_config

debug1: /etc/ssh/ssh\_config line 51: Applying options for \*

debug2: ssh\_connect: needpriv 0

...

[student@server4 .ssh]$ ssh desktop4

Last login: Tue Feb 3 13:16:14 2015 from server4.example.com

[student@desktop4 ~]$

CUSTOMIZAR SSH Service Configuration

- Seguridad de acceso fisica

- Seguridad a nivel del RED (paquetes)

- Seguridad Filtrado y TCP-wrappers

- Seguridad Servicios

- Seguridad SSH

vim /etc/ssh/sshd\_config

- Puertos > 1024 Cualquier usuario puede hacer un socket (ya que es un port administrativo)

#Port 22

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

# The default requires explicit activation of protocol 1

#Protocol 2

# HostKey for protocol version 1

#HostKey /etc/ssh/ssh\_host\_key

# HostKeys for protocol version 2

HostKey /etc/ssh/ssh\_host\_rsa\_key

#HostKey /etc/ssh/ssh\_host\_dsa\_key

HostKey /etc/ssh/ssh\_host\_ecdsa\_key

#PermitRootLogin yes -- Por defecto permite a root !!! OJO... se aconseja poner NO

#PasswordAuthentication yes -- Si ponemos NO es mas seguro

GENERACION DE CLAVES type=DSA

-Cuando ejecutamos el cliente SSH busca estos ficheros en el $HOME/.ssh/

identity

id\_rsa

id\_rsa.pub

-Si no las encuentra da un error de este tipo:

"/usr/bin/ssh-copy-id: ERROR: No identities found"

Practica:

1)

[student@desktop4 .ssh]$ ssh-copy-id student@server4

/usr/bin/ssh-copy-id: ERROR: No identities found

[student@desktop4 .ssh]$ ll

total 12

-rw-------. 1 student student 1651 Dec 9 23:22 authorized\_keys

-rw-------. 1 student student 668 Feb 4 09:33 studen\_desktop4

-rw-r--r--. 1 student student 618 Feb 4 09:33 studen\_desktop4.pub

[student@desktop4 .ssh]$ ssh-copy-id -i studen\_desktop4 student@server4

The authenticity of host 'server4 (172.25.4.11)' can't be established.

ECDSA key fingerprint is e0:e3:6c:90:c8:ee:88:15:d2:0a:93:e0:bf:58:e7:c5.

Are you sure you want to continue connecting (yes/no)? yes

/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed

/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys

student@server4's password: student

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'student@server4'"

and check to make sure that only the key(s) you wanted were added.

2) SI MIRAMOS EN SERVER4, veremos :

[student@server4 .ssh]$ tail authorized\_keys

ssh-dss  student@desktop4.example.com

3)

[student@desktop4 .ssh]$ ssh server4

student@server4's password: -- Ops .. pero me pide clave !!

4) Si le especifico el el fichero de intentidad que le he mandado ==> ya no me pide clave

[student@desktop4 .ssh]$ ssh -i /home/student/.ssh/studen\_desktop4 server4 ( -i = identity\_file )

Last login: Wed Feb 4 09:12:42 2015 from 172.25.4.250

[student@server4 ~]$

5) Si miramos en /etc/ssh/ssh\_config (fichero de configuracion del cliente)

# Configuration data is parsed as follows: -- Este es el orden de como actual el cliente SSH

# 1. command line options -- 1. por linea de comando

# 2. user-specific file -- 2. por fichero de usuario especifico

# 3. system-wide file -- 3. por fichero global del sistema

6) man 5 ssh\_config

SYNOPSIS

~/.ssh/config 1º mira en FICHERO CONFIG. del usuario

/etc/ssh/ssh\_config 2º mira en FICHERO GLOBAL de la maquina

student@desktop4 .ssh]$ vim ~/.ssh/config -- Creamos este fichero con permisos 600

Host server4 server0.example.com 172.25.4.11

IdentityFile ~/.ssh/studen\_desktop4

User student -- solo para student

UserKnownHostsFile /dev/null -- cada vez que hago un SSH le pide la clave al servidor

StrictHostKeyChecking no -- OJO! no=no pregunta las claves al servidor !!!

(StrictHostKeyChecking yes|no|ask)

VisualHostKey yes

OJO, con esto "student" nunca se podrá conectar por SSH !!!

UserKnownHostsFile /dev/null -- cada vez que hago un SSH le pide la clave al servidor

StrictHostKeyChecking yes -- OJO! pregunta las claves al servidor !!!

[student@desktop4 .ssh]$ ssh server4

No ECDSA host key is known for server4 and you have requested strict checking.

Host key verification failed.

ssh-agent:

- Es un llavero de claves que memoriza las passphrase.

- Se encarga de los passphrase de la sesion

- En GNOME va diferente

-Solo lee las claves privadas del tipo:

identity

rsa

dsa

-A no ser que hagamos:

ssh-keygen -p -f studen\_desktop4 (le ponemos student)

-COMO VEMOS SI ESTA LANZADO el shs-agent?

[student@desktop4 .ssh]$ eval $(ssh-agent) -- Vemos el PID del ssh-agent

Agent pid 30299

- VAMOS A DECIRLE AL SSH-AGENT QUE AÑADA EL FICHERO:

[student@desktop4 .ssh]$ ssh-add studen\_desktop4

Enter passphrase for studen\_desktop4:

Identity added: studen\_desktop4 (studen\_desktop4)

[student@desktop4 .ssh]$

SERVIDOR SSH

Vamos a ver el fichero /etc/ssh/sshd\_config

-Directivas importantes:

1)

DenyUsers -- Le vamos a pasar una lista que USERS que no van a poder acceder por SSH

2)

Allowusers

Ej Allowusers visitor@server4.example.com studen@server4.example.com admin

Allowusers \*.example.com

3)

DenyGroups

4)

AllowGroups

Herramienta PORT-KNOCKER:

Se hace peticiones porp "Puerto, frecuencia y protocolo"

El paquete es knckd

TUNELING de SSH

-Son los albores de las VPNs

-Los servidores FTP hoy en dia tienen el modo ASCII deshabilitado

TUNEL SSH

- Abrimos una conexion por SSH y por debajo transferiemos un servicio

INSTALAMOS EL HTTP en server4

sudo yum install -y httpd -- Instalamos el httpd

[student@server4 ssh]$ sudo systemctl start httpd

[student@server4 ssh]$ sudo systemctl status httpd

httpd.service - The Apache HTTP Server

Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled)

Active: active (running) since Wed 2015-02-04 11:13:31 CET; 9s ago

Main PID: 30922 (httpd)

Status: "Processing requests..."

CGroup: /system.slice/httpd.service

├─30922 /usr/sbin/httpd -DFOREGROUND

├─30923 /usr/sbin/httpd -DFOREGROUND

├─30924 /usr/sbin/httpd -DFOREGROUND

├─30925 /usr/sbin/httpd -DFOREGROUND

├─30926 /usr/sbin/httpd -DFOREGROUND

└─30927 /usr/sbin/httpd -DFOREGROUND

Feb 04 11:13:31 server4.example.com systemd[1]: Started The Apache HTTP Server.

[student@server4 ssh]$ ss -tulipan|grep :80

tcp LISTEN 0 128 :::80 :::\*

[student@server4 ssh]$

[root@server4 ~]# firewall-cmd --add-service=http -- Permitimos al FIREWALL el http

success

Ahora ya si accedemos desde desktop4 al http

VAMOS A TUNELIZAR LA CONEXION HTTP:

[student@desktop4 .ssh]$ ssh --help

unknown option -- -

usage: ssh [-1246AaCfgKkMNnqsTtVvXxYy] [-b bind\_address] [-c cipher\_spec]

[-D [bind\_address:]port] [-E log\_file] [-e escape\_char]

[-F configfile] [-I pkcs11] [-i identity\_file]

[-L [bind\_address:]port:host:hostport] [-Q protocol\_feature]

[-l login\_name] [-m mac\_spec] [-O ctl\_cmd] [-o option] [-p port]

[-R [bind\_address:]port:host:hostport] [-S ctl\_path]

[-W host:port] [-w local\_tun[:remote\_tun]]

[user@]hostname [command]

[student@desktop4 .ssh]$ ssh -L 8080:server4:80 root@server4

--Explicacion: Desde el puerto 8080 de la maquina local (desktop4) --> redirigimos hacia puerto 80 de server4

--Es un tunel directo: puerto --> puerto

root@server4's password:

Last login: Wed Feb 4 11:18:58 2015

[student@desktop4 .ssh]$ ssh -NL 8080:server4:80 root@server4 N= No command

[student@desktop4 .ssh]$ ssh -NfL 8080:server4:80 root@server4 f =devuelve la sesion

Ahora si ponemos en el navegador de student4:

http://localhost:8080 --> Accedemos al apache de server4

[student@desktop4 ~]$ ss -tulipan|grep 8080

tcp LISTEN 0 128 127.0.0.1:8080 \*:\* users:(("ssh",1022,5))

tcp LISTEN 0 128 ::1:8080 :::\* users:(("ssh",1022,4))

[student@desktop4 ~]$ ps aux|grep ssh

student 1022 0.0 0.2 76652 4084 pts/0 S+ 12:14 0:00 ssh -L 8080:server4:80 root@server4

root 1154 0.0 0.1 82956 3540 ? Ss 09:08 0:00 /usr/sbin/sshd -D

student 1245 0.0 0.0 112640 936 pts/1 R+ 12:28 0:00 grep --color=auto ssh

root 1536 0.0 0.2 135680 4824 ? Ss 09:11 0:00 sshd: student [priv]

student 1540 0.0 0.1 135680 2200 ? S 09:11 0:00 sshd: student@pts/0

root 30214 0.0 0.2 135680 4824 ? Ss 10:39 0:00 sshd: student [priv]

student 30218 0.0 0.1 135680 2204 ? S 10:39 0:00 sshd: student@pts/1

student 30299 0.0 0.0 53320 768 ? Ss 10:40 0:00 ssh-agent

student 32213 0.0 0.0 53320 572 ? Ss 11:18 0:00 /usr/bin/ssh-agent /bin/sh -c exec -l /bin/bash -c "env GNOME\_SHELL\_SESSION\_MODE=classic gnome-session --session gnome-classic"

[student@desktop4 ~]$

SSH tiene un char de ESCAPE ==> ~

Si tecleamos "~" + "C"

[root@server4 ~]#

ssh> --Nos sale un prompt del SSH

ssh> help

Commands:

-L[bind\_address:]port:host:hostport Request local forward

-R[bind\_address:]port:host:hostport Request remote forward

-D[bind\_address:]port Request dynamic forward

-KL[bind\_address:]port Cancel local forward

-KR[bind\_address:]port Cancel remote forward

-KD[bind\_address:]port Cancel dynamic forward

[root@server4 ~]#

ssh> -L 8080:server4:80 -- Ahora es como si estuvieramos en "desktop4" : En el cliente

-- Crea el Port Forwarding

Forwarding port.

ssh> -KL 8080 -- Cancela el reenvio

Canceled forwarding.

AHORA

TUNEL DINAMICO

[student@desktop4 ~]$ ssh -D 1080 server4 -- Creo un proxy dinamico hacia server4

-- Todas las conexiones que se hagan en el puerto 1080

- Esto es crear un proxy DINAMICO version 5

PS1

COLORES:

man dir\_colors -- Para poner colores al Prompt

Los colores se dividen en 3 sections:

1º section 0-5 Para alterar el comportamiento

2ª section 30-37 Foregorund Color : en primer plano

3ª section 40-47 Background Color: el fondo

0 to restore default color

1 for brighter colors

4 for underlined text

5 for flashing text

30 for black foreground

31 for red foreground

32 for green foreground

33 for yellow (or brown) foreground

34 for blue foreground

35 for purple foreground

36 for cyan foreground

37 for white (or gray) foreground

40 for black background

41 for red background

42 for green background

43 for yellow (or brown) background

44 for blue background

45 for purple background

46 for cyan background

47 for white (or gray) background

- Cada shell interpreta las secuencias de escapes de una forma distinta

Hay 2 tipos de ESCAPE:

1) char de ESCAPE = Ej: \n (salto de linea)

2) secuencia de ESCAPE = secuencia INICIO \[ e[ (left code)

secuencia FIN m\] (right code)

$EUID = Efective User IDentification

CHARS UNICODE:

SHIFT + CTRL + U ==> u + Secuencia de caracteres (ej: 10392)

5-2-11

Chapter 10. Analizing and Storing Logs

En RHEL7 el tema de los LOGS: CAMBIA BASTANTE

Cambios:

1. journald: Registra los eventos del sistema en los LOGS

2. Sigue estando NTP pero vamos a usar CRON

DIRECTORIO DE LOGS: /var/log

Los LOG's estan gestionado por 2 servicios:

1. systemd-journdald - Demonio que captura eventos generados por kernel, early stages, boot process, salida standar/error

de los demonios que arranquen y se ejecuten... asi como el syslog.

- Los muestra mas ampliados y detallados

2. rsyslog Servicio que ordena los mensajes del syslog

Guarda los eventos en /var/log

Vistazo de ficheros log del sistema:

/var/log/messages Casi todos los eventos del sistema van aqui

/var/log/secure Eventos relativos a las autenticaciones

/var/log/maillog Eventos relativos a los mails SMTP

/var/log/cron Eventos relativos al cron

/var/log/boot.log Eventos relativos al arranque del sistema

Reviewing Syslog Files rsyslog

-syslogd es heredado de otras versiones de RH

syslog vs rsyslog

rsyslog Permite trabajar con servers remotos con TCP y cifradas

syslog Solo UDP y sin cifrar

rsyslogd: Genera eventos de un recurso

recursos: Son elementos que generan EVENTO.

auth

authpriv

kernel

mail

user

local0 .. local7

prioridad: Es el nivel de importancia del EVENTO

De menos a mas en orden inverso

- Codigos de prioridad:

7 Debug

6 Info

5 notice

4 warnning

3 err

2 crit

1 alert

0 emerg (antes panic, en desuso)

Cuando se guarda un evento, se registran desde la prioridad mas alta hacia la mas baja (ej: prior=4 ==> 4+3+2+1+0)

Fichero de configuracion:

/etc/rsyslog.conf -Aqui habrá directvias

cd /etc/rsyslog.d/; ll - Estos ficheros de conf. los lee en orden alfabetico (ASCII)

total 16

-rw-r--r--. 1 root root 253 Dec 3 2013 21-cloudinit.conf

-rw-r--r--. 1 root root 2564 Feb 4 2014 gluster.conf.example

-rw-r--r--. 1 root root 49 Apr 2 2014 listen.conf

-rw-r--r--. 1 root root 291 Jan 27 2014 spice-vdagentd.conf

[root@server4 etc]# cat /etc/rsyslog.conf -Dividido en MODULOS y REGLAS

1ª parte de rsyslog.conf

#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsock.

