Contents

1 Enterprise Linux 7 (RedHat, CentOS)

Last Modified: 2015-01-20 16:12:38

Command cheat sheet for EL7. For every action, I try to give the ‘canonical’ command, as recommended by RedHat. That means using `systemd`, NetworkManager, `journald`, etc.

1.1 Network configuration

Action	Command
List interfaces (and IP addresses)	`ip address`, `ip a`
Route table	`ip route`, `ip r`
DNS servers	`cat /etc/resolv.conf`
Set IP address of an interface*	`ip address add 192.168.56.1/24 dev vboxnet0`

(*) This example is actually a workaround for a bug that causes NetworkManager 0.9.9 to manage virtual network interfaces.

1.1.1 NetworkManager

Action	Command
Show available network connection profiles	`nmcli connection show`
Show active network connection profiles	`nmcli connection show active`
Show network device status	`nmcli device status`
Connect to profile CONNECTION	`nmcli connection up id CONNECTION`
Disconnect profile CONNECTION	`nmcli connection down id CONNECTION`
Query Wifi status	`nmcli radio wifi`
Turn Wifi on/off	`nmcli radio wifi {on,off}`
List available wireless networks	`nmcli device wifi list`
Refresh list of wireless networks	`nmcli device wifi rescan`

Action	Command
Connect to wireless network SSID	`nmcli device wifi connect SSID`

`connection` and `device` can be abbreviated to `con` and `dev`, respectively.

1.1.2 Host name

There are *three* kinds of host names:

- Static: “traditional” host name, stored in `/etc/hostname`
- Transient: dynamic, set in kernel. Default value is the static host name, can be set by e.g. DHCP or mDNS.
- Pretty: free form, for presentation to the user. Default value is the static host name.

Action	Command
Get hosti names	`hostnamectl`
Set (all) host names	`hostnamectl set-hostname HOSTNAME`
Set specific host name	`hostnamectl set-hostname --static HOSTNAME`
	`hostnamectl set-hostname --transient HOSTNAME`
	`hostnamectl set-hostname --pretty HOSTNAME`

1.1.3 Resources

- RedHat Enterprise Linux 7 Networking Guide
- Fedora Wiki: Networking/CLI
- RHEL 7: How to get started with Systemd, at certdepot.net

1.2 Managing services with `systemctl`

Action	Command
List services	`systemctl list-units --type service`
Query SERVICE status	`sudo systemctl status SERVICE.service`
List failed services on boot	`sudo systemctl --failed`
Start SERVICE	`sudo systemctl start SERVICE.service`
Stop SERVICE	`sudo systemctl stop SERVICE.service`
Restart SERVICE	`sudo systemctl restart SERVICE.service`
Kill SERVICE (all processes) with SIGTERM	`sudo systemctl kill SERVICE.service`
Kill SERVICE (all processes) with SIGKILL	`sudo systemctl kill -s SIGKILL SERVICE.service`
Start SERVICE on boot	`sudo systemctl enable SERVICE.service`
Don’t start SERVICE on boot	`sudo systemctl disable SERVICE.service`

1.3 Runlevels

Run with root privileges (`sudo`)

Action	Command
Go to single user mode	`systemctl rescue`
Go to multi-user mode	`systemctl isolate multi-user.target`
(= old runlevel 3)	`systemctl isolate runlevel3.target`

Action	Command
Go to graphical level	`systemctl isolate graphical.target`
Get default runlevel	`systemctl get-default`
Set default runlevel	`systemctl set-default graphical.target`
Shutdown	`systemctl poweroff`
Reboot, suspend, hibernate	`systemctl STATE`

1.3.1 Resources

- RedhHat 7 System Administrator's Guide
- Systemd for Administrators, Part IV: Killing Services

1.4 Perusing system logs

On Linux distros based on systemd, logs can be viewed using the `journalctl` command. This requires root privileges. However, users that are members of the `adm` group get access as well. So, add your user to the `adm` group to make viewing logs easier.

Action	Command
Show log since last boot	`journalctl -b`
Kernel messages (like `dmesg`)	`journalctl -k`
Show latest log and wait for changes	`journalctl -f`
Reverse output (newest first)	`journalctl -r`
Show only errors and worse	`journalctl -b -p err`
Filter on time (example)	`journalctl --since=2014-06-00 --until="2014-06-07 12:00:00"`
Since yesterday	`journalctl --since=yesterday`
Show only log of SERVICE	`journalctl -u SERVICE`
Match executable, e.g. `dhclient`	`journalctl /usr/sbin/dhclient`
Match device node, e.g. `/dev/sda`	`journalctl /dev/sda`

1.4.1 "Traditional" logs

Traditionally, logs are text files in `/var/log`. Some services still write their logs to these text files and not to journald.

Action	Command
Live view of log FILE	`tail -f /var/log/FILE`
Colorized live view of boot/kernel messages	`dmesg -wH`

1.4.2 Resources

- Systemd for Administrators, Part XVII: Using the journal

1.5 Configuring the firewall with `firewalld`

The `firewalld-cmd` should run with root privileges, do always use `sudo`.

Action	Command
Firewall state	`firewall-cmd --state`
Reload permanent rules	`firewall-cmd --reload`
Currently enabled features	`firewall-cmd --list-all-zones`

Action	Command
List supported zones	`firewall-cmd --get-zones`
List preconfigured services	`firewall-cmd --get-services`
Enabled features in current zone	`firewall-cmd --list-all`
Enabled features in zone	`firewall-cmd [--permanent] [--zone=ZONE] --list-all`
Enable a service in zone	`firewall-cmd [--permanent] [--zone=ZONE] --add-service=http`
Remove service frome zone	`firewall-cmd [--permanent] [--zone=ZONE] --remove-service=http`
Enable a port in zone	`firewall-cmd [--permanent] [--zone=ZONE] --add-port=80/tcp`
Remove a port from zone	`firewall-cmd [--permanent] [--zone=ZONE] --remove-port=80/tcp`
Turn panic mode on	`firewall-cmd --panic-on`
Turn panic mode off	`firewall-cmd --panic-off`

- Configuration is stored in `/etc/firewalld` and `/usr/lib/firewalld`
- The default zone is `public`, which you don't have to specify on the command line when adding/removing rules
- Adding permanent rules

1.5.1 Resources

- Using Firewalls, in *RHEL 7 Security Guide*
- FirewallD, in *Fedora Project Wiki*