Enterprise Linux 7 (RedHat, CentOS)

Last Modified: 2014-08-15 14:55:42

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.

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`

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

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

Resources

- [RedHat Enterprise Linux 7 Networking Guide](#)
- [Fedora Wiki: Networking/CLI](#)

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`

Action	Command
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`

Resources

- [RedhHat 7 System Administrator's Guide](#)
- [Systemd for Administrators, Part IV: Killing Services](#)

Perusing system logs with `journalctl`

Viewing logs 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`

Resources

- [Systemd for Administrators, Part XVII: Using the journal](#)

Configuring the firewall with `firewalld`

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

Action	Command
List preconfigured services	`firewall-cmd –get-services`
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

Resources

- [Using Firewalls, in RHEL 7 Security Guide](#)
- [FirewallD, in Fedora Project Wiki](#)