$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)

$ModLoad imjournal # provides access to the systemd journal

#$ModLoad imklog # reads kernel messages (the same are read from journald)

#$ModLoad immark # provides --MARK-- message capability

# Provides UDP syslog reception

#$ModLoad imudp

#$UDPServerRun 514

# Provides TCP syslog reception

#$ModLoad imtcp

#$InputTCPServerRun 514

2ª parte de rsyslog.conf

REGLAS = Coincidencias de EVENTOS

Ojo, un evento puede ser generado sin prioridad = none

#### RULES ####

# Log all kernel messages to the console.

# Logging much else clutters up the screen.

#kern.\* /dev/console

# 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

El guion (-) significa que hace writes asincronas

# 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

3ª parte:

REGLAS DE RE-ENVIO (a parte de servidor, rsyslog puede ser cliente)

Hay que indicar: resurce, prioridad, protocolo a enviar, puerto

@ = UDP

@@ = TCP

Se aplican todas las reglas

# ### begin forwarding rule ###

# The statement between the begin ... end define a SINGLE forwarding

# rule. They belong together, do NOT split them. If you create multiple

# forwarding rules, duplicate the whole block!

# Remote Logging (we use TCP for reliable delivery)

#

# An on-disk queue is created for this action. If the remote host is

# down, messages are spooled to disk and sent when it is up again.

#$ActionQueueFileName fwdRule1 # unique name prefix for spool files

#$ActionQueueMaxDiskSpace 1g # 1gb space limit (use as much as possible)

#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown

#$ActionQueueType LinkedList # run asynchronously

#$ActionResumeRetryCount -1 # infinite retries if host is down

# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional

#\*.\* @@remote-host:514 -- Se puede enviar a un server remoto

# ### end of the forwarding rule ###

ELINKS

sudo yum install elinks -- Es una utilidad para ver mejor la info en el firefox

Log file rotation

Utilidad logrotate

-Cuando un log es rotado pasara de llamarse /var/log/message . . .> /var/log/message-20150205

-Cuando rotan todos los logs: Siempre se elimina el mas antiguo de todos.

less /etc/logrotate.conf --> fichero de configuracion del "logrotate"

---------------------------

# see "man logrotate" for details

# rotate log files weekly

weekly -- Rota cada semana

# keep 4 weeks worth of backlogs

rotate 4 -- Hay 4 copias de segurdad

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

create -- Crea un fichero vacio

# use date as a suffix of the rotated file

dateext -- Usamos la fecha como extension (SUFIJO) de los logs

# uncomment this if you want your log files compressed

#compress

# RPM packages drop log rotation information into this directory

include /etc/logrotate.d -- Ficheros de conf. adicional

# no packages own wtmp and btmp -- we'll rotate them here

/var/log/wtmp {

monthly -- Rota cada mes

create 0664 root utmp

minsize 1M -- Cuando alcaza el 1MG rotará

rotate 1 -- Nº de copias que se mantienen (en total serían 2)

}

/var/log/btmp {

missingok -- Es posible que el fichero no exista

monthly -- Rotacion mensual

create 0600 root utmp -- Usuario/grupo= root:utmp

rotate 1 -- Solo 1 copia (btmp y btmp.1)

}

# system-specific logs may be also be configured here

FILTROS

- Podemos añadir FILTROS en base al payload (el cuerpo del mensaje):

http://www.rsyslog.com/doc/v7-stable/configuration/filters.html

:msg, contains, "informational" ~ -- La culebrilla = solo para este FILTRO

less /etc/logrotate.d/syslog

/var/log/cron -- Mensajes que logs que van a rotar

/var/log/maillog

/var/log/messages

/var/log/secure

/var/log/spooler

{

sharedscripts

postrotate -- Que hará cuando rote

/bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true

endscript

}

¿QUIEN SE ENCARGA DE LA ROTACION?

[root@server4 /]# ll /etc/cron.daily/

total 20

-rwxr-xr-x. 1 root root 332 Apr 8 2014 0yum-daily.cron

-rwx------. 1 root root 180 Jul 31 2013 logrotate -- Aqui está! dentro de /etc/cron.daily

[root@server4 cron.daily]# cat logrotate

#!/bin/sh

/usr/sbin/logrotate /etc/logrotate.conf

EXITVALUE=$?

if [ $EXITVALUE != 0 ]; then

/usr/bin/logger -t logrotate "ALERT exited abnormally with [$EXITVALUE]"

fi

exit 0

tail -n1 /var/log/secure -- desmenuzamos un log cualquiera:

Feb 5 10:10:13 - - Fecha / hora

localhost --Maquina

polkitd[581]: --Programa que ha generado el evento

Registered Authentication Agent for unix-session:7 (system bus name :1.70 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en\_US.UTF-8)

-- Cuerpo del mensaje: Nos dice el Agenteque lo ha provocado, shell, path-Agente, y el locale

- Podemos invocar directamente nosotros al logrotate con el comando logger:

loggerp -p Generamos un evento artificial con EVENTO y PRIORIDAD

logger -p local6.emerg "Hay que reiniciar Windows" -- locale6 es un recurso local

Reviewing systemd Journal Entries: journalcrl

-Guarda sus logs en un sitio volatil: /run/log por defecto

journalctl

-- Logs begin at Thu 2015-02-05 09:32:55 CET, end at Thu 2015-02-05 10:54:01 CET. --

Feb 05 09:32:55 localhost systemd-journal[83]: Runtime journal is using 8.0M (max 92.0M, leaving 138.0M of free 912.5M

Feb 05 09:32:55 localhost systemd-journal[83]: Runtime journal is using 8.0M (max 92.0M, leaving 138.0M of free 912.5M

Feb 05 09:32:55 localhost kernel: Initializing cgroup subsys cpuset

Feb 05 09:32:55 localhost kernel: Initializing cgroup subsys cpu

Feb 05 09:32:55 localhost kernel: Initializing cgroup subsys cpuacct

Feb 05 09:32:55 localhost kernel: Linux version 3.10.0-123.el7.x86\_64 (mockbuild@x86-017.build.eng.bos.redhat.com) (g

En negrita:: Eventos: NOTICE o WARNING

En ROJO Eventos: ERRORS y superior

journalctl -n -- 10 ultimas entradas

journalctl -n 2 -- 2 ultimas entradas

Ejemplo:

Feb 05 09:32:55 localhost kernel: Initializing cgroup subsys cpuacct

Feb 05 09:32:55 localhost kernel: Linux version 3.10.0-123.el7.x86\_64 (mockbuild@x86-017.build.eng.bos.redhat.com) (gc

Feb 05 09:32:55 localhost kernel: Command line: BOOT\_IMAGE=/boot/vmlinuz-3.10.0-123.el7.x86\_64 root=UUID=9bf6b9f7-92ad

Feb 05 09:32:55 localhost kernel: Failed to access perfctr msr (MSR c1 is 0)

[root@server4 journal]# pwd

/run/log/journal

[root@server4 journal]# ll

total 0

drwxr-xr-x. 2 root root 60 Feb 5 09:32 689415920a314574b19ba85bbe57ceb6

drwxr-sr-x. 2 root systemd-journal 60 Feb 5 09:33 946cb0e817ea4adb916183df8c4fc817

journalctl -p 3 -n1 -- Prioridad 3, muestra 1 linea

-- Logs begin at Thu 2015-02-05 09:32:55 CET, end at Thu 2015-02-05 10:54:01 CET. --

Feb 05 10:10:12 server4.example.com bluetoothd[2319]: Parsing /etc/bluetooth/input.conf failed: No such file or direct

journalctl -f -- Follow (como tail -f)

journalctl --since today -- Eventos generados desde HOY a las 00:00

journalctl --since "2015-02-05 10:00:00" --until "2015-02-05 11:00:00"

journalctl --since "2015-02-05 10:00" --until "2015-02-05 11:00" \_COMM=logger

comando "logger"

systemd Journal de manera persistente

-Para que sea persistente el journald ==> Creamos el directorio y hacemos estos pasos:

mkdir /var/log/journal

chown root:systemd-journal /var/log/journal - Dueño rooot y grupo systemd-journal

chmod 2775 /var/log/journal - sgid=1

killall -USR1 systemd-journald -- reiniciamos el demonio journal

journalctl -b -- Muestra mensajes desde el ultimo reinicio (solo tiene sentido para los persistentes) -b=boot

journalctl -b -1 -- Muestra mensajes desde el arranque anterior al ultimo arranque

Maintaining Accurate Time (mantenimiento de la hora exacta)

-Nos olvidamos del comando date !!

-Aunque podemos ejecutarlo para ver la fecha/hora

-Ahora se usa:

timedatectl -- Nos muestra como está configurado

Local time: Thu 2015-02-05 12:22:31 CET

Universal time: Thu 2015-02-05 11:22:31 UTC

RTC time: Thu 2015-02-05 11:22:31 RTC=Real Time Clock (suele ir con pilas)

Timezone: Europe/Madrid (CET, +0100)

NTP enabled: yes

NTP synchronized: no

RTC in local TZ: no

DST acti ve: no

Last DST change: DST ended at

Sun 2014-10-26 02:59:59 CEST

Sun 2014-10-26 02:00:00 CET

Next DST change: DST begins (the clock jumps one hour forward) at

Sun 2015-03-29 01:59:59 CET

Sun 2015-03-29 03:00:00 CEST

¿ZONAS HORARIAS?

timedatectl list-timezones --Nos muestra todas las que hay

Africa/Abidjan

Africa/Accra

Africa/Addis\_Ababa

Africa/Algiers

Africa/Asmara

Africa/Bamako

tzselect -- Para ver la zona en la que estoy

¿COMO MODIFICO LA ZONA?

timedatectl set-timezone Europe/London --Si queremos cambiarla

¿ESTABLECER LA HORA?

timedatectl set-time 12:30

¿HABILITAR/DESHABILITAR SERVICIOS DE HORA?

timedatectl set-ntp yes/false

HORA

-Se puede seguir usando NTP , pero usa servicios systemV

-RHEL7 usa chronyd

-Los NTP time se determinan por stratos

stratos: Son capas de servers

Peers: Son servers que están en el mismo strato

Fichero de Configuracion de chronyd: /etc/chrony.conf

[student@server4 ~]$ cat /etc/chrony.conf

# Use public servers from the pool.ntp.org project.

# Please consider joining the pool (http://www.pool.ntp.org/join.html).

server 0.rhel.pool.ntp.org iburst --Formato: server DNS / IP Address [ iburst ] (iburst=4 veces la peticion)

server 1.rhel.pool.ntp.org iburst

server 2.rhel.pool.ntp.org iburst

server 3.rhel.pool.ntp.org iburst

# Ignore stratum in source selection.

stratumweight 0

# Record the rate at which the system clock gains/losses time.

driftfile /var/lib/chrony/drift -- Fichero de desliz: Almacena el desliz de tiempo des-ajustado

"cuantas partes de tiempo pierde el reloj del sistema"

- Cuando la hora-sistema es +- 15minutos ==> deja de sincronizarse

- Esto es por si hay ataques MITM

- Hubo que crearlo a mano

# Enable kernel RTC synchronization.

rtcsync

# In first three updates step the system clock instead of slew

# if the adjustment is larger than 10 seconds.

makestep 10 3

# Allow NTP client access from local network.

#allow 192.168/16

# Listen for commands only on localhost.

bindcmdaddress 127.0.0.1

bindcmdaddress ::1

# Serve time even if not synchronized to any NTP server.

#local stratum 10

keyfile /etc/chrony.keys

# Specify the key used as password for chronyc.

commandkey 1

# Generate command key if missing.

generatecommandkey

# Disable logging of client accesses.

noclientlog

# Send a message to syslog if a clock adjustment is larger than 0.5 seconds.

logchange 0.5

logdir /var/log/chrony

#log measurements statistics tracking

[student@server4 ~]$ chronyc sources -v == lo que antes era el "ntp -q"

-- Verifica el time-source para sincronizacion del sistema

210 Number of sources = 4

.-- Source mode '^' = server, '=' = peer, '#' = local clock.

/ .- Source state '\*' = current synced, '+' = combined , '-' = not combined,

| / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.

|| .- xxxx [ yyyy ] +/- zzzz

|| / xxxx = adjusted offset,

|| Log2(Polling interval) -. | yyyy = measured offset,

|| \ | zzzz = estimated error.

|| | |

MS Name/IP address Stratum Poll Reach LastRx Last sample

===============================================================================

^? 84.88.69.32 0 10 0 10y +0ns[ +0ns] +/- 0ns

^? 147.83.123.133 0 10 0 10y +0ns[ +0ns] +/- 0ns

^? julio.masbytes.es 0 10 0 10y +0ns[ +0ns] +/- 0ns

^? static-21.hercom.es 0 10 0 10y +0ns[ +0ns] +/- 0ns

Chapter 11. Networking

nux = Servidor de Repositorio Externo a RHEL

Terminator = Desde li.nux.ro se puede descargar

TCP/IP standard: 4 capas:

4. Aplicacion: Comunicacion entre C/S. Ejemplos: Web, telnet, ssh

3. Transport: Protocolo que va a usar: TCP / UDP

TCP = Confiable, orientadoa la comunicacion

UPD = Protocolo de Datagrama connectionless

/etc/services = Ports well-know

2. Internet. ping

1. Link.

802.3 Ethernet

802.11 WLAN

Cada device tiene una MAC

DNS

1ª busqueda:

Stub Resolver

Es un DNS local: Fichero /etc/hosts

2 busqueda:

Direccion del servidor DNS

(OJO con el fichero de hosts... porque podemos traernos IP's falsas que hagan PISHING)

DHCP

Se va a usar la MAC de la maquina para asignar direcciones IP's

1. configuracion estatica:

Tenemos en 1 tabla todas las MAC's de las maquina

Es mas segura.

