Comandos útiles

Autores: Emiliano López (emiliano.lopez@gmail.com)
Maximiliano Boscovich (maximiliano@boscovich.com.ar)
Fecha: 23/05/2018 17:08

Vagrant

Vagrant nos permite gestionar máquinas virtuales de un modo muy cómodo. A continuación algunos de los comandos más usados:

```
vagrant up      # levanta la vm
vagrant reload  # recargar la vm
vagrant halt    # apaga la vm
vagrant ssh     # sesión ssh a la vm
vagrant destroy # elimina la vm
```

Para que inicie la máquina virtual en modo gráfico se debe especificar en el Vagrantfile la opción `vb.gui = true`.

ACTIVIDAD 0.1: Pruebe los comandos anteriores parado en el directorio donde se encuentra el archivo Vagrantfile provisto.

Redes

El amado `ifconfig` y el entrañable `route` han sido deprecados, ahora se utiliza el comando `ip`.

El querido `netstat` también se esfumó y ahora usamos `ss` (socket statistics).

Los nombres `ethX` también desaparecieron por los fácilmente memorizables `esp02n0x`.

Los nostálgicos aun pueden hacer uso de estas herramientas instalando el paquete `net-tools`.

Nombres de las interfaces

`ls /sys/class/net`

- en01, en02, … andem1, em2,

Firmware-numbered interfaces embedded on the motherboard.

- ens1, ens2, …

Firmware-numbered PCIe hotplug interfaces.

- enp2s0

At PCI bus address 02:00.0.

- p7p1

A card plugged into PCIe slot #7.

ACTIVIDAD 0.2: Examine con el comando `ls` todas las interfaces de red disponibles.

Servicio de red

Si bien sigue funcionando `/etc/init.d/network restart` es conveniente usar `systemctl` para consultar su estado, iniciar, detener o reiniciar un servicio del siguiente modo:

```
systemctl [status|stop|start|restart] network.service
```

ACTIVIDAD 0.3: Pruebe reiniciar la red, y luego verifique el estado de la misma utilizando `systemctl`. ¿Qué información del estado se muestra?.

Direcciones estáticas

Para una interfaz de red que se denomine `enp0s3` la configuración se encuentra en `# /etc/sysconfig/network-scripts/ifcfg-enp0s3`. Por ejemplo:

```
DEVICE="enp0s3"
BOOTPROTO=static
ONBOOT=yes
TYPE="Ethernet"
IPADDR=192.168.20.60
NAME="System enp0s3"
HWADDR=00:0C:29:28:FD:4C
GATEWAY=192.168.20.1
```

ACTIVIDAD 0.4: Examine el directorio `/etc/sysconfig/network-scripts` y comente que se encuentra dentro del mismo.

ip

Se puede encontrar una comparación entre los comando útiles de ifconfig y ip en https://p5r.uk/blog/2010/ifconfig-ip-comparison.html.

Veamos los más usuales:

```
ip addr add 192.168.50.5 dev eth1       # agregar ip
ip addr show                            # mostrar ip
ip addr del 192.168.50.5/24 dev eth1    # borrar ip
ip link set eth1 up                     # habilitar iface
ip link set eth1 down                   # deshabilitar iface
```

Algunos para rutas:

```
ip route show # muestra ruta
ip route add 10.10.20.0/24 via 192.168.50.100 dev eth0  # agrega ruta
ip route del 10.10.20.0/24                              # borra ruta
ip route add default via 192.168.50.100                 # default gateway
```

Para agregar una ruta estática en forma permanente se debe modificar `/etc/sysconfig/network-scripts/route-eth0` agregándola del siguiente modo:

```
10.10.20.0/24 via 192.168.50.100 dev eth0
```

ACTIVIDAD 0.5: Pruebe agregar una ruta estática de manera temporal, utilizando el comando `ip`. Verifique su creación y luego elimínela. Ahora prueba agregar la misma ruta pero de forma permanente, reinicie la máquina virtual y verifique que la misma se encuentre definida.

Interfaces virtuales

Con el ya casi obsoleto comando `ifconfig` se creaba una interfaz virtual asociada a una real (física) haciendo `ifconfig eth0:0 192.168.1.2 netmask 255.255.255.0 up`. El número luego de los dos puntos la identificaba, y el nombre previo era la placa física a la que estaba asociada.

