Red Hat Cheat Sheet

by nextnely via cheatography.com/71363/cs/18089/

Services

systemctl list-unit-files -at service	Lists enabled/disabled service unit files.
systemctl list-units -at service	Lists enabled/disabled running services.
systemctl list-units -t service --state running	Shows active running services.
-t	Shows enabled service unit files.
-a	Shows both enabled and disabled service unit files.
systemctl mask [service name]	Prevents service from starting.

Cron

/var/spool/cron/[user]	User cron jobs.
/etc/cron.d	System cron jobs.
[minute 0-59] [hour] [day of the month] [month of the year] [day of the week] [path of script]	Cron job time format.
crontab-generator.org	Crontab generator.
0 1 *	Runs job everyday at 1 a.m.
0 1 * [user]	Format for system wide cron jobs.
/etc/at.allow	Allow access to the AT services.
/etc/cron.allow	Allow access to cron services.
/etc/at.deny	

Cron (cont)

/etc/cron.deny

An empty deny file means nobody is denied.
An empty allow file means nobody is allowed.
If both are missing nobody is allowed.
Root always has access.

RPM

rpm -qa	Queries all installed packages.
rpm -qa | sort	
rpm -qi [package]	Shows information about the package.
rpm -qa Group="System Environment/Shells"	
rpm --qa -last	Shows packages install sorted by date
rpm -ql yum	Queries for list of file paths.
rpm -qc yum	
rpm -qf [path to file]	Query file.
rpm -qdf [path to file]	Shows all documentation for specified command/file.
rpm -q --provide	
rpm -q --requires [file]	
rpm -q --changelog [file]	Shows changes to package.

SELinux

Enforcing mode	Security policy is enforced.
Permissive mode	Security policy is observed and warnings are printed but policy is not enforced.

SELinux (cont)

Disabled	Mandatory access control if turned off.
sestatus	Shows SELinux status.
set setenforce <mode>	Temporarily changes SELinux mode.
vi /selinux/-config	SELinux config file.

Networking

nmtui	graphical network editor

Logs

less -N /etc/r-syslog.conf	View rsyslog config-uration file with line numbering turned on.
cat /var/log/-messages	Lists messages log.
grep -v 'systemd:' /var/log/mes-sages	Lists everything that does not include systemd.
tail -f /var/log/-messages	Follows log file.
/var/log/secure	Private authentication messages (logins)
/etc/cron.daily	Logrotate cron job.
/etc/logrota-te.conf	Logrotate configuration file.
logger "mes-sage"	Writes message to messages log file.

yum

yum --showduplicates -list [pacakge name]	Shows versions of a package.
yum list installed	Lists all packages installed.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

Red Hat Cheat Sheet

by nextnely via cheatography.com/71363/cs/18089/

yum (cont)

Bold	Update available in repository.
Bold and underline	Current kernel
Red	Package doesn't exist in repository.
Yellow	Newer package then in repository.
yum list updates	Lists updates for packages installed.
yum list available	
yum info [package name]	Shows package info.
yum deplist [package name]	Shows dependencies for package.
yum search [package name]	Searches for package name.
yum reinstall [package name]	Reinstalled package.
yum reinstall --skip-broken [package name]	
yum remove [package name]	Removes package.
yum autoremove [package name]	Removes packages including dependencies.
yum package-cleanup	Shows unused packages.
yum install yum-utils	
yum check--update	Checks for updates.
yum list obsoletes	
yum install yum-plugin-versionlock	
yum versionlock [package name]	Prevents package from updating.
yum versionlock	Lists version locked packages.

yum (cont)

yum versionlock delete [output from yum versionlock]	Removes version lock from package.
yum update --security	Only updates security packages.
yum update-minimal --security	Install strictly security updates. Doesn't include bug fixes.
yum install yum-plugin changelog	View package change logs.
yum changelog updates	Gets all change logs for packages with updates.
yum changelog [package name]	View change log for specific package.
yum list installed kernel-*	Lists currently installed kernel.
ls -l /boot	Kernel directory.
uname -r	Shows running kernel.
yum list available kernel	Lists available kernel.
yum -y update kernel	Updates kernel.
yum remove kernel	
grub2-set-default [kernel number]	Changes kernel.
ls /lib/modules/$(uname -r)/kernel	Lists kernel module directory.
lsmod	Lists modules.

Time

timedatectl	Lists local time for current timezone.
timedatectl list-timezones | grep America	Filters timezones via grep.
timedatectl set-timezone [timezone]	Sets timezone.
timedatectl set-time 24:00:00	Manually sets time.
timedatectl set-time 2018-12-30	Manually sets date.
timedatectl set-ntp true	Enables NTP.
systemctl restart systemd-timedated	Restarts NTP service.
yum install ntp	Installs NTP client.
/etc/ntp.conf	NTP config file.
ntpdate -q <server address>	Checks NTP server address.
ntpdate <server address>	Sets NTP server.
systemctl enable ntpdate	Enables NTP synchronization.

Journal

journalctl	Lists all journal entries.
journalctl /sbin/crond	Specifies journal.
journalctl -f	Tails journal.
mkdir /var/log/journal	Directory for persistent journals.

By **nextnely**
cheatography.com/nextnely/

Published 19th December, 2018.
Last updated 19th December, 2018.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

File Access Control

ls -l [file name]	Lists group owners.	The user-owner is the third column from the left. THe group--owner is the fourth column.
Read (r)	4	
Write (w)	2	
Execute (x)	1	
-rw-rw-r--	--userowner-groupowner-other	
chmod u=rwx,-g=rx,o=<file>	Symbolic permission format.	
chmod u+rwx <file>	Adds permissions format.	
chmod o-x <file>	Remove permissions format.	
chmod a-x <file>	Removes execute from all positions.	
-R	Recursively adds permissions.	
umask	View umask.	
umask -S	View umask in symbolic notation.	
775	Default directory permissions.	rwxrwxrwx
755	rwx-r-xr-x	

File Access Control (cont)

664	Default file permissions. (umask 002)	rw-rw-r--
umask 022	Changes umask.	
umask 002	rw-rw-r--	Directories- rwx-r--xr-x, Files- rwxr--r--
vi ~/bashrc	User umask startup file	add new umask to end of file.
vi /etc/profile.d/-unmash.sh	System wide unmask.	if ["$UID" -ge 1000] ;then
getfacl <file>	lists ACLs on file.	-t
setfacl -m user:<user>:-<permissions> aclfile	Sets ACLs on file.	setfacl -m user:root:rwx /home/file.txt
setfacl -m group:<group>:<permission> <file>		
setfacl -x group:root <file/dir>		-x remove specific ACL, -k removes all default ACLs, -b removes all ACLs

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com