2. configuracion dinamica:

En el server DHCP hay una tabla de leases (arrendamientos):

Siempre va a asingar la misma direccion IP

MAC- IP - TTL (TTL=Tiempo de vida)

A veces para eliminar una fila de la tabla de leases --> es necesario resetear el router

NETWORK INTERFACES name

RHEL5:

eth0 wlan1 Ethernet

efcoe Fibber Channel

wlan0 wlan1 WLAN

RHEL7:

Interfaces:

en Ethernet

wl WLAN

ww WWAN

Tipo Adaptador

o on-board Placa

s hotplug-slot Conectable

p PCI

Number:

1

2

Puerto:

s1

s2

- -- - -

Ejemplo:

enp1s2

en ethernet

p1 pci1

s2 Puerto s2

-Para tener las conveciones anteriores, es necesario instalar el paquete:

biosdevname (no va instalado en RHEL7)

rpm -q biosdevname -- Comprobacion

biosdevname-0.5.0-10.el7.x86\_64

udevadm - Controla el comportamiento de ejecución de udevd systemd

udevadm info /sys/class/net/eth0

P: /devices/pci0000:00/0000:00:03.0/virtio0/net/eth0

E: DEVPATH=/devices/pci0000:00/0000:00:03.0/virtio0/net/eth0

E: ID\_BUS=pci

E: ID\_MM\_CANDIDATE=1

E: ID\_MODEL\_FROM\_DATABASE=Virtio network device

E: ID\_MODEL\_ID=0x1000

E: ID\_NET\_NAME\_MAC=enx52540000040b

E: ID\_PCI\_CLASS\_FROM\_DATABASE=Network controller

E: ID\_PCI\_SUBCLASS\_FROM\_DATABASE=Ethernet controller

E: ID\_VENDOR\_FROM\_DATABASE=Red Hat, Inc

E: ID\_VENDOR\_ID=0x1af4

E: IFINDEX=2

E: INTERFACE=eth0

E: SUBSYSTEM=net

E: SYSTEMD\_ALIAS=/sys/subsystem/net/devices/eth0

E: TAGS=:systemd:

E: USEC\_INITIALIZED=82462

cat /etc/udev/rules.d/70-xx -- Aqui se puede poner reglas, para dejar persistentes los nombres de interfaces

Validate Network Configuration

No usar ifconfig !!!

Las confifguraciones que hagamos con NETWORK MANAGER ==> NO SERAN VISIBLES SI LAS HACEMOS CON ifconfig

Comando ip

Permite modirficar y visualizar la conf de red.

ip addr

ip link

ip route

Practica: Estando en server4:

ip addr

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN

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 pfifo\_fast state UP qlen 1000

link/ether 52:54:00:00:04:0b brd ff:ff:ff:ff:ff:ff

inet 172.25.4.11/24 brd 172.25.4.255 scope global dynamic eth0

valid\_lft 16526sec preferred\_lft 16526sec

inet6 fe80::5054:ff:fe00:40b/64 scope link

valid\_lft forever preferred\_lft forever

ip addr show eth0 --Vemos la interfaz de red como link

2: eth0: <BROADCAST,MULTICAST, UP ,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP qlen 1000

link/ether 52:54:00:00:04:0b brd ff:ff:ff:ff:ff:ff mac

inet 172.25.4.11/24 brd 172.25.4.255 scope global dynamic eth0 ipv4

valid\_lft 16499sec preferred\_lft 16499sec

inet6 fe80::5054:ff:fe00:40b/64 scope link ipv6

valid\_lft forever preferred\_lft forever

Aqui estan los AUTO-COMPLETADOS de bash:

ls /usr/share/bash-completion/completions/

addpart eject ibus.bash lvremove pvremove ssh vgck

blkdiscard fallocate ionice lvrename pvs su vgconvert

blkid fdformat ip lvresize pvscan sudo vgcreate

blockdev fdisk ipcrm lvs quota swaplabel vgdisplay

bzip2 find ipcs lvscan quotacheck swapon vgexport

cal findmnt iptables mcookie quotaoff systemctl vgextend

cfdisk firewall-cmd isosize mdadm quotaon systemd-analyze vgimport

chage flock journalctl mkfs raw systemd-coredumpctl vgmerge

chcpu fsck kernel-install mkfs.cramfs readprofile systemd-run vgmknodes

chfn fsck.cramfs ldattach mkfs.minix rename tailf vgreduce

chgrp fsck.minix localectl mkswap renice taskset vgremove

chown fsfreeze logger more repquota tcpdump vgrename

chpasswd fstrim loginctl mount resizepart timedatectl vgs

chrt gdbus .- look mountpoint rev udevadm vgscan

chsh getopt losetup namei rtcwake udisksctl vgsplit

col gnome-control-center lsblk nmcli runuser ul wdctl

colcrt groupadd lscpu nsenter script umount wget

colrm groupdel lsinitrd partx scriptreplay unshare whereis

column groupmod lslocks passwd semanage useradd wipefs

cpio grub lvchange ping setarch userdel write

ctrlaltdel gsettings lvcreate pivot\_root setpriv usermod xz

curl gvfs lvdisplay prlimit setquota utmpdump

dconf gzip lvextend pvchange setsebool uuidgen

delpart hexdump lvm pvcreate setsid vgcfgbackup

dmesg hostnamectl lvmdiskscan pvdisplay setterm vgcfgrestore

dracut hwclock lvreduce pvmove sfdisk vgchange

ip -s link show eth0 -- Estadisticas..pero es un SNAPSHOT !!

2: eth0: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP mode DEFAULT qlen 1000

link/ether 52:54:00:00:04:0b brd ff:ff:ff:ff:ff:ff

RX: bytes packets errors dropped overrun mcast

345570 4060 0 0 0 0

TX: bytes packets errors dropped carrier collsns

60229 444 0 0 0 0

watch : Ejecuta un programa periodicamente

watch ip -s link show eth0 -- Hace 1 bloque. .. podemos ver una evolucion del trafico!!

watch -n 3 ip -s link show eth0 -n 3 = cada 3 segundos

watch -n 1 -d ip -s link show eth0 -d = resalta lo que cambia

watch 'ip -s link show eth0 | grep -A1 RX' -- FILTRO con grep

ip route

ip r

default via 172.25.4.254 dev eth0 proto static metric 1024 -- Gateway

172.25.4.0/24 dev eth0 proto kernel scope link src 172.25.4.11 -- Ruta con 1 direccion de RED

172.25.253.254 via 172.25.4.254 dev eth0 proto static metric 1 -- Ruta con 1 direccion concreta

ip -6 route -- Rutas en formatos IPv6

unreachable ::/96 dev lo metric 1024 error -101

unreachable ::ffff:0.0.0.0/96 dev lo metric 1024 error -101

unreachable 2002:a00::/24 dev lo metric 1024 error -101

unreachable 2002:7f00::/24 dev lo metric 1024 error -101

unreachable 2002:a9fe::/32 dev lo metric 1024 error -101

unreachable 2002:ac10::/28 dev lo metric 1024 error -101

unreachable 2002:c0a8::/32 dev lo metric 1024 error -101

unreachable 2002:e000::/19 dev lo metric 1024 error -101

unreachable 3ffe:ffff::/32 dev lo metric 1024 error -101

fe80::/64 dev eth0 proto kernel metric 256

ping

En linux es eterno, en windows hace 4 iteraciones

ping -c 4 -i 3 -a -c 4 = Iteraciones -i 3 = intervalo 3 segundos -a = emite un sonido

tracepath

traceroute

sudo mtr access.redhat.com MytraceRoute : es mas agil, mas visual

server4.example.com (0.0.0.0) Fri Feb 6 04:50:44 2015

Keys: Help Display mode Restart statistics Order of fields quit

Packets Pings

Host Loss% Snt Last Avg Best Wrst StDev

1. classroom.example.com 0.0% 3 0.5 0.6 0.5 0.7 0.0

2. ???

3. 192.168.0.1 0.0% 3 2.4 2.3 1.8 2.7 0.0

4. 209.red-193-152-65.static.ccgg.telefonica.net 0.0% 3 7.0 5.0 3.1 7.0 1.7

5. ???

6. 217.Red-81-46-1.staticIP.rima-tde.net 0.0% 2 7.6 7.3 6.9 7.6 0.0

7. 153.Red-81-46-1.staticIP.rima-tde.net 0.0% 2 12.1 9.9 7.7 12.1 3.0

8. ???

9. a23-193-17-37.deploy.static.akamaitechnologies.com 0.0% 2 4.8 4.1 3.5 4.8 0.0

TECLA D = Se ven los paquetes que van perdiendo

TECLA R = Se ven los paquetes recibidos

PUERTOS y SERVICIOS

PUERTOS

< 1024 Puertos administrativos Solo root puede abrir sockets

Vienen con unos flagas del kernel

> 1024 Puertos

SOCKET : Asociacion de = direccion IP+Puerto (origen) <------> direccion IP+Puerto (destino)

-Los Puertos siempre están abiertos (OPEN) por defecto

¿COMO VEMOS LOS SOCKETs ABIERTOS?

Comando ss = Sockets Statistics

ss -ta -a= all (listening y no-listening: Established, , listen o wait) -t=TCP

State Recv-Q Send-Q Local Address:Port Peer Address:Port

LISTEN 0 100 127.0.0.1:smtp \*:\*

LISTEN 0 128 \*:sunrpc \*:\*

LISTEN 0 128 \*:55442 \*:\*

LISTEN 0 128 \*:ssh \*:\*

ESTAB 0 0 172.25.4.11:ssh 172.25.4.250:48786

LISTEN 0 100 ::1:smtp :::\*

LISTEN 0 128 :::sunrpc :::\*

LISTEN 0 128 :::57905 :::\*

LISTEN 0 128 :::ssh :::\*

ss -tan -n = numbers de PUERTO (mira en /etc/services)

LISTEN 0 100 127.0.0.1:25 \*:\*

LISTEN 0 128 \*:111 \*:\*

LISTEN 0 128 \*:55442 \*:\*

LISTEN 0 128 \*:22 \*:\*

ESTAB 0 0 172.25.4.11:22 172.25.4.250:48957

ESTAB 0 0 172.25.4.11:22 172.25.4.250:48786

ss -tulpan

Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port

tcp UNCONN 0 0 \*:68 \*:\*

tcp UNCONN 0 0 \*:111 \*:\*

tcp UNCONN 0 0 \*:123 \*:\*

tcp UNCONN 0 0 \*:5353 \*:\*

tcp UNCONN 0 0 127.0.0.1:323 \*:\*

t = tcp Protocolo TCP

u = udp Protocolo UDP

l = listening Only sockets listening

p = process Muestra el proceso usando el socket

a = all Display both listening and non-listening (for TCP this means established connections) sockets.

n = numeric No intenta resolver names

Configuring Networking wtih "nmcli"

-En RHEL7, el NETWORK MANAGER está muy mejorado y se recomienda usar

- Herramienta: nmcli

- Visualiza y gestiona la red

2 capas principales:

nmcli dev -Device Solo puede tener 1 conf. ACTIVA pero puede tener varias asignadas

nmcli con -Connection Perfil. Aplicar unos datos de red a un DEVICE

Se puede poner varios perfiles por cada WLAN a la que nos queramos conectar.

nmcli dev [status]

DEVICE TYPE STATE CONNECTION

eth0 ethernet connected System eth0(nombre del perfil)

lo loopback unmanaged --

nmcli con show -- vemos que hay 1 conexion solo (perfil)

NAME UUID TYPE DEVICE

System eth0 5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03 802-3-ethernet eth0

nmcli con show --active --Solo las activas

nmcli con show "System eth0" -- Veo las caracteristicas de un perfil (conexion)

connection.id: System eth0

connection.uuid: 5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03

connection.interface-name: eth0

connection.type: 802-3-ethernet

connection.autoconnect: yes

connection.timestamp: 1423220942

connection.read-only: no

connection.permissions:

connection.zone: --

connection.master: --

connection.slave-type: --

connection.secondaries:

connection.gateway-ping-timeout: 0

802-3-ethernet.port: --

802-3-ethernet.speed: 0

802-3-ethernet.duplex: --

802-3-ethernet.auto-negotiate: yes

802-3-ethernet.mac-address: --

802-3-ethernet.cloned-mac-address: --

802-3-ethernet.mac-address-blacklist:

802-3-ethernet.mtu: auto

802-3-ethernet.s390-subchannels:

802-3-ethernet.s390-nettype: --

802-3-ethernet.s390-options:

ipv4.method: auto

ipv4.dns:

ipv4.dns-search:

ipv4.addresses:

ipv4.routes:

ipv4.ignore-auto-routes: no

ipv4.ignore-auto-dns: no

ipv4.dhcp-client-id: --

ipv4.dhcp-send-hostname: yes

ipv4.dhcp-hostname: --

ipv4.never-default: no

ipv4.may-fail: yes

ipv6.method: ignore

ipv6.dns:

ipv6.dns-search:

ipv6.addresses:

ipv6.routes:

ipv6.ignore-auto-routes: no

ipv6.ignore-auto-dns: no

ipv6.never-default: no

ipv6.may-fail: yes

ipv6.ip6-privacy: -1 (unknown)

ipv6.dhcp-hostname: --

GENERAL.NAME: System eth0

GENERAL.UUID: 5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03

GENERAL.DEVICES: eth0

GENERAL.STATE: activated

GENERAL.DEFAULT: yes

GENERAL.DEFAULT6: no

GENERAL.VPN: no

GENERAL.ZONE: --

GENERAL.DBUS-PATH: /org/freedesktop/NetworkManager/ActiveConnection/0

GENERAL.CON-PATH: /org/freedesktop/NetworkManager/Settings/0

GENERAL.SPEC-OBJECT: --

GENERAL.MASTER-PATH: --

IP4.ADDRESS[1]: ip = 172.25.4.11/24, gw = 172.25.4.254

IP4.ROUTE[1]: dst = 172.25.253.254/32, nh = 172.25.4.254, mt = 0

IP4.DNS[1]: 172.25.254.254

IP4.DOMAIN[1]: example.com

DHCP4.OPTION[1]: requested\_domain\_search = 1

DHCP4.OPTION[2]: dhcp\_message\_type = 5

DHCP4.OPTION[3]: requested\_time\_offset = 1

DHCP4.OPTION[4]: requested\_domain\_name = 1

DHCP4.OPTION[5]: requested\_rfc3442\_classless\_static\_routes = 1

DHCP4.OPTION[6]: requested\_broadcast\_address = 1

DHCP4.OPTION[7]: requested\_classless\_static\_routes = 1

DHCP4.OPTION[8]: expiry = 1423241001

DHCP4.OPTION[9]: domain\_name = example.com

DHCP4.OPTION[10]: next\_server = 172.25.4.254

DHCP4.OPTION[11]: broadcast\_address = 172.25.4.255

DHCP4.OPTION[12]: requested\_interface\_mtu = 1

DHCP4.OPTION[13]: requested\_subnet\_mask = 1

DHCP4.OPTION[14]: dhcp\_lease\_time = 21600

DHCP4.OPTION[15]: ip\_address = 172.25.4.11

DHCP4.OPTION[16]: requested\_nis\_domain = 1

DHCP4.OPTION[17]: routers = 172.25.4.254

DHCP4.OPTION[18]: requested\_wpad = 1

DHCP4.OPTION[19]: requested\_static\_routes = 1

DHCP4.OPTION[20]: requested\_nis\_servers = 1

DHCP4.OPTION[21]: domain\_name\_servers = 172.25.254.254

DHCP4.OPTION[22]: requested\_domain\_name\_servers = 1

DHCP4.OPTION[23]: requested\_ntp\_servers = 1

DHCP4.OPTION[24]: requested\_routers = 1

DHCP4.OPTION[25]: requested\_ms\_classless\_static\_routes = 1

DHCP4.OPTION[26]: subnet\_mask = 255.255.255.0

DHCP4.OPTION[27]: requested\_host\_name = 1

DHCP4.OPTION[28]: network\_number = 172.25.4.0

DHCP4.OPTION[29]: dhcp\_server\_identifier = 172.25.253.254

IP6.ADDRESS[1]: ip = fe80::5054:ff:fe00:40b/64, gw = ::

nmcli dev show eth0 -- Veo la configuracion del device: eth0

GENERAL.DEVICE: eth0

GENERAL.TYPE: ethernet

GENERAL.HWADDR: 52:54:00:00:04:0B

GENERAL.MTU: 1500

GENERAL.STATE: 100 (connected)

