

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/rsyslog.conf` View rsyslog configuration file with line numbering turned on.

`cat /var/log/message` Lists messages log.

`grep -v 'systemd:' /var/log/message` Lists everything that does not include systemd.

`tail -f /var/log/message` Follows log file.

`/var/log/secure` Private authentication messages (logins)

`/etc/cron.daily` Logrotate cron job.

`/etc/logrotate.conf` Logrotate configuration file.

`logger "message"` Writes message to messages log file.

yum

`yum --showduplicates -list [package name]` Shows versions of a package.

`yum list installed` Lists all packages installed.



yum (cont)		yum (cont)		Time	
Bold	Update available in repository.	yum versionlock delete [output from yum versionlock]	Removes version lock from package.	timedatectl	Lists local time for current timezone.
Bold and underline	Current kernel	yum update --security	Only updates security packages.	timedatectl list-timezones grep America	Filters timezones via grep.
Red	Package doesn't exist in repository.	yum update-minimal --security	Install strictly security updates. Doesn't include bug fixes.	timedatectl set-timezone [timezone]	Sets timezone.
Yellow	Newer package then in repository.	yum install yum-plugin changelog	View package change logs.	timedatectl set-time 24:00:00	Manually sets time.
yum list updates	Lists updates for packages installed.	yum changelog updates	Gets all change logs for packages with updates.	timedatectl set-time 2018-12-30	Manually sets date.
yum list available		yum changelog [package name]	View change log for specific package.	timedatectl set-ntp true	Enables NTP.
yum info [package name]	Shows package info.	yum list installed kernel-*	Lists currently installed kernel.	systemctl restart systemd-timedated	Restarts NTP service.
yum deplist [package name]	Shows dependencies for package.	ls -l /boot	Kernel directory.	yum install ntp	Installs NTP client.
yum search [package name]	Searches for package name.	uname -r	Shows running kernel.	/etc/ntp.conf	NTP config file.
yum reinstall [package name]	Reinstalled package.	yum list available kernel	Lists available kernel.	ntpdate -q <server address>	Checks NTP server address.
yum reinstall --skip-broken [package name]		yum -y update kernel	Updates kernel.	ntpdate <server address>	Sets NTP server.
yum remove [package name]	Removes package.	yum remove kernel		systemctl enable ntpdate	Enables NTP synchronization.
yum autoremove [package name]	Removes packages including dependencies.	grub2-set-default [kernel number]	Changes kernel.	Journal	
yum package-cleanup	Shows unused packages.	ls /lib/modules/\$(uname -r)/kernel	Lists kernel module directory.	journalctl	Lists all journal entries.
yum install yum-utils		lsmod	Lists modules.	journalctl /sbin/cron	Specifies journal.
yum check-update	Checks for updates.			journalctl -f	Tails journal.
yum list obsoletes				mkdir /var/log/journal	Directory for persistent journals.
yum install yum-plugin-versionlock					
yum versionlock [package name]	Prevents package from updating.				
yum versionlock	Lists version locked packages.				



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 Symbolic permission format.
u=rwx,g
=rx,o=
<file>

chmod Adds permissions format.
u+rwx
<file>

chmod Remove permissions format.
o-x
<file>

chmod Removes execute from all positions.
a-x
<file>

-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 wide /unmask.sh System if ["\$UID" -ge 1000] ;then unmask.

getfacl lists ACLs on file. -t

setfacl -m user: ACLs on file. <user>:<permissions> acfile 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