Con el comando ip, se asocia una nueva dirección ip a un dispositivo de red haciendo

`ip address add [ip]/[mask] dev [nic] label [nic]:[name]`, donde *[ip]/[mask]* hace referencia a la dirección ip y a la máscara de red, *nic* al nombre del dispositivo físico y *[name]* al nombre de interfaz virtual, que en general suele ser un número aunque no está limitado a ello. En el siguiente ejemplo creamos una interfaz virtual asociada a la placa inalámbrica wlp2s:

```
ip address add 10.10.10.47/24 dev wlp2s0 label wlp2s0:1
```

Con lo precedente se agregan ips en forma temporal, si es necesario hacer el cambio permanente se deben crear tantos archivos como interfaces virtuales se requieran en `/etc/sysconfig/network-scripts`, usando la nomeclatura `ifcfg-[nic]:[name]`, donde *[nic]* es el nombre de la interfaz física y *[name]* el número de la interfaz alias.

Por ejemplo, el archivo `/etc/sysconfig/network-scripts/ifcfg-enp0s3:1` tendría algo similar a lo siguiente:

```
DEVICE="enp0s3:1"
BOOTPROTO=static
ONBOOT=yes
TYPE="Ethernet"
IPADDR=10.10.10.66
NETMASK=255.255.255.0
HWADDR=00:0C:29:28:FD:CC
GATEWAY=10.10.10.1
```

Finalmente reiniciar el servicio de red: `systemctl restart network`

SS

```
ss              # lista todas las conexiones establecidas (tcp/udp/unix)
ss -[tux]       # t tcp, u udp, x unix establecidos
ss -ta          # sockets tcp establecidos y escuchando
ss -tan         # muestra números de puertos e ips en vez de nombres
ss -ltn         # solo escuchando, tcp, números
ss -ltnp        # procesos que abrieron los sockets (sudo)
```

Es interesante utilizar el filtrado basado en direcciones y puertos. Por ejemplo para mostrar todas las conexiones cuyo puerto de origen o destino sean ssh:

`ss -at '( dport = :ssh or sport = :ssh )'`

U otro ejemplo donde el número de puerto destino es el 80 o 443:

`ss -nt '( dst :443 or dst :80 )'`

Combinado con el comando watch es posible ver en tiempo real las conexiones que se establecen bajo el filtrado previo. Por ejemplo, para ver en tiempo real con un intervalo de 1 segundo el filtrado previo:

`watch -n1 "ss -nt '( dst :443 or dst :80 )'"`

ACTIVIDAD 0.6: Deje corriendo el comando watch junto a ss, para que muestre las conexiones SSH, y pídale a su compañero que desde su equipo se conecte vía ssh al suyo para verificar como se muestran las conexiones (estado, origen, etc).

dhclient

La bandera `-r` explicitamente libera la asociación actual, por ejemplo:

```
$ sudo dhclient -r
```

Ahora obtenemos una nueva IP:

```
$ sudo dhclient
```

¿Cómo lo renovamos para una interfaz específica, digamos, eth0?

```
$ sudo dhclient -r eth0
$ sudo dhclient eth0
```

Firewalld

Firewalld es un frontend para iptables que viene por defecto a partir de CentOS 7.

```
systemctl [disable|stop|start|status] firewalld
firewall-cmd --state                                # ver estado
```

Administrar servicios

Systemd es un administrador de sistema y servicios para los sistemas operativos Linux. Está diseñado para mantener compatibilidad con los scripts init de SysV.

Systemd introduce el concepto de *unidades* que son representadas por archivos de configuración almacenados en

- `/usr/lib/systemd/system/` creados con la instalación de paquetes RPM
- `/run/systemd/system/` creados en tiempo de ejecución
- `/etc/systemd/system/` creados por `systemctl enable`

que encapsulan información sobre los servicios del sistema, sockets, etc. Para una lista completa sobre los tipos de unidades de systemd vea la Tabla 9.1 "Available systemd Unit Types" (p.99) del *Red Hat Enterprise Linux 7 System Administrator's Guide*.

En versiones previas se utilizaban los scripts *init* que se almacenaban en `/etc/rc.d/init.d` y generalmente eran escritos en Bash y permitian al administrador controlar el estado de los servicios y demonios en el sistema. Bien, ahora estos script han sido reemplazados con los *service units*.