GENERAL.CONNECTION: System eth0

GENERAL.CON-PATH: /org/freedesktop/NetworkManager/ActiveConnection/0

WIRED-PROPERTIES.CARRIER: on

IP4.ADDRESS[1]: ip = 172.25.4.11/24, gw = 172.25.4.254

IP4.ROUTE[1]: dst = 172.25.253.254/32, nh = 172.25.4.254, mt = 0

IP4.DNS[1]: 172.25.254.254

IP4.DOMAIN[1]: example.com

IP6.ADDRESS[1]: ip = fe80::5054:ff:fe00:40b/64, gw = ::

¿COMO CREO UNA CONEXION?

-Hay que darle parametros al "nmcli"

- nmcli : lo puede usar cualquier usuario del sistema !!

- Los perfiles que crea root son INAMOVIBLES, el resto de usarios NO.

- A los devices hay que asignarles un perfil de conexion

-- Creo una confexion conexion llamada "default"

nmcli con add con-name "default" type ethernet ifname eth0 -- no hay IP, pq la coge del DHCP

Connection 'default' (211bad52-4945-44c2-becc-98bcbed525f7) successfully added.

-- Creo una conf. conexion llamada "static"

nmcli con add con-name "static" ifname eth0 autoconnect no type ethernet ip4 172.25.4.10/24 gw4 172.25.4.254

Connection 'static' (5696f9d2-d4ed-42b1-b0e4-1b0a68afed28) successfully added

- Al hacer esto crea estos ficheros:

[root@desktop4 ~]# ll /etc/sysconfig/network-scripts/ifcfg\*

-rw-r--r--. 1 root root 277 Feb 6 12:24 /etc/sysconfig/network-scripts/ifcfg-default

-rw-r--r--. 1 root root 301 Feb 6 12:34 /etc/sysconfig/network-scripts/ifcfg-static

nmcli con up "static" 1 -- Cambio eth a una conexion estatica

Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/2)

nmcli connection show

NAME UUID TYPE DEVICE

static 5696f9d2-d4ed-42b1-b0e4-1b0a68afed28 802-3-ethernet eth0

default 211bad52-4945-44c2-becc-98bcbed525f7 802-3-ethernet --

System eth0 5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03 802-3-ethernet --

nmcli con up "default" 2-- Vuelvo a la conexion DHCP

Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)

nmcli connection show

NAME UUID TYPE DEVICE

static 5696f9d2-d4ed-42b1-b0e4-1b0a68afed28 802-3-ethernet --

default 211bad52-4945-44c2-becc-98bcbed525f7 802-3-ethernet eth0

System eth0 5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03 802-3-ethernet --

PARA MODIFICAR UNA CONEXION:

nmcli mod

nmcli connection modify default connection.interface-name eth1 -- pero ojo el device eth1 no existe !!

nmcli connection up default

Error: no device found for connection 'default' -- No existe el device eth1 !!

uuidgen -- Crea ID aleatorios

5ed85a3b-f7a4-4b34-a38a-ea55be0d5487

uuidgen

d78eeb8d-d1e8-47cf-9e4c-1e15957afd98

uuidgen

b276afdd-5d03-44cf-93cb-90328ed92772

AÑADIR/QUITAR DNS primarios / Secundarios a una conexion

nmcli connection modify static ipv4.dns 172.25.0.254 -Defino DNS

nmcli connection modify static +ipv4.dns 8.8.8.8 -Añado DNS

nmcli connection modify static -ipv4.dns 8.8.8.8 -Elimino DNS

nmcli connection show static

ipv4.dns: 172.25.0.254, 8.8.8.8

AÑADIR/QUITAR IP's VIRTUALES a una conexion

nmcli connection modify static +ipv4.addresses 10.10.10.10/8 -Añador una IP virtual

nmcli device wifi list -- Ver las conexiones WIFI

Edinting Network Configuration Files

Solo se pueden tocar ficheros cuando:

1-Nombres de devices fisicos

2-Nombres de conexiones creados por nmcli

- En RHEL7, despues de tocar los ficheros de configuracion hay que hacer:

nmcli con reload -- para que relea los ficheros de conf

DNS: Configuring Host Names and Name Resolution

Antes usabamos

hostname

¿ahora?

hostnamectl

[root@desktop4 ~]# hostname -- Nos dice el hostname de la maquina

desktop4.example.com

[root@desktop4 ~]# hostnamectl -- A parte del hostname nos dice muchas mas info

Static hostname: n/a

Transient hostname: desktop4.example.com

Icon name: computer

Chassis: n/a

Machine ID: 946cb0e817ea4adb916183df8c4fc817

Boot ID: eb05f44c6eb4411cb404b81455fa413f

Virtualization: kvm

Operating System: Red Hat Enterprise Linux Server 7.0 (Maipo)

CPE OS Name: cpe:/o:redhat:enterprise\_linux:7.0:GA:server

Kernel: Linux 3.10.0-123.el7.x86\_64

Architecture: x86\_64

¿Como cambiamos el hostname del sistema?

hostnamectl set-hostname maquina-andresss

hostname

maquina-andresss

Resolucion de nombres a 2 niveles:

1) fichero /etc/hosts

2) fichero /etc/resolv.comf -- Ojo con tocar a mano: Se usa NetworkManager (nmcli)

nameserver IP1

nameserver IP2

9-2-15

Chapter 12. Archiving ann Copying Files Between Systems

Vamos a ver como:

- Empaquetamos ficheros

- Enviamos ficheros de 1 maquina a otra

Cuotas de tamaño: Van a nivel de usuario y en base a:

- Tamaño total

- Nª de ficheros

TAR

Empaquetar ficheros/directorios:

Algoritmos de compresion:

gzip: compression standard

Algoritmo de compression sencillo

bzip2: No siempre disponible

Algoritmo de compression mas sofisticado

xz: El mejor

Algoritmo de compression mejor

Opciones del tar: SOLO 1 opcion

c create file

t test (table content )

x eXtract ficheros de un tar

p permisos (conservar )

- (leading) : no es requerido

v verbose

f siempre tiene que venir despues: el nombre del fichero (a empaquetar o desempaquetar)

OJO:

- Si ese encuentra un fichero con el mismo nombre de destino ==> MACHACA AL DES-TAREAR!!! OJO!!

CREAR un fichero TAR

tar cf archive.tar lista-ficheros-directorios

Cuando tar empaqueta: Elimina el "/" raiz = leading slash

[root@maquina-andresss ~]# tar cf /root/etc.tar /etc --Cuando ponemos una ruta absoluta elimina el / incial

tar: Removing leading `/' from member names

tar cf etc.tar /etc/shadow

tar xf etc.tar (en otra maquina desde el /) ... lo machacamos !!!!

Importante:

tar por defecto, no guarda todos los atributos de los ficheros

--xattrs Guarda CONTEXTO de SELINUX y ACLs

chattr +i /etc/resolv.conf == Convierte al fichero en INAMOVIBLE (ni root puede modificarlo)

+i = inamovible

EXTRAER ficheros TAR

tar xf archive.tar : Extrae siempre en el directorio ACTUAL

VER ficheros TAR

tar tvf archive.tar : v = Listado largo

COMPRIMIR un fichero TAR

z gzip

j bzip2

J xz

tar czf archive.tar.gz fiile1 file2 file3

tar cjf archive.tar.bz2 fiile1 file2 file3

tar cJf archive.tar.xz fiile1 file2 file3

MAGIC NUMBER = Primeros chars de la cabecera de fichero que nos dice que TIPO es

RHEL no lee en base a la extension del fichero

El comando file ===> Si nos dice el TIPO DE FICHERO (lee el magic number)

tar : puede leer fichero basados en su extension

opcion a = Lee la extension y en base a esa extension USA el algoritmo de compresion adecuado

= CREAR : mira la extension

= EXTRAER: lee el MAGIC NUMBER

tar caf archive.tar

tar xaf

SCP: Copying Files Between Systems Securily

scp LOCAL REMOTO

scp /etc/hosts student@server4 -- Se asume que va al home de student

-- Si el destino es un fichero ==> se machaca el fichero

-- Si el destino es un directorio ==> se crea el directorio

SFTP: Transfer files remotely with sftp

OJO , no es FTP!!... es un SSH TUNEL DINAMICO

Su interfaz es muy similiar al FTP

sftp desktop4

The authenticity of host 'desktop4 (172.25.4.10)' can't be established.

ECDSA key fingerprint is e0:e3:6c:90:c8:ee:88:15:d2:0a:93:e0:bf:58:e7:c5.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'desktop4,172.25.4.10' (ECDSA) to the list of known hosts.

root@desktop4's password:

Connected to desktop4.

sftp> ls -- Hacemos un ls pero estamos en remoto

sftp> put -- Es un uploading Subir un fichero de local a remoto

sftp> get -- Es un downloading Bajarse un fichero de remoto a local

RSYNC: Syncronizing Files Between Systems Securely

rsync remote syncronizacion: es como scp, copia ficheros entre 2 sistemas, pero solo copia las diferencias

es una "navaja suiza" ojo, puede hacer muchas cosas

De forma segura y eficiente. Si se corta la comunicacion, al lanzarlo reanuda lo copiado

Tambien sirver para sincros locales

sincronizacion: Tener 2 directorios en 2 maquinas distintas identicos

rsync Hace un cheksum de los diretorios LOCALES y REMOTOS y transfiere los datos faltantes

Ventaja: Si transferimos un ISO y se corta... cuando se reanuda continua donde se dejó

-n : Drive run : simulacion de lo que va a ocurrir. Ejecucion en seco

rsync tiene muchas opciones: borrar o no ficheros en origen / destino

-a Tiene muchas opciones embebidas -a = ( l + p + t + g + o + D)

En maquinas clones es UTIL... en maquinas distintas.. ojo PUEDE DAR PROBLEMAS

-l preserva links simbolicos (crea en destino el link)

-p preserva permisos

-t preserva time-stamps

-g preserva la membresia del grupo

-o preserva la membresia del owner (propietario)

-D preserva files Device (para copiar un disco entero)

-H preserva los Hard link

-h preserva los human readable

-P muestra un progreso (del total de los ficheros... no del tamaño total) (1/25)

Ej

rsync -avhP

rsync LOCAL REMOTO lo normal

rsync LOCAL LOCAL es posible tambien

rsync REMOTO REMOTO NO SE PUEDE HACER!!!

By default: contexto SELUNIX y ACLs no se transfiere con rsync

-A syncro de ACLs

-X syncro de SELinux contexts

Idea de Juan

git clone http:/pagina-web -- Nos baja a un directorio una pagina WEB completa

yum search git

Opcion interesante:

-e Le podemos decir cual es el comando de ejecucion para obtener la SHELL remota

rsync -avhP -e "ssh -o identifyFile..." -o = options del ssh

Ej:

rsync -avhP -e "ssh -o KeepAlive=yes" FicheroGRANDE.txt destop4:

chapter 13. Installing and Updating Software Packages

-RH no tiene licencias pero si subscripciones:

-Gestion de seguimientos de paquetes

-Mejoras

Debemos tener una Subscrpcion con un certificado (Entitlements). Tipos de subscripcion:

Middleware

HA de RedHat

Tendremos asi un CONJUNTO DE REPOSITORIOS, en base a esta Subscripcion

Hay que registrar el equipo

4 tareas basicas:

1- Registrar un equipo con nuestra SUSBCRIPCION

Tendremos la capacidad de enviar a RH la info de nuestro sistema

Podemos ver HW

2- Subscripcion acorde con el registro

3- Enable repositories

Una subscripcion nos puede habilitar respositorios de SW adicionales

4- Review and track

Nota:

Oracle Aplicable Linux: Es un CLON de Redhat, que apunta a sus propios repositorios de ORACLE

Redhat saca un parche y Centos, oracle, .... copia en código fuente y lo distribuyen (Gracias a la Free-Sofware-Fundation)

NOTAS IMPORTANTES:

-Hay algunas librerias que RH tiene una version ligeramente antigua

-Esto es porque RH apunta a SW maduro y no tiene la ultimisima version

-No se puede hacer una MIGRACION de librerias de Redhat hacia Centos ¿porque? porque Centos tiene librerias propias.

subscription-manager-gui como root

Hay muchos tipos de subuscripcion:

- Por ejemplo, por cada maquina fisica, podremos instalar X maquina virtuales (en f/ de RAM, sockets, cores, etcc)

REGISTRO ----> SUBSCRIPCION ----> CONTRATO

Una vez instalado, se accede a la web de RedHat:

http://www.redhat.com/subscriptions

Red Hat Subscription Management RH7

Red Hat Classic Management RH6

Aqui podriamos ver el SW, HW, de nuestro SISTEMA (maquina) SUBSCRITO

- Desde la web , podemos ver los parches CRITICOS que le faltan a nuestra maquina e incluso instalarlos.

- Incluso podemos programar un APAGADO de la maquina.

postgre DB = Es un SGBD externo

subscription-manager list --available --Veo las suscripciones

subscription-manager remove --all -- Borrar todos los entitles (suscripciones)

subscription-manager unregister -- Des-registro el sistema

cd /etc/pki

drwxr-xr-x. 6 root root 57 May 7 2014 CA

drwxr-xr-x. 4 root root 48 May 7 2014 ca-trust

drwxr-xr-x. 2 root root 6 Mar 25 2014 consumer

drwxr-xr-x. 2 root root 6 Mar 25 2014 entitlement

Aqui tengo los ficheros \*.pem

drwxr-xr-x. 2 root root 20 May 7 2014 java

drwxr-xr-x. 2 root root 97 May 7 2014 nssdb

drwxr-xr-x. 2 root root 19 May 7 2014 product

drwxr-xr-x. 2 root root 4096 May 7 2014 rpm-gpg

drwx------. 2 root root 6 Mar 26 2014 rsyslog

drwxr-xr-x. 5 root root 76 May 7 2014 tls

rct -- Displays information (headers) about or size and statistics of a entitlement, product, or identity certificate

-- used by Red Hat Subscription Manager.

Usage: rct MODULE-NAME [MODULE-OPTIONS] [--help]

Primary Modules:

cat-cert Print certificate information

cat-manifest Print manifest information

dump-manifest Dump the contents of a manifest

stat-cert Print certificate statistics and sizes

RPM - Software Package and Yum

Red Hat fue la 1ª version en distribuir Linux

Red Hat desarrolló el RPM (RedHat Package Manager)

Ofrece el codigo fuente compilado y nos los instala en el sistema

Tras RPM Debian sacó los paquetes .DEF

1 paquete RPM se compone de :

Ficheros que se instalarán en la maquina (permisos, directorios, etc)

Adicionalmente un conjunto de scripts

Informacion a cerca del paquete

Estructura de 1 paquete RPM:

NAME VERSION RELEASE ARCH

httpd-tools- 2.4.6 7.e17 x86\_64.rpm

-Con solo especifiicar el nombre del paquete, nos vale

- Version: la mayor que tenga RH

- Release: la que se adapte mejor

Un paquete RPM no resuelve DEPENDENCIAS -- Esto es un PROBLEMA!!

up2date : sistema de gestion de DEPENDENCIAS inicial de RedHat

yellowdog : 1ª distro LINUX que se instaló para un PowerPC RISC para PlayStation

RedHat adquirió este SW y lo llamó:

YUM : Yellowdog Update Manager

YUM

Repositorio : Conjunto de paqs. que ofrece un conjunto de paquetes

- Yum permite manejar paquetes RPM, los intenta instalar y analiza las depencias, formando lo que se llama: un arbol de depencias.

Hasta que no tenga todos los paquetes que le hagan faltan, no los instala.

[root@server4 ~]# yum --help

Loaded plugins: langpacks

Usage: yum [options] COMMAND

List of Commands:

check Check for problems in the rpmdb

check-update Check for available package updates

clean Remove cached data

deplist List a package's dependencies

distribution-synchronization Synchronize installed packages to the latest available versions

downgrade downgrade a package

erase Remove a package or packages from your system

fs Creates filesystem snapshots, or lists/deletes current snapshots. NUEVA en RHEL7

fssnapshot Creates filesystem snapshots, or lists/deletes current snapshots. NUEVA en RHEL7

yum repolist -- Repositorios a los que tengo acceso

Loaded plugins: langpacks

repo id repo name status

rhel\_dvd Remote classroom copy of dvd 4,305

repolist: 4,305

cd /var/cache/yum/x86\_64/7Server/rhel\_dvd/ -- Aqui hay 3 ficheros comprimidos

ll

total 3632

372d69e9829f47feb7dcec7723914ed70b3dd5a6cee2ad9fb88e3c6e47022406-primary.sqlite.bz2

4821b54c29735412a3d190a0427d07683a4ae8e61de0f237544fab418be0bc66-productid.gz

49299e96d4edd28b46448c5693ec0d21e7e921f2ef53b13d1ca6b8893ef23069-comps-Server.x86\_64.xml.gz

file 372d69e9829f47feb7dcec7723914ed70b3dd5a6cee2ad9fb88e3c6e47022406-primary.sqlite.bz2

372d69e9829f47feb7dcec7723914ed70b3dd5a6cee2ad9fb88e3c6e47022406-primary.sqlite.bz2: bzip2 compressed data, block size = 500k

bunzip2 372d69e9829f47feb7dcec7723914ed70b3dd5a6cee2ad9fb88e3c6e47022406-primary.sqlite.bz2

sqlite3 372d69e9829f47feb7dcec7723914ed70b3dd5a6cee2ad9fb88e3c6e47022406-primary.sqlite

SQLite version 3.7.17 2013-05-20 00:56:22

Enter ".help" for instructions

Enter SQL statements terminated with a ";"

sqlite> select \* from files;

Nos dan todos los ficheros

sqlite> select \* from packages;

Nos da todos los paquetes RPMs

sqlite> .q salir

------------------------------------------------------------------------------------------------------------------------------------------------------------------------

YUM usa este fichero .sqllite

yum clean all -- borra la CACHE DE YUM

-- Borra el fichero

372d69e9829f47feb7dcec7723914ed70b3dd5a6cee2ad9fb88e3c6e47022406-primary.sqlite.bz2

yum repolist -- Vuelve a descargarrse las BBDD : los 3 ficheros comprimidos

yum list yum\* -- es un globbing

Loaded plugins: langpacks

Installed Packages

yum.noarch 3.4.3-117.el7 installed

yum-langpacks.noarch 0.4.2-3.el7 @rhel\_dvd

yum-metadata-parser.x86\_64 1.1.4-10.el7 installed

yum-rhn-plugin.noarch 2.0.1-4.el7 installed

yum-utils.noarch 1.1.31-24.el7 installed

Available Packages

yum.noarch 3.4.3-118.el7 rhel\_dvd

yum-plugin-aliases.noarch 1.1.31-24.el7 rhel\_dvd

yum-plugin-changelog.noarch 1.1.31-24.el7 rhel\_dvd

yum-plugin-tmprepo.noarch 1.1.31-24.el7 rhel\_dvd

yum-plugin-verify.noarch 1.1.31-24.el7 rhel\_dvd

yum-plugin-versionlock.noarch 1.1.31-24.el7 rhel\_dvd

yum list installed -- Instalados

yum list available -- Disponibles

yum list all -- Ambos

yum grouplist -- Muestra los grupos de paquetes

yum groupinfo Virtualization Host --

Loaded plugins: langpacks

Warning: group/environment Virtualization does not exist.

Warning: group/environment Host does not exist.

[root@server4 rhel\_dvd]# yum groupinfo "Virtualization Host"

Loaded plugins: langpacks

Environment Group: Virtualization Host

Environment-Id: virtualization-host-environment

Description: Minimal virtualization host.

Mandatory Groups: -- Grupos obligatorios

base

core

+virtualization-hypervisor

+virtualization-tools

Optional Groups:

+network-file-system-client

+remote-system-management

+virtualization-platform

yum groupinfo Virtualization Virtualization\ Hypervisor -- A veces es mas facil instalar por GRUPOS

Loaded plugins: langpacks que paquete a paquete

Warning: group/environment Virtualization does not exist.

Group: Virtualization Hypervisor

Group-Id: virtualization-hypervisor

Description: Smallest possible virtualization host installation.

Mandatory Packages:

+libvirt

qemu-kvm

Optional Packages:

qemu-kvm-tools

OJO: En los RPMs puede haber script maliciosos

RedHat no soporta RPMs Third Part - EXTERNOS --- OJO !!!

Aunque leamos la cabecera, no fiarse

Ojo con los ficheros que vengan deroot con el SUID activado

10-2-15

YUM

SEMANTICA: ACID

Atomicidad

Consistencia

Isolation (aislamiento)

Durabilidad

yum --help

operaciones comunes

Opciones (Relativas a plugin)

yum list { nombre | lista\_paquetes }

-Lista los paquetes disponibles en los repositorios para instalarlos en el sistema.

-Tanto INSTALLED como en tods los REPOSITORIOS

yum list httpd

yum list httpd\\* -- globing. mejor

yum list \\*httpd\\* -- que contenga el literal "httpd"

yum list httpd\* -- Ojo que si tenemos un fichero en el dir local saldrá

yum list installed -- PAQ instalados

yum list available -- PAQ disponibles en nuestro Repositorio

yum list all

-Yum descarga de la BBDD sqllite, con los siguientes campos:

Nombre los PAQ

Ficheros de cada PAQ

Info de cada paq

yum search

- Busca una cadena de texto en todos los campos de Yum (mirar arriba)

- Para estas querys puede hacerlo cualquier usuario en principio (siempre que tenga permisos)

A veces sabemos un fichero, pero ... NO SABEMOS que PAQ lo instala... ¿Como averiguamos el paquete?

yum provides Fichero

yum provides /var/http

yum provides /bin/pv\*

yum install paq / lista\_paq - Instala un PAQ o una lista de PAQs

yum install gcc-gfortran (como root)

- Se baja la info del paquete

- Intenta resolver dependencias

yum install vsftpd

Loaded plugins: langpacks

rhel\_dvd | 4.1 kB 00:00

Resolving Dependencies

--> Running transaction check

---> Package vsftpd.x86\_64 0:3.0.2-9.el7 will be installed

--> Finished Dependency Resolution

Dependencies Resolved dependencias:

================================================================================

Package Arch Version Repository Size

================================================================================

Installing:

vsftpd x86\_64 3.0.2-9.el7 rhel\_dvd 166 k

Transaction Summary

================================================================================

Install 1 Package

Total download size: 166 k

Installed size: 343 k

Is this ok [y/d/N]: y

Downloading packages:

vsftpd-3.0.2-9.el7.x86\_64.rpm | 166 kB 00:00:00

Running transaction check

Running transaction test

Transaction test succeeded

Running transaction

Installing : vsftpd-3.0.2-9.el7.x86\_64 1/1

Verifying : vsftpd-3.0.2-9.el7.x86\_64 1/1

Installed:

vsftpd.x86\_64 0:3.0.2-9.el7

Complete!

yum install vsftpd -- Si intento RE-INSTALAR nos dice que ya existe la ultima version

Loaded plugins: langpacks

Package vsftpd-3.0.2-9.el7.x86\_64 already installed and latest version

Nothing to do

- SE PUEDE HACER UN DOWNGRADE a un paquete

Hay que mirar bien las dependencias

Usar la opcion OBSOLETE

KERNEL

- EL PAQUETE DEL KERNEL se instala con yum install pero las actualizaciones NO

yum update == yum upgrade

yum update -- Tratará de instalar todos los paquetes mas recientes !!

yum upgrade -- Tratará de instalar todos los paquetes mas recientes !!

(update y upgrade hacen lo mismo)

yum update vsftp -- Si le ponemos un paquete solo mirará para ese PAQ

yum update yum -- acutalizo el propio yum !!

-Desinstala todos los paquete del PAQ antiguo e instala los ficheros del PAQ nuevo

- Deja intactos los fichero de config antiguos y

y crea otros fichero de configuracion \*..rpm.new

yum remove vsftpd --Borrar un paquete

-- Borrar un paquete

-- Los ficheros de configuracion PERMANECEN con la extension \*.rpm.save

- Cuando borramos un paquete y RHEL encuentra DEPENDENCIAS:

-Los paquetes padres ==>NO SE BORRAN

-Los paquetes hijos (los dependendientes) ==> SI SE BORRAN OJO !!

YUM GROUP -- GRUPOS DE PAQUETES

yum group

yum group list -- Lista los grupos disponibles (instalados o no)

yum group install -- Instalará un grupo de PAQ

yum group info -- Dará

yum group list

Loaded plugins: langpacks

Installed environment groups:

Server with GUI

Available environment groups: -- Grupos de Grupos

Minimal Install

Infrastructure Server

File and Print Server

Basic Web Server

Virtualization Host

Available Groups: -- Grupos directos

Compatibility Libraries

Console Internet Tools

Development Tools

Graphical Administration Tools

Legacy UNIX Compatibility

Scientific Support

Security Tools

Smart Card Support

System Administration Tools

System Management

Done

yum group info "Web Server"

Loaded plugins: langpacks

Group: Web Server

Group-Id: web-server

Description: Allows the system to act as a web server, and run Perl and Python web applications.

Mandatory Packages: -- Paqs Obligatorios. Se instalarán

+httpd

Default Packages: -- Paqs Defaults: Se instalarán

+crypto-utils

+httpd-manual

+mod\_fcgid

+mod\_ssl

Optional Packages: -- Paqs OPTIONAL: no se instalarán, (quizas me gustaria tenerlos)

certmonger

libmemcached

memcached

mod\_auth\_kerb

mod\_nss

mod\_revocator

mod\_security

mod\_security\_crs

perl-CGI

perl-CGI-Session

python-memcached

squid

yum group info "Basic Web server"

Loaded plugins: langpacks

Environment Group: Basic Web Server

Environment-Id: web-server-environment

Description: Server for serving static and dynamic internet content.