Estos *service units* finalizan con la extensión **.service**. A continuación un resumen de su uso mas frecuente:

```
systemctl [start|stop|restart|status] name.service
systemctl reload name.service
systemctl [enable|disable|is-enabled] name.service

# Displays the status of all services.
systemctl list-units --type service --all

# Lists all services and checks if they are enabled
systemctl list-unit-files --type service
```

Para más detalles se recomienda la lectura de *CHAPTER 9. MANAGING SERVICES WITH SYSTEMD* de *Red Hat Enterprise Linux 7 System Administrator's Guide*.

Modos de inicio

Al instalar GNOME o KDE el nivel de ejecución por defecto sigue siendo el modo consola, para cambiar este comportamiento y que automáticamente ingrese al entorno gráfico es necesario hacer:

```
systemctl set-default graphical.target
```

Antes de systemd se modificaba en `/etc/inittab` el nivel de ejecución, ahora se denominan `targets` y se utiliza el comando previo con dos opciones:

- multi-user.target
- graphical.target

Para saber el target en el que se encuentra basta con ejecutar `systemctl get-default`

Al setear un target por defecto lo que se hace es crear un enlace simbólico en `/etc/systemd/system/default.target` apuntando a `graphical.target` o `multi-user.target` en /usr/lib/systemd/system/

Proxy

Con el fin de economizar tráfico frecuentemente se accede a una red a través de un servidor proxy. Muchos de los comandos que realizamos en el sistema pueden ser redireccionados a través de un proxy con solo configurar la variable de entorno `http_proxy` y `https_proxy`.

Esto se realiza haciendo uso del comando `export` del siguiente modo:

```
$export http_proxy="http://PROXY:PUERTO"
$export https_proxy="http://PROXY:PUERTO"
```

Se debe tener en cuenta que esto se mantiene siempre y cuando persista el usuario en la misma terminal. Si se desea realizar una acción con permisos de `sudo` entonces primero debe pasarse a administrador con `sudo -s` y finalmente realizar el `export`.

Si se desea habilitar el proxy para YUM en forma permanente entonces se debe modificar el archivo `/etc/yum.conf` agregando una linea que contenga `proxy=http://PROXY:PUERTO`. Para conocer todas las opciones de configuración ver `man yum.conf`.

En los labs de la UTN FRSF el proxy es `frsf.utn.edu.ar` y el puerto `8080`.

Acceso a los logs con journalctl

Desde que se implementó systemd, el acceso a los logs ha cambiado. Ahora cada proceso, servicio o el mismo kernel, generan lo que se conocen como journals (diarios), y estos pueden ser accedidos de manera centralizada por medio de la herramienta `journalctl`.

Veamos algunas opciones disponibles:

- Ver todos los logs

```
[root@localhost ~]# journalctl -f
-- Logs begin at Sat 2018-03-24 09:12:29 -03, end at Tue 2018-05-08 22:55:06 -03. --
mar 24 09:12:29 tesla kernel: random: get_random_bytes called from start_kernel+0x42/0x4
```

```
mar 24 09:12:29 tesla kernel: Linux version 4.13.0-37-generic (buildd@lcy01-amd64-026) (
u 7.2.0-8ubuntu3.2)) #42-Ubuntu SMP Wed Mar 7 14:13:23 UTC 2018 (Ubuntu 4.13.0-37.42-gen
mar 24 09:12:29 tesla kernel: Command line: BOOT_IMAGE=/@/boot/vmlinuz-4.13.0-37-generic
-4cae-a48b-26bcbbb4f871 ro rootflags=subvol=@ quiet splash vt.handoff=7
mar 24 09:12:29 tesla kernel: KERNEL supported cpus:
mar 24 09:12:29 tesla kernel:   Intel GenuineIntel
mar 24 09:12:29 tesla kernel:   AMD AuthenticAMD
mar 24 09:12:29 tesla kernel:   Centaur CentaurHauls
mar 24 09:12:29 tesla kernel: x86/fpu: Supporting XSAVE
```

- Ver logs en vivo (similar a tail -f)

```
[root@localhost ~]# journalctl -f
-- Logs begin at mar 2018-05-08 22:50:21 -03. --
may 08 22:53:42 localhost.localdomain systemd[1]: Created slice User Slice of vagrant.
may 08 22:53:42 localhost.localdomain systemd[1]: Starting User Slice of vagrant.
may 08 22:53:42 localhost.localdomain systemd[1]: Started Session 2 of user vagrant.
may 08 22:53:42 localhost.localdomain systemd-logind[632]: New session 2 of user vagrant
may 08 22:53:42 localhost.localdomain systemd[1]: Starting Session 2 of user vagrant.
may 08 22:53:42 localhost.localdomain sshd[3116]: pam_unix(sshd:session): session opened
may 08 22:53:52 localhost.localdomain sudo[3139]:  vagrant : TTY=pts/0 ; PWD=/home/vagra
may 08 22:53:52 localhost.localdomain su[3140]: (to root) vagrant on pts/0
may 08 22:53:52 localhost.localdomain su[3140]: pam_unix(su-l:session): session opened f
may 08 22:54:02 localhost.localdomain chronyd[641]: Selected source 190.228.30.178
```