Mandatory Groups:

base

core

+web-server -- Aqui ya vemos el webserver

Optional Groups:

+backup-client

+directory-client

guest-agents

+hardware-monitoring

+java-platform

+large-systems

+load-balancer

+mariadb-client

+network-file-system-client

+performance

+perl-web

+php

+postgresql-client

+python-web

+remote-system-management

+web-servlet

Viewing Transactions history

tail /var/log/yum.log -- Fichero de log

Dec 09 17:36:19 Installed: iwl2000-firmware-18.168.6.1-34.el7.noarch

Dec 09 17:36:20 Installed: iwl5150-firmware-8.24.2.2-34.el7.noarch

Dec 09 17:36:20 Installed: 2:mtr-0.85-7.el7.x86\_64

Dec 09 17:36:21 Installed: rfkill-0.4-9.el7.x86\_64

Dec 09 17:36:22 Installed: 1:bash-completion-2.1-6.el7.noarch

Dec 09 17:36:22 Installed: biosdevname-0.5.0-10.el7.x86\_64

Dec 09 17:36:23 Installed: mlocate-0.26-5.el7.x86\_64

Dec 09 17:36:23 Installed: words-3.0-22.el7.noarch

Feb 10 09:36:25 Installed: vsftpd-3.0.2-9.el7.x86\_64

Feb 10 09:45:50 Erased: vsftpd-3.0.2-9.el7.x86\_64

Historico de Transaccciones:

ll /var/lib/yum/history/

total 1180

drwxr-xr-x. 5 root root 30 Feb 10 09:45 2014-12-09

-rw-------. 1 root root 1179648 Feb 10 09:45 history-2014-12-09.sqlite

-rw-------. 1 root root 25280 Feb 10 09:45 history-2014-12-09.sqlite-journal

yum history -- Muestra la ultimas 50 transacciones

Loaded plugins: langpacks

ID | Login user | Date and time | Action(s) | Altered

-------------------------------------------------------------------------------

3 | root <root> | 2015-02-10 09:45 | Erase | 1

2 | root <root> | 2015-02-10 09:36 | Install | 1

1 | System <unset> | 2014-12-09 23:23 | Install | 881 EE

history list

yum history info 2 -- Info de la Transaction con ID=2

Loaded plugins: langpacks

Transaction ID : 2

Begin time : Tue Feb 10 09:36:22 2015

Begin rpmdb : 1208:ee0edcdf11792d5a32309530e21264b4b9abc650

End time : 09:36:26 2015 (4 seconds)

End rpmdb : 1209:d2998320d44014a972341020989604c2b320cd24

User : root <root>

Return-Code : Success

Command Line : install vsftpd

Transaction performed with:

Installed rpm-4.11.1-16.el7.x86\_64 installed

Installed yum-3.4.3-117.el7.noarch installed

Packages Altered:

Install vsftpd-3.0.2-9.el7.x86\_64 @rhel\_dvd -- rhel\_dvd es el repos

history info

yum history undo 2 -- Deshacer solo la transaccion=2

Loaded plugins: langpacks

Undoing transaction 2, from Tue Feb 10 09:36:22 2015

Install vsftpd-3.0.2-9.el7.x86\_64 @rhel\_dvd

No package matched to remove: vsftpd-0:3.0.2-9.el7

history undo

yum history redo 2 -- Volver a REHACER una transaccion UNDO

Loaded plugins: langpacks

Repeating transaction 2, from Tue Feb 10 09:36:22 2015

Install vsftpd-3.0.2-9.el7.x86\_64 @rhel\_dvd

Resolving Dependencies

--> Running transaction check

---> Package vsftpd.x86\_64 0:3.0.2-9.el7 will be installed

--> Finished Dependency Resolution

Dependencies Resolved

==============================================================================================================================================

Package Arch Version Repository Size

==============================================================================================================================================

Installing:

vsftpd x86\_64 3.0.2-9.el7 rhel\_dvd 166 k

Transaction Summary

==============================================================================================================================================

Install 1 Package

Total download size: 166 k

Installed size: 343 k

Is this ok [y/d/N]:

yum history

Loaded plugins: langpacks

ID | Login user | Date and time | Action(s) | Altered

-------------------------------------------------------------------------------

4 | Student User <student> | 2015-02-10 10:16 | Install | 1

3 | root <root> | 2015-02-10 09:45 | Erase | 1

2 | root <root> | 2015-02-10 09:36 | Install | 1

1 | System <unset> | 2014-12-09 23:23 | Install | 881 EE

history list

Idea: A partir de dia X.. la cosa empezó a ir mal y quiero

yum history rollback 3 -- Deshago todo hasta la transaccion ID=3

yum history packages-list vsftpd -- Si quiero saber QUE HA PASADO CON el PAQUETE vsftpd???

Loaded plugins: langpacks

ID | Action(s) | Package

-------------------------------------------------------------------------------

4 | Install | vsftpd-3.0.2-9.el7.x86\_64

3 | Erase | vsftpd-3.0.2-9.el7.x86\_64

2 | Install | vsftpd-3.0.2-9.el7.x86\_64

history packages-list

yum list yum-plugin\\*

Loaded plugins: langpacks

Available Packages

yum-plugin-aliases.noarch 1.1.31-24.el7 rhel\_dvd

yum-plugin-changelog.noarch 1.1.31-24.el7 rhel\_dvd

yum-plugin-tmprepo.noarch 1.1.31-24.el7 rhel\_dvd

yum-plugin-verify.noarch 1.1.31-24.el7 rhel\_dvd

yum-plugin-versionlock.noarch

yum install vsftpd

Loaded plugins: langpacks

Resolving Dependencies

--> Running transaction check

---> Package vsftpd.x86\_64 0:3.0.2-9.el7 will be installed

--> Finished Dependency Resolution

Dependencies Resolved

==============================================================================================================================================

Package Arch Version Repository Size

==============================================================================================================================================

Installing:

vsftpd x86\_64 3.0.2-9.el7 rhel\_dvd 166 k

Transaction Summary

==============================================================================================================================================

Install 1 Package

Total download size: 166 k

Installed size: 343 k

Is this ok [y/d/N]: d -- Download = descarga el file .rpm

Background downloading packages, then exiting:

vsftpd-3.0.2-9.el7.x86\_64.rpm | 166 kB 00:00:00

exiting because "Download Only" specified

¿DONDE LO HA DESCARGADO?

ll /var/cache/yum/x86\_64/7Server/rhel\_dvd/packages/

total 172

-rw-r--r--. 1 root root 169476 Apr 2 2014 vsftpd-3.0.2-9.el7.x86\_64.rpm

pero.. QUIERO DESCARGARLO EN OTRO SITIO "" ¿como?

yum install vsftpd --downloaddir=.

ll /tmp/packages

-rw-r--r--. 1 root root 169476 Apr 2 2014 vsftpd-3.0.2-9.el7.x86\_64.rpm

¿Que paquete instala el comando reposync?

yum provides $(which reposync)

Loaded plugins: langpacks

yum-utils-1.1.31-24.el7.noarch : Utilities based around the yum package manager

Repo : installed

Matched from:

Filename : /bin/reposync

¿COMO SYNCRONIZAMOS REPOSITORIOS?

Con el comando reposync

[root@server4 packages]# reposync --repoid=rhel\_super --download\_path=.

(1/3): pv-1.4.6-1.el7.x86\_64.rpm | 47 kB 00:00:00

(2/3): vte-0.28.2-10.el7.x86\_64.rpm | 361 kB 00:00:00

(3/3): terminator-0.97-6.el7.nux.noarch.rpm | 415 kB 00:00:00

[root@server4 packages]# ll

total 8

drwxr-xr-x. 2 root root 4096 Feb 10 11:03 rhel\_dvd

drwxr-xr-x. 2 root root 4096 Feb 10 11:03 rhel\_super

[root@server4 packages]# mv rhel\_super/ Packages

[root@server4 packages]# ll

total 8

drwxr-xr-x. 2 root root 4096 Feb 10 11:03 Packages

drwxr-xr-x. 2 root root 4096 Feb 10 11:03 rhel\_dvd

[root@server4 packages]# createrepo -v .

Spawning worker 0 with 49 pkgs

Worker 0: reading Packages/pv-1.4.6-1.el7.x86\_64.rpm

Worker 0: reading Packages/terminator-0.97-6.el7.nux.noarch.rpm

Worker 0: reading Packages/vte-0.28.2-10.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/389-ds-base-1.3.1.6-25.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/389-ds-base-libs-1.3.1.6-25.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/ElectricFence-2.2.2-39.el7.i686.rpm

Worker 0: reading rhel\_dvd/ElectricFence-2.2.2-39.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/GConf2-3.2.6-8.el7.i686.rpm

Worker 0: reading rhel\_dvd/GConf2-3.2.6-8.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/GeoIP-1.5.0-9.el7.i686.rpm

Worker 0: reading rhel\_dvd/GeoIP-1.5.0-9.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/ImageMagick-6.7.8.9-10.el7.i686.rpm

Worker 0: reading rhel\_dvd/ImageMagick-6.7.8.9-10.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/ImageMagick-c++-6.7.8.9-10.el7.i686.rpm

Worker 0: reading rhel\_dvd/ImageMagick-c++-6.7.8.9-10.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/ImageMagick-perl-6.7.8.9-10.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/ModemManager-1.1.0-6.git20130913.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/ModemManager-glib-1.1.0-6.git20130913.el7.i686.rpm

Worker 0: reading rhel\_dvd/ModemManager-glib-1.1.0-6.git20130913.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/MySQL-python-1.2.3-11.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/NetworkManager-0.9.9.1-13.git20140326.4dba720.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/NetworkManager-config-server-0.9.9.1-13.git20140326.4dba720.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/NetworkManager-glib-0.9.9.1-13.git20140326.4dba720.el7.i686.rpm

Worker 0: reading rhel\_dvd/NetworkManager-glib-0.9.9.1-13.git20140326.4dba720.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/NetworkManager-libreswan-0.9.8.0-5.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/NetworkManager-tui-0.9.9.1-13.git20140326.4dba720.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/ORBit2-2.14.19-13.el7.i686.rpm

Worker 0: reading rhel\_dvd/ORBit2-2.14.19-13.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/OpenEXR-libs-1.7.1-7.el7.i686.rpm

Worker 0: reading rhel\_dvd/OpenEXR-libs-1.7.1-7.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/OpenIPMI-2.0.19-11.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/OpenIPMI-libs-2.0.19-11.el7.i686.rpm

Worker 0: reading rhel\_dvd/OpenIPMI-libs-2.0.19-11.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/OpenIPMI-modalias-2.0.19-11.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/PackageKit-0.8.9-11.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/PackageKit-command-not-found-0.8.9-11.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/PackageKit-device-rebind-0.8.9-11.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/PackageKit-glib-0.8.9-11.el7.i686.rpm

Worker 0: reading rhel\_dvd/PackageKit-glib-0.8.9-11.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/PackageKit-gstreamer-plugin-0.8.9-11.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/PackageKit-gtk3-module-0.8.9-11.el7.i686.rpm

Worker 0: reading rhel\_dvd/PackageKit-gtk3-module-0.8.9-11.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/PackageKit-yum-0.8.9-11.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/PyGreSQL-4.0-9.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/PyPAM-0.5.0-19.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/PyQt4-4.10.1-13.el7.i686.rpm

Worker 0: reading rhel\_dvd/PyQt4-4.10.1-13.el7.x86\_64.rpm

Worker 0: reading rhel\_dvd/PyQt4-devel-4.10.1-13.el7.i686.rpm

Worker 0: reading rhel\_dvd/PyQt4-devel-4.10.1-13.el7.x86\_64.rpm

Worker 0: Error: Could not open local rpm file: /tmp/packages/./rhel\_dvd/PyQt4-devel-4.10.1-13.el7.i686.rpm: RPM Error opening Package

Worker 0: Error: Could not open local rpm file: /tmp/packages/./rhel\_dvd/PyQt4-devel-4.10.1-13.el7.x86\_64.rpm: RPM Error opening Package

Workers Finished

Failed to process 2 package(s).

[root@server4 packages]# ll

total 8

drwxr-xr-x. 2 root root 4096 Feb 10 11:03 Packages

drwxr-xr-x. 2 root root 6 Feb 10 11:04 repodata

drwxr-xr-x. 2 root root 4096 Feb 10 11:03 rhel\_dvd

yum repolist

Loaded plugins: langpacks

repo id repo name status

rhel\_dvd Remote classroom copy of dvd 4,305

rhel\_super Super Repo Aula Getafe 3

SHELL INTERACTIVA DE YUM:

yum shell

Loaded plugins: langpacks

>

yum help

--nogpgcheck disable gpg signature checking --OJO con poner esto, que nos saltamos la seguridad

yum group install "Web Server" -x httpd\_manual -- Excluye el paquete http\_manual

yum group install "Web Server" -x mod\*

--Ojo con excluir los mandatory (obligarorios)

Quiero saber los PACKAGES que hay en 1 repos particular:

yum list available --disablerepo=\* -- Disable TODOS los repos

Loaded plugins: langpacks

yum list available --disablerepo=\* --enablerepo=\*super\* -- Solo el respo = super

Loaded plugins: langpacks

Available Packages

pv.x86\_64 1.4.6-1.el7 rhel\_super

terminator.noarch 0.97-6.el7.nux rhel\_super

vte.x86\_64 0.28.2-10.el7 rhel\_super

yum --skip-broken skip packages with depsolving problems

Util para no tener en cuenta dependencias

yum --releasever=RELEASEVER

set value of $releasever in yum config and repo files

-- Podemos poner una version distinta en los repos y config files

mkir /tmp/vm1

yum group install "Minimal Install" --installroot=/tmp/vm1

-- Este comando me instala una version de RedHat minima en ese directorio

-- Luego puedo comprimirlo o hacer una ISO para que arranaque una maquina virtual

-- Tambien puedo hacer un chroot y trabajar en ese directorio

ENABLING YUM SOTFTWARE REPOSITORIES

-REPOSITORIO: Conjunto de SW y librerias

-Puede ser distribuido con diferentes protocolos:

http://

ftp://

file:// Es un protocolo especial tipo fichero

Fichero:

/etc/yum.repos.d/ \*.repo

-Yum leerá cualquier fichero con la extesion .repo

-Los repos tienen un ID local unico

cd /etc/yum.repos.d/

-rw-r--r--. 1 root root 186 Dec 9 23:22 rhel\_dvd.repo

-rw-r--r--. 1 root root 179 Feb 5 13:12 super.repo

cat rhel\_dvd.repo

# Created by cloud-init on Tue, 09 Dec 2014 22:22:59 +0000

[rhel\_dvd] -- Id Unico

gpgcheck = 0 -- Directivas

enabled = 1

baseurl = http://content.example.com/rhel7.0/x86\_64/dvd --Directiva obligatorio

name = Remote classroom copy of dvd

--------------------------------------------------------------------------------------------------------------------------------------------

DIRECTIVAS

baseurl = Tiene la ubicacion del Repos (normalmente http, ftp o file)

mirror = Puede aparecer en vez de baseurl, y apuntará a una lista de servidores

gpgcheck = 1 -- Verificacion de la integridad de las claves publicas (1=si verirfica

enabled = -- Si este repos está enable en todas las ejecuciones de yum

name = -- Descripcion mas larga

--------------------------------------------------------------------------------------------------------------------------------------------

yum repolist all -- Vemos todos los repos , tanto enables como disables

Loaded plugins: langpacks

repo id repo name status

rhel\_dvd Remote classroom copy of dvd enabled: 4,305

rhel\_super Super Repo Aula Getafe enabled: 3

repolist: 4,308

[root@server4 yum.repos.d]#

yum-config-manager --disable rhel\_super

yum repolist all

Loaded plugins: langpacks

repo id repo name status

rhel\_dvd Remote classroom copy of dvd enabled: 4,305

rhel\_super Super Repo Aula Getafe disabled

repolist: 4,305

rm -rf / etc/yum.repos.d/super.repo

yum repolist all

Loaded plugins: langpacks

repo id repo name status

rhel\_dvd Remote classroom copy of dvd enabled: 4,305

repolist: 4,305

Dentro de la empresa: hemos construido un respositorio externo

¿como hacemos? (es tipo Third Party)

yum-config-manager --add-repo="http://172.25.254.50/rhel7.0/x86\_64/super"

Loaded plugins: langpacks

adding repo from: http://172.25.254.50/rhel7.0/x86\_64/super

[172.25.254.250\_rhel7.0\_x86\_64\_super]

name=added from: http://172.25.254.250/rhel7.0/x86\_64/super

baseurl=http://172.25.254.50/rhel7.0/x86\_64/super

enabled=1

ll /etc/yum.repos.d/

total 8

-rw-r--r--. 1 root root 158 Feb 10 12:21 172.25.254.250\_rhel7.0\_x86\_64\_super.repo

yum repolist

Loaded plugins: langpacks

repo id repo name status

172.25.254.250\_rhel7.0\_x86\_64\_super added from: http://172.25.254.250/rhel7.0/x86\_64/super 3

rhel\_dvd Remote classroom copy of dvd 4,305

repolist: 4,308

EPEL

Extra Package for Enterprise Linux

https://fedoraproject.org/wiki/EPEL#How\_can\_I\_use\_these\_extra\_packages.3F

Importar la clave publica de EPEL:

https://dl.fedoraproject.org/pub/epel/RPM-GPG-KEY-EPEL-7

Examing RPM Package files

rpm

Es un comando basico

Con RPM podemos hacer queries de 2 formas:

Actuando directamente sonbre los paquetes (es la que vamos a usar)

Actuando sobre los repos

Estas 3 opciones no se deben usar:!!!!

rpm -i instalar un PAQ

rpm -U Update un PAQ

rpm -e Erase un PAQ

Para que se usa RPM?

Recordemos que un Paquete tiene:

Ficheros del paquete

Info del paquete

Scripts del paquete

rpm -q paquete -- Comprueba si el paquete esta instalado o no

rpm -q httpd

httpd-2.4.6-17.el7.x86\_64

rpm -qa -- Muestra all packages instalados

rpm -qa --last |head -- Los 10 mas recintes

httpd-2.4.6-17.el7.x86\_64 Tue 10 Feb 2015 01:00:00 PM CET

mailcap-2.1.41-2.el7.noarch Tue 10 Feb 2015 12:59:57 PM CET

httpd-tools-2.4.6-17.el7.x86\_64 Tue 10 Feb 2015 12:59:56 PM CET

apr-util-1.5.2-6.el7.x86\_64 Tue 10 Feb 2015 12:59:56 PM CET

apr-1.4.8-3.el7.x86\_64 Tue 10 Feb 2015 12:59:54 PM CET

yum-3.4.3-118.el7.noarch Tue 10 Feb 2015 12:47:50 PM CET

kernel-3.10.0-123.1.2.el7.x86\_64 Tue 10 Feb 2015 12:47:38 PM CET

gpg-pubkey-352c64e5-52ae6884 Tue 10 Feb 2015 12:38:33 PM CET

gnuplot-4.6.2-3.el7.x86\_64 Tue 10 Feb 2015 10:28:51 AM CET

gnuplot-common-4.6.2-3.el7.x86\_64 Tue 10 Feb 2015 10:28:50 AM CET

Antes de instalar un paquete == > Siempre hay que ver la procedencia

rpm -qp

rpm -qip -- query info

rpm -qlp -- query list files (muestra los ficheros que se instalaran)

rpm -qdp -- query docu

rpm -qcp -- query config files

rpm -qc -- query config

rpm -qc httpd

/etc/httpd/conf.d/autoindex.conf

/etc/httpd/conf.d/userdir.conf

/etc/httpd/conf.d/welcome.conf

/etc/httpd/conf.modules.d/00-base.conf

/etc/httpd/conf.modules.d/00-dav.conf

/etc/httpd/conf.modules.d/00-lua.conf

/etc/httpd/conf.modules.d/00-mpm.conf

/etc/httpd/conf.modules.d/00-proxy.conf

/etc/httpd/conf.modules.d/00-systemd.conf

/etc/httpd/conf.modules.d/01-cgi.conf

/etc/httpd/conf/httpd.conf

/etc/httpd/conf/magic

/etc/logrotate.d/httpd

/etc/sysconfig/htcacheclean

/etc/sysconfig/httpd

rpm -qc --changelog httpd --Cambios que ha ido teniendo elpaquete

\* Thu Mar 20 2014 Jan Kaluza <jkaluza@redhat.com> - 2.4.6-17

- mod\_dav: add security fix for CVE-2013-6438 (#1077907)

- mod\_log\_config: add security fix for CVE-2014-0098 (#1077907)

\* Wed Mar 05 2014 Joe Orton <jorton@redhat.com> - 2.4.6-16

- mod\_ssl: improve DH temp key handling (#1057687)

\* Wed Mar 05 2014 Joe Orton <jorton@redhat.com> - 2.4.6-15

- mod\_ssl: use 2048-bit RSA key with SHA-256 signature in dummy certificate (#1071276)

rpm -qc --scripts httpd -- Script de PRE y POST instalacion del paquete

preinstall scriptlet (using /bin/sh):

# Add the "apache" user

/usr/sbin/useradd -c "Apache" -u 48 \

-s /sbin/nologin -r -d /usr/share/httpd apache 2> /dev/null || :

postinstall scriptlet (using /bin/sh):

if [ $1 -eq 1 ] ; then

# Initial installation

/usr/bin/systemctl preset httpd.service htcacheclean.service >/dev/null 2>&1 || :

fi

preuninstall scriptlet (using /bin/sh):

PASAR DE RPM to CPIO

rpm2cpio

rpm2cpio pv-1.4.6-1.el7.x86\_64.rpm | cpio -tv t=test

-rwxr-xr-x 1 root root 45368 Jan 24 2014 ./usr/bin/pv

drwxr-xr-x 2 root root 0 Jan 24 2014 ./usr/share/doc/pv-1.4.6

-rw-r--r-- 1 root root 8875 May 6 2012 ./usr/share/doc/pv-1.4.6/COPYING

-rw-r--r-- 1 root root 9454 Jan 24 2014 ./usr/share/doc/pv-1.4.6/NEWS

-rw-r--r-- 1 root root 5659 Jan 24 2014 ./usr/share/doc/pv-1.4.6/README

-rw-r--r-- 1 root root 808 Dec 11 2012 ./usr/share/doc/pv-1.4.6/TODO

-rw-r--r-- 1 root root 5249 Jan 24 2014 ./usr/share/locale/de/LC\_MESSAGES/pv.mo

-rw-r--r-- 1 root root 5957 Jan 24 2014 ./usr/share/locale/fr/LC\_MESSAGES/pv.mo

-rw-r--r-- 1 root root 3977 Jan 24 2014 ./usr/share/locale/pl/LC\_MESSAGES/pv.mo

-rw-r--r-- 1 root root 4343 Jan 24 2014 ./usr/share/locale/pt/LC\_MESSAGES/pv.mo

-rw-r--r-- 1 root root 5791 Jan 24 2014 ./usr/share/man/man1/pv.1.gz

rpm2cpio pv-1.4.6-1.el7.x86\_64.rpm | cpio -imvd m=manten permisos

d=directorio

./usr/bin/pv

./usr/share/doc/pv-1.4.6

./usr/share/doc/pv-1.4.6/COPYING

./usr/share/doc/pv-1.4.6/NEWS

./usr/share/doc/pv-1.4.6/README

./usr/share/doc/pv-1.4.6/TODO

./usr/share/locale/de/LC\_MESSAGES/pv.mo

./usr/share/locale/fr/LC\_MESSAGES/pv.mo

./usr/share/locale/pl/LC\_MESSAGES/pv.mo

./usr/share/locale/pt/LC\_MESSAGES/pv.mo

./usr/share/man/man1/pv.1.gz

190 blocks

rpm2cpio pv-1.4.6-1.el7.x86\_64.rpm | cpio -imvd '\*gz' extraeme solo los que tengan \*gz\*

Chapter 14. Accesing Linux File Systems

- Vamos a ver los ficheros de tipo bloque:

- r w x r w x r w x (+)

b = block

d = directory

s = socket

p = pipe

c = char (terminal, impresora, teclado..)

l = link

- Cualquier device que reconozca el KERNEL lo va a poner en el directorio:

/dev

-Antiguamente eran:

SCSI, ATA e IDE

hd = ATA e IDE

sd = SCSI

- Hoy en dia todos aparecen referenciados como :

/dev/sd

-Todos los devices se van cargando segun un ORDEN a, b, c, d

- Los devices tipo bloque se pueden dividir en PARTICIONES

- Cada particion puede tener un type File System diferente:

Recordar: FAT : ficheros <= 4Gb

2 sistemas de PARTICIONADOS:

1. IBM Standard

Cada device en 4 PARTICIONES FISICAS

Dentro de una FISICA, podemos tener una EXTENDIDA que a su vez puede tener particiones LOGICAS

Maximo: 3 fisicas +1 extendia (11 logicas)

2. Otros

GPT : Hasta un maximos de 128 particiones

Devices Fisicos:

/dev/sda

/dev/sdb

Librerias Virt-IO : Virtualizan devices de I/O

KVM:

/dev/vda

/dev/vdb

XEN:

/dev/xvda

/dev/xvdb

Veremos LVM:

El nombrado es diferente

Usan un modulo del KERNEL llamado "Device Manager"

/dev/dm-0

/dev/dm-1

- Se crearan linsk simbolicos dentro de

/dev/mapper

FILE SYSTEMS

RHEL7 usa por defecto el file system: xfs

Ventajas:

Mayor Tamaño de ficheros

Mayor Nº de particiones

Tiene Journal

Inconveniente: No se pùede reducir

File systems:

- Pueden estar montados o no (a un directorio)

TAMAÑOS

df -- disk space file system

Filesystem 1K-blocks Used Available Use% Mounted on

/dev/vda1 10473900 4250960 6222940 41% /

devtmpfs 922268 0 922268 0% /dev

tmpfs 942660 80 942580 1% /dev/shm

tmpfs 942660 17000 925660 2% /run

tmpfs 942660 0 942660 0% /sys/fs/cgroup

df -T -T = nos dice el Tipo de File System

Filesystem Type 1K-blocks Used Available Use% Mounted on

/dev/vda1 xfs 10473900 4250960 6222940 41% /

devtmpfs devtmpfs 922268 0 922268 0% /dev

tmpfs tmpfs 942660 80 942580 1% /dev/shm

tmpfs tmpfs 942660 17000 925660 2% /run

tmpfs tmpfs 942660 0 942660 0% /sys/fs/cgroup

df -Th - Formato human-binario 1024

Filesystem Type Size Used Avail Use% Mounted on

/dev/vda1 xfs 10G 4.1G 6.0G 41% /

devtmpfs devtmpfs 901M 0 901M 0% /dev

tmpfs tmpfs 921M 80K 921M 1% /dev/shm

tmpfs tmpfs 921M 17M 904M 2% /run

tmpfs tmpfs 921M 0 921M 0% /sys/fs/cgroup

df -TH - Formato human-decimal 1000

Filesystem Type Size Used Avail Use% Mounted on

/dev/vda1 xfs 11G 4.4G 6.4G 41% /

devtmpfs devtmpfs 945M 0 945M 0% /dev

tmpfs tmpfs 966M 82k 966M 1% /dev/shm

tmpfs tmpfs 966M 18M 948M 2% /run

tmpfs tmpfs 966M 0 966M 0% /sys/fs/cgroup

Tamaños de los devices:

Formato BINARIO = KiB MiB GiB 1 K =1024 bytes

Formato DECIMAL = KB MB GB 1 K = 1000 bytes

USAGE

du directorio - Disk Usage

du $HOME

4 /home/student/.ssh

0 /home/student/.config/abrt

4 /home/student/.config/dconf

12 /home/student/.config

4 /home/student/.cache/abrt

4 /home/student/.cache

4 /home/student/.dbus/session-bus

4 /home/student/.dbus

52 /home/student

du -h $HOME -- Human format

4.0K /home/student/.ssh

0 /home/student/.config/abrt

4.0K /home/student/.config/dconf

12K /home/student/.config

4.0K /home/student/.cache/abrt

4.0K /home/student/.cache

4.0K /home/student/.dbus/session-bus

4.0K /home/student/.dbus

52K /home/student

du -h $HOME | sort -h -- Ordenar por Tamaños

0 /home/student/.config/abrt

4.0K /home/student/.cache

4.0K /home/student/.cache/abrt

4.0K /home/student/.config/dconf

4.0K /home/student/.dbus

4.0K /home/student/.dbus/session-bus

4.0K /home/student/.ssh

12K /home/student/.config

52K /home/student

PASOS genericos para usar un disco:

- El KERNEL reconozca el device

- Particionar el disco

- Montar la particion en un directorio

MONTAJE

Montaje manual:

- Solo lo puede hacer root

- Desmontarlo tambien excepto 1 caso

Montaje automatico:

- En el arranque del sistema

- Dinamico a traves de GNOME (en este caso el usuario puede desmontarlo)

¿COMO MONTAMOS?

2 formas:

- Por /dev

- Por UUID

Realmente corresponde al Filesystem

Se crea cuando se formatea, .. si lo vuelvo a formatear cambia

(- Tambien por label, pero está desaoconsejado, porque puede repetirse )

blkid = locate/print block device attributes

blkid -- Muestra info de los device tipo bloque, con sistema de ficheros

/dev/vda1: UUID="9bf6b9f7-92ad-441b-848e-0257cbb883d1" TYPE="xfs"

lsblk = list block devices

lsblk -- Muestra device tipo bloque en una estructura de arbol, los devices montados

NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT

vda 252:0 0 10G 0 disk

└─vda1 252:1 0 10G 0 part /

vdb 252:16 0 10G 0 disk

lsblk -f --fs = Output info about filesystems.