- Ver solo los logs del kernel

```
[root@localhost ~]# journalctl -k
-- Logs begin at Sat 2018-03-24 09:12:29 -03, end at Tue 2018-05-08 23:05:10 -03. --
may 08 22:02:41 tesla kernel: Linux version 4.15.0-20-generic (buildd@lgw01-amd64-039) (
may 08 22:02:41 tesla kernel: Command line: BOOT_IMAGE=/@/boot/vmlinuz-4.15.0-20-generic
may 08 22:02:41 tesla kernel: KERNEL supported cpus:
may 08 22:02:41 tesla kernel:   Intel GenuineIntel
may 08 22:02:41 tesla kernel:   AMD AuthenticAMD
may 08 22:02:41 tesla kernel:   Centaur CentaurHauls
may 08 22:02:41 tesla kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating poi
may 08 22:02:41 tesla kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
may 08 22:02:41 tesla kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
may 08 22:02:41 tesla kernel: x86/fpu: Supporting XSAVE feature 0x008: 'MPX bounds regis
may 08 22:02:41 tesla kernel: x86/fpu: Supporting XSAVE feature 0x010: 'MPX CSR'
```

- Para ver los logs desde el último booteo

```
[root@localhost ~]# journalctl -b
-- Logs begin at mar 2018-05-08 22:50:21 -03, end at mar 2018-05-08 23:06:06 -03. --
may 08 22:50:21 localhost.localdomain systemd-journal[86]: Runtime journal is using 6.2M
may 08 22:50:21 localhost.localdomain kernel: Initializing cgroup subsys cpuset
may 08 22:50:21 localhost.localdomain kernel: Initializing cgroup subsys cpu
may 08 22:50:21 localhost.localdomain kernel: Initializing cgroup subsys cpuacct
may 08 22:50:21 localhost.localdomain kernel: Linux version 3.10.0-693.21.1.el7.x86_64 (
```

```
may 08 22:50:21 localhost.localdomain kernel: Command line: BOOT_IMAGE=/vmlinuz-3.10.0-6
may 08 22:50:21 localhost.localdomain kernel: e820: BIOS-provided physical RAM map:
```

```
root@tesla:~# journalctl -b -3
-- Logs begin at Sat 2018-03-24 09:12:29 -03, end at Tue 2018-05-08 23:39:17 -03
may 06 07:36:12 tesla kernel: Linux version 4.15.0-20-generic (buildd@lgw01-amd6
may 06 07:36:12 tesla kernel: Command line: BOOT_IMAGE=/@/boot/vmlinuz-4.15.0-20
may 06 07:36:12 tesla kernel: KERNEL supported cpus:
may 06 07:36:12 tesla kernel:   Intel GenuineIntel
may 06 07:36:12 tesla kernel:   AMD AuthenticAMD
may 06 07:36:12 tesla kernel:   Centaur CentaurHauls
may 06 07:36:12 tesla kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floa
may 06 07:36:12 tesla kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE regi
may 06 07:36:12 tesla kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX regi
may 06 07:36:12 tesla kernel: x86/fpu: Supporting XSAVE feature 0x008: 'MPX boun
may 06 07:36:12 tesla kernel: x86/fpu: Supporting XSAVE feature 0x010: 'MPX CSR'
may 06 07:36:12 tesla kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:
may 06 07:36:12 tesla kernel: x86/fpu: xstate_offset
```