NAME FSTYPE LABEL UUID MOUNTPOINT

vda

└─vda1 xfs 9bf6b9f7-92ad-441b-848e-0257cbb883d1 /

vdb

Pasos habituales:

1-Creamos el DIRECTORIO VACIO

2-Montamos el DEVICE en el DIRECTORIO VACIO

mount DEVICE DIRECTORIO

umount DEVICE

umount DIRECTORIO

¿QUE HACEMOS SI NO NOS DEJA DES-MONTAR?

lsof - Nos muestra todos los elementos usando 1 File System

- Podemos mandarle un SIGTERM o SIGKILL en ultimo caso

Accessing removable storage Device

Se montan en:

/run /media /user /etiqueta

Device USB:

-En Linux son operaciones asincronas

sync ==> "Todas las operaciones de write pendientes ejecutalas y pasalas a disco"

Es bueno ejecutar esto ante de extraer el pen-drive

En teoria hay un demonio (udev) que vigila todos estos devices, pero a veces no va bien

Making Links Between Files

- Todo fichero tiene un ID dentro del FileSystem = I-node

[student@server4 ~]$ touch file{1,2,3}

[student@server4 ~]$ ll -i

total 0

11562 -rw-rw-r--. 1 student student 0 Feb 11 10:16 file1

2532972 -rw-rw-r--. 1 student student 0 Feb 11 10:16 file2

2532973 -rw-rw-r--. 1 student student 0 Feb 11 10:16 file3

[student@server4 ~]$ ll -lin

total 0

11562 -rw-rw-r--. 1 1000 1000 0 Feb 11 10:16 file1

2532972 -rw-rw-r--. 1 1000 1000 0 Feb 11 10:16 file2

2532973 -rw-rw-r--. 1 1000 1000 0 Feb 11 10:16 file3

- Cada File System : Tiene un nº MAXIMO de ficheros admisibles.

TABLA de I-NODES:

i-node

Metadatos

11562

File: ‘file1’

Size: 0 Blocks: 0 IO Block: 4096 regular empty file

Device: fc01h/64513d Inode: 11562 Links: 1

Access: (0664/-rw-rw-r--) Uid: ( 1000/ student) Gid: ( 1000/ student)

Context: unconfined\_u:object\_r:user\_home\_t:s0

Access: 2015-02-11 10:16:12.448644800 +0100

Modify: 2015-02-11 10:16:12.448644800 +0100

Change: 2015-02-11 10:16:12.448644800 +0100

2532972

.... file2

2532973

... file3

Los i-nodes : NO ALMACENAN LOS DATOS. Apuntan al sector del device

[student@server4 ~]$ stat file1

File: ‘file1’

Size: 0 Blocks: 0 IO Block: 4096 regular empty file

Device: fc01h/64513d Inode: 11562 Links: 1

Access: (0664/-rw-rw-r--) Uid: ( 1000/ student) Gid: ( 1000/ student)

Context: unconfined\_u:object\_r:user\_home\_t:s0

Access: 2015-02-11 10:16:12.448644800 +0100

Modify: 2015-02-11 10:16:12.448644800 +0100

Change: 2015-02-11 10:16:12.448644800 +0100

Birth: -

[student@server4 ~]$ chmod 640 file1

[student@server4 ~]$ stat file1

File: ‘file1’

Size: 0 Blocks: 0 IO Block: 4096 regular empty file

Device: fc01h/64513d Inode: 11562 Links: 1

Access: (0640/-rw-r-----) Uid: ( 1000/ student) Gid: ( 1000/ student)

Context: unconfined\_u:object\_r:user\_home\_t:s0

Access: 2015-02-11 10:16:12.448644800 +0100

Modify: 2015-02-11 10:16:12.448644800 +0100

Change: 2015-02-11 10:23:45.944644800 +0100

ll -lin /home/

total 4

12897 drwx------. 6 1000 1000 4096 Feb 11 10:16 student

TABLA DENTRY:

i-node

Directory

i-nodes contenidos

12897

(/home/student)

11562 2532972 2532973

(file1 file2 file3)

Tipos de LINKS

HARD LINK

Formato:

ln FICHERO-ORIGINAL HARD-LINK

Desventaja:

- Solo se pueden crear dentro del mismo File System

- Cuando creamos un enlace duro : se añade un nombre mas en la tabla de i-nodes

- No se pueden crear sobre directorios

Ventajas:

- No ocupan i-nodos nuevos

- chmod y chown: cambian en los dos original y harlink

- Idea:

etc/httpd : Solo root y apache pueden modificarlo

Podemos crear un hardlink: a /etc/httpd para que puedan modificarlo el resto de usuarios

El fichero se va actualizando

Pero si un usuario lo borra/modifica siempre root tendrá la copia original

[student@server4 ~]$ date > file2

[student@server4 ~]$ cat file2

Wed Feb 11 10:34:31 CET 2015

[student@server4 ~]$ ln file2 hardllink (Origen Destino)

[student@server4 ~]$ ll

total 8

-rw-r-----. 1 student student 0 Feb 11 10:16 file1

-rw-rw-r--. 2 student student 29 Feb 11 10:34 file2

-rw-rw-r--. 1 student student 0 Feb 11 10:16 file3

-rw-rw-r--. 2 student student 29 Feb 11 10:34 hardllink

[student@server4 ~]$ rm file2

[student@server4 ~]$ cat hardllink

Wed Feb 11 10:34:31 CET 2015

[student@server4 ~]$ ll

total 4

-rw-r-----. 1 student student 0 Feb 11 10:16 file1

-rw-rw-r--. 1 student student 0 Feb 11 10:16 file3

-rw-rw-r--. 1 student student 29 Feb 11 10:34 hardllink

SOFT LINK

Formato:

ln -s FICHERO-ORIGINAL LINK-SYMBOLIC

"Es un nombre apuntando a otro nombre"

- Puedo crear un hardlink apuntando a otro FILESYSTEM

Consejo:

- Cuando creemos soft link ==> Crearlos con rutas absolutas

[root@server4 ~]# pwd

/root

[root@server4 ~]# touch file1

[root@server4 ~]# ln file1 /mnt/newspace/fileHL

ln: failed to create hard link ‘/mnt/newspace/fileHL’ => ‘file1’: Invalid cross-device link

[root@server4 ~]#

[root@server4 ~]# ln -s file1 /mnt/newspace/fileSL

[root@server4 ~]# ll -i file1 /mnt/newspace/fileSL

12009704 -rw-r--r--. 1 root root 0 Feb 11 10:49 file1

131 lrwxrwxrwx. 1 root root 5 Feb 11 10:51 /mnt/newspace/fileSL -> file1

OJO:

Con borrar directorios con enlaces symbolicos poruqe podemos borrar ficheros ind

rm -rf dir2/ -- Borro todos lo que hay dentro de dir2 y dir1

mejor

rm dir2 -- Solo borro el link symbolic

LOCATE

Busca files/dir en el sistema

- Se crea una BBDD en el arranque del sistema

- Se crea cada dia

- Es mas rapido que find, pero no es 100% fiable: puedo no

locate passwd

/usr/share/man/zh\_CN/man8/chpasswd.8.gz

/usr/share/man/zh\_TW/man8/chpasswd.8.gz

/usr/share/vim/vim74/ftplugin/passwd.vim

/usr/share/vim/vim74/syntax/passwd.vim

updatebd - Actualiza la BBDD de locate

locate -i passwd -- Insensitve a mayusculas

locate passwd -n5 -- Muestra las 5 primeras que tenga la BBD

FIND

find Muestra files/dir dentro del DIRECTORIO ACTUAL

find /mnt/ -name file -- Busca un fichero por nombre

find /mnt/ -name i ---No encuentra nada !!

find /mnt/ -name '\*i\*' -- Ahopra si , por globbing

find /mnt/ -iname file -- case insensitive

find /root -user student -- Busca ficheros del user: student

find /root -group student -- Busca ficheros del grupo: student

find /root -uid 1000 -- ficheros que pertenezcan al UID=1000

find /root -perm 644 -- Por permisos

find /root -perm -004 -- Que other tenga permisos AL MENOS de read r - -

find /root -perm -005 -- Que other tenga permisos AL MENOS de read y execution r - x

find / -perm -4000 -- Que tengan AL MENOS el SUID=1

-Creamos un file de 10Mb

dd if=/dev/zero of=big\_file bs=1M count=10

find -size 10M -- Exactamente 10M

find -size -10M -- Inferior a 10M

find -size +10M -- Superior a 10M

find -atime +1 -- Fichero que se ha accedido HACE MAS DE 1 DIA

find -atime -1 -- Fichero que se ha accedido HACE MENOS DE 1 DIA

find -atime 1 -- Fichero que se ha accedido JUSTO HOY

find -mtime +1 -- Modificar

find -ctime +1 -- Cuyos permisos, nombre (METADATOS)... Status del Fichero

find -amin -- ACCESO .. MINUTOS

find -mmin -- MODIFICAR .. MINUTOS

find -cmin -- METADATOS.. MINUTOS

find -type -- Buscar por tipo de fichero

find -type f Ficheros regulares

find -type l link

find -type d directorio

find -type b tipo bloque

find -type c tipo character

find -type p pipes = tuberias

find -type s sockets

find -type f -links +1 -- Busca ficheros tipo regular y + de 1 HARD LINK

CONJUNCION DE OPCIONES

find -type f -links +1 -user root -permi --444 -- Idem user "root" y permisos al menos r-x r-x r-x

-- Es como si pusieramos un AND ... es identico a poner:

find -type f -a -links +1 -a -user root -a -permi --444

-a = AND

-o = OR

find -type l -o -user student

find \( -type f -o -user student \) -perm -400 -ls -- Agrupamos por bloques y hacemos un ls

--Poniendo ok = ejecutamos un comando sobre cada fichero encontrado.

-- Las llaves {} es el argumento (fichero).

-- NOS PREGUNTA por cada fichero

find \( -type f -o -user student \) -perm -400 -ok chown root:student {} \;

- Poniendo exec = NO PREGUNTA

find \( -type f -o -user student \) -perm -400 -exec rm {} \;

- Poniendo exec

find \( -type f -o -user student \) -perm -400 -exec rm -i {} \;

Chapter 15. Virtualized Systems

KVM : Kernel-based Virtual Machine

Capas: HW, kernel, SO, Aplicaciones

Antes habitualmente:

- Para virtualizar :necesitabamos un Hypervisor (capa encima del kernel)

- Full-Virtualization. "La MV no sabe que es una MV"

- MV y MF compiten por los recursos... se puede bloquear la Maquina FISICA (MF) !!!

Red Hat tenia 2 ramas:

1) XEN (se abandonó)

Tenia licencias privativas

Usa hypervisor

2) KVM : No necesita Hypervisor (digamos que forma parte del kernel)

Desde kernel version 2.6.2

- Es Paravirtualizacion (es mejor)

RH ofrece 3 entornos de virtualizacion:

1- Sistemas FISICOS (el entorno de clase)

2 - Entorno privado

RHEV-M Virtualizacion-Manager

Es un RedHat MODIFICADO

Tenemos:

Storage virtual compartido

Network virtual compartido

3 - Entorno Publico

OpenStack

Permite gestionar nubes publicas

4 - Nubes hibridas: Parte de las instancias en nube privadas y parte en nubes publicas

CloudForms

Requerimientos del sistema:

- Al menos 1 procesador de 1 nucelo con hyperthread

- Minimo 2 Gb de RAM anfitrion (en maquina fisica con RHEL7) + RAM de cada VM

1 Gb es reservado para el kernel.

- 6 Gb disk space para el anfitrion + space para cada VM

CPU = Tiene que tener activado el flag activado de VIRTUALIZACION

INTEL: vmx

AMD: svm

En /proc tenemos toda la info del kernel (está en RAM)

cat /proc/cpuinfo

flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pd pe1gb rdtscp lm constant\_tsc arch\_perfmon pebs bts rep\_good nopl xtopology nonstop\_tsc aperfmperf eagerfpu pni pclmulqdq dtes64 monitor ds\_cpl vmx smx est tm2 ssse3 fma cx16 xtpr pdcm pcid sse4\_1 sse4\_2 x2apic movbe popcnt tsc\_deadline\_timer aes xsave avx f16c rdrand lahf\_lm abm ida arat epb xsaveopt pln pts dtherm tpr\_shadow vnmi flexpriority ept vpid fsgsbase tsc\_adjust bmi1 hle avx2 smep bmi2 erms invpcid rtm

core id : 1

core id : 2

flag lm : Procesador de 64 bits

Para un entorno de virtualizacion de red es necesario tb el flag: nx (no execute) Restringe accesos a memorias reservadas

Ojo:

Las BIOS tienen que tener habilitado el uso de la virtualizacion

- Si la BIOS lo tiene inhabilitado

Paquetes:

qemu-kbm

qemu-img

Herramientas:

virt-manager

libvirt

libvirt-pyton

pyton-virinst

libvirt-client

ANACONDA:

Desde RHEL7: NO SE PERMITEN INSTALAR PAQUETES INDIVIDUALES , EN LA INSTALACION ESTANDARD

En la Post-instalacion SI SE PUEDE

virsh

Gestionar VMs

virsh list --all

virsh start server\_am

virt-manager

Herramienta grafica

RHEV-M

oVirt = Es el RHEL comunitario abierto Open Virtualization

http://www.ovirt.org/

¿COMO INSTALAR UNA MAQUINA VIRTUAL?

Pasos:

1. Desde Virutal Machine Manager

rht-vmctl

Error: missing subcommand or VMNAME.

This utility manages the Red Hat Training supplied VMs on the local

hypervisor.

Usage: rht-vmctl [-q|--quiet] VMCMD VMNAME

rht-vmctl -h|--help

where VMCMD is one of:

reset - poweroff, return to saved or original state, start VMNAME

view - launches console viewer of VMNAME

start - obtain and start up VMNAME

stop - stop a running VMNAME

poweroff - if running, force stop VMNAME

save - stop, backup image, start VMNAME

restore - poweroff, restore image, start VMNAME

fullreset - poweroff, reobtain from server, start VMNAME (bad save/image)

get - if not here, obtain VMNAME from server

status - display libvirt status of VMNAME

rht-vmctl stop server\_am

Stopping server\_am..................

Powering off server\_am..

Despues de instalar en primer reinicio:

FIRST BOOT

Podemos crear 1

Aceptamos EULA