- Si queremos ver los últimos 15 mensajes

```
root@tesla:~# journalctl -n 15
-- Logs begin at Sat 2018-03-24 09:12:29 -03, end at Tue 2018-05-08 23:39:25 -03
may 08 23:39:17 tesla systemd[7707]: Starting D-Bus User Message Bus Socket.
may 08 23:39:17 tesla systemd[7707]: Listening on GnuPG cryptographic agent (ssh
may 08 23:39:17 tesla systemd[7707]: Listening on GnuPG network certificate mana
may 08 23:39:17 tesla systemd[7707]: Reached target Timers.
may 08 23:39:17 tesla systemd[7707]: Listening on GnuPG cryptographic agent and
may 08 23:39:17 tesla systemd[7707]: Reached target Paths.
may 08 23:39:17 tesla systemd[7707]: Listening on GnuPG cryptographic agent and
may 08 23:39:17 tesla systemd[7707]: Listening on GnuPG cryptographic agent and
may 08 23:39:17 tesla systemd[7707]: Listening on D-Bus User Message Bus Socket.
may 08 23:39:17 tesla systemd[7707]: Reached target Sockets.
may 08 23:39:17 tesla systemd[7707]: Reached target Basic System.
may 08 23:39:17 tesla systemd[7707]: Reached target Default.
may 08 23:39:17 tesla systemd[7707]: Startup finished in 167ms.
may 08 23:39:17 tesla systemd[1]: Started User Manager for UID 0.
```

- Ver los logs de los últimos 10 minutos

```
root@tesla:~# journalctl --since -15m
-- Logs begin at Sat 2018-03-24 09:12:29 -03, end at Tue 2018-05-08 23:40:33 -03
may 08 23:32:16 tesla pkexec[7507]: pam_unix(polkit-1:session): session opened f
may 08 23:32:16 tesla pkexec[7507]: mboscovich: Executing command [USER=root] [T
may 08 23:32:44 tesla smartd[1046]: Device: /dev/sda [SAT], SMART Usage Attribut
may 08 23:32:44 tesla smartd[1046]: Device: /dev/sda [SAT], SMART Usage Attribut
may 08 23:32:44 tesla smartd[1046]: Device: /dev/sdb [SAT], SMART Usage Attribut
may 08 23:33:02 tesla gnome-shell[2233]: Object .Gjs_AppIndicatorIconActor__1 (0
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: == Stack trace for context
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #0 0x7ffe62973740 I   resou
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #1 0x56139ea7c220 i   /usr/
```

```
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #2 0x7ffe62974340 I   resou
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #3 0x7ffe62974400 b   self-
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #4 0x7ffe629744f0 b   resou
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #5 0x56139ea7c198 i   /usr/
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #6 0x7ffe62975160 I   resou
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #7 0x56139ea7c0f0 i   /usr/
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #8 0x7ffe62975d60 I   resou
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #9 0x56139ea7c078 i   /usr/
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #10 0x56139ea7bfb8 i   reso
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #11 0x56139ea7bf38 i   reso
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #12 0x7ffe62976a80 b   self
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #13 0x56139ea7beb8 i   reso
```

- Ver los logs desde una fecha particular

```
root@tesla:~# journalctl --since='2018-05-08 23:30'
-- Logs begin at Sat 2018-03-24 09:12:29 -03, end at Tue 2018-05-08 23:41:35 -03. --
may 08 23:32:16 tesla pkexec[7507]: pam_unix(polkit-1:session): session opened for user
may 08 23:32:16 tesla pkexec[7507]: mboscovich: Executing command [USER=root] [TTY=unkno
may 08 23:32:44 tesla smartd[1046]: Device: /dev/sda [SAT], SMART Usage Attribute: 190 A
may 08 23:32:44 tesla smartd[1046]: Device: /dev/sda [SAT], SMART Usage Attribute: 194 T
may 08 23:32:44 tesla smartd[1046]: Device: /dev/sdb [SAT], SMART Usage Attribute: 194 T
may 08 23:33:02 tesla gnome-shell[2233]: Object .Gjs_AppIndicatorIconActor__1 (0x5613a0f
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: == Stack trace for context 0x56139e
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #0 0x7ffe62973740 I   resource:///o
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #1 0x56139ea7c220 i   /usr/share/gn
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #2 0x7ffe62974340 I   resource:///o
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #3 0x7ffe62974400 b   self-hosted:9
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #4 0x7ffe629744f0 b   resource:///o
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #5 0x56139ea7c198 i   /usr/share/gn
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #6 0x7ffe62975160 I   resource:///o
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #7 0x56139ea7c0f0 i   /usr/share/gn
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #8 0x7ffe62975d60 I   resource:///o
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #9 0x56139ea7c078 i   /usr/share/gn
may 08 23:33:02 tesla org.gnome.Shell.desktop[2233]: #10 0x56139ea7bfb8 i   resource:///
```

Referencias

- *Red Hat Enterprise Linux 7 System Administrator's Guide*, 2014. D. Brien.