Initialization: init

- The init process is always the first started (has a PID of 1) and will remain running until the system is shut down
- With init running, the kernel moves to the background awaiting system calls
  - init's first step is to invoke /etc/inittab
  - this script's responsibility is to establish the default runlevel to start in (usually runlevel 5)
  - this file may have other commands as well (see the next slide)

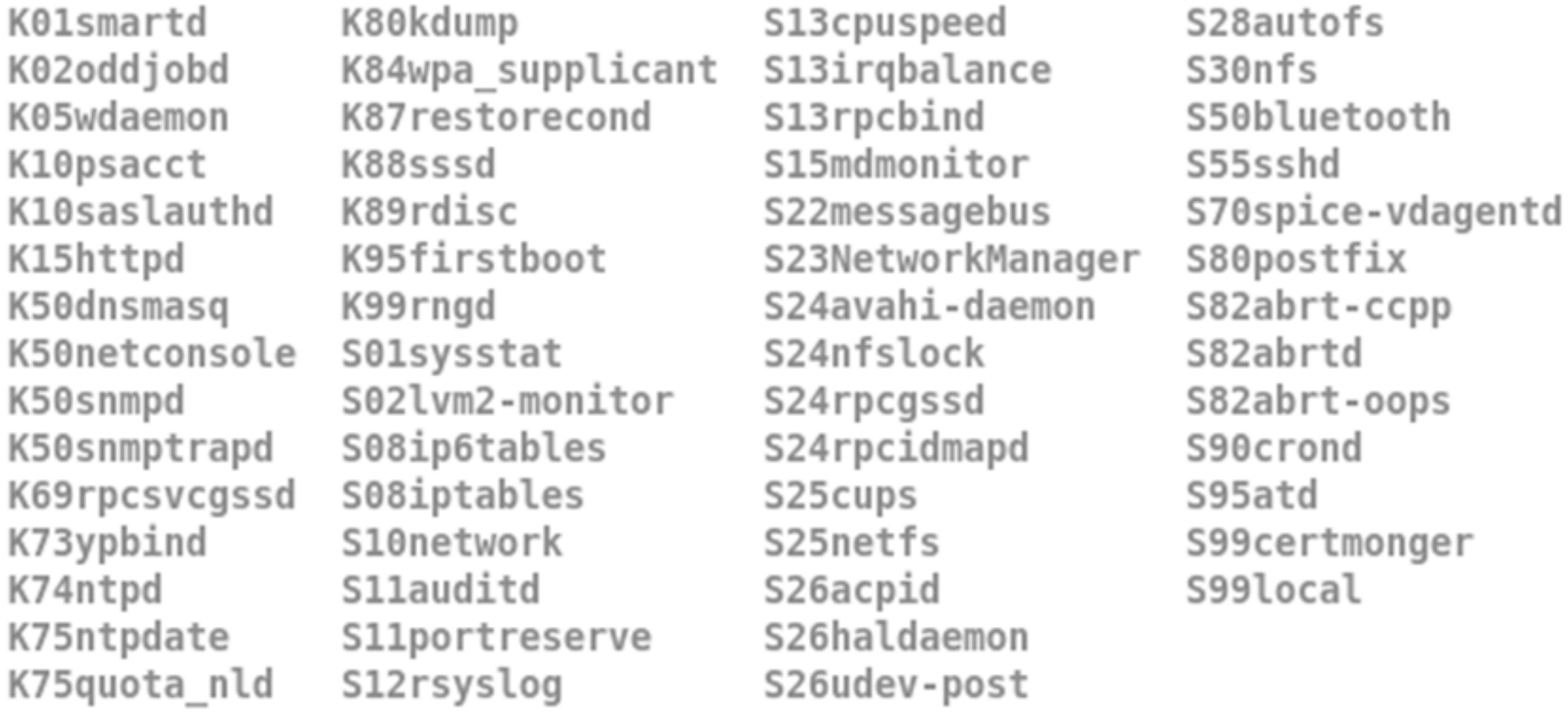
Initialization: runlevels

Run Level	Name	Common Usage
0	Halt	Shuts down the system; not used in inittab as it would immediately shut down on initialization.
1	Single-user mode	Useful for administrative tasks including unmounting partitions and reinstalling portions of the OS; when used, only root access is available.
2	Multi-user mode	In multi-user mode, Linux allows users other than root to log in. In this case, network services are not started so that the user is limited to access via the console only.
3	Multi-user mode with Networking	Commonly used mode for servers or systems that do not require graphical interface.
4	Not used	For special/undefined purposes.
5	Multi-user mode with Networking and GUI	Most common mode for a Linux workstation.
6	Reboot	Reboots the system; not used in inittab because it would reboot repeatedly.

Initialization: rc

The following is the listing for /etc/rc5.d

These are symbolic links to the actual scripts in /etc/init.d to start and stop
The various services for runlevel 5



```
K01smartd      K80kdump           S13cpuspeed        S28autofs
K02oddjobd     K84wpa_supplicant  S13irqbalance      S30nfs
K05wdaemon     K87restorecond     S13rpcbind         S50bluetooth
K10psacct      K88sssd            S15mdmonitor       S55sshd
K10saslauthd   K89rdisc           S22messagebus      S70spice-vdagentd
K15httpd       K95firstboot       S23NetworkManager  S80postfix
K50dnsmasq     K99rngd            S24avahi-daemon    S82abrt-ccpp
K50netconsole  S01sysstat         S24nfslock         S82abrtd
K50snmpd       S02lvm2-monitor    S24rpcgssd         S82abrt-oops
K50snmptrapd   S08ip6tables       S24rpcidmapd       S90crond
K69rpcsvcgssd  S08iptables        S25cups            S95atd
K73ypbind      S10network         S25netfs           S99certmonger
K74ntpd        S11auditd          S26acpid           S99local
K75ntpdate     S11portreserve     S26haldaemon
K75quota_nld   S12rsyslog         S26udev-post
```

Services

- A piece of OS code used to handle requests
- Services are divided into different categories
- Services have distinct features from other OS components or servers
  - Run in the background
  - Handle requests that could come in from different types of sources (user, application software, system software, network message, hardware)
  - They are configurable
  - Services can be started or stopped as desired

Services: Categories

- boot
- file system
- hardware
- language support
- logging
- network, web/Internet
- power management
- scheduling
- system maintenance

Services: Notable Ones in CentOS

Name	Type	Description
acpi	power management	laptop battery fan monitor
acpid	event handling	handles acpi events
anacron	scheduling	for scheduling startup tasks at initialization time
apmd	power management	laptop power management
arpwatch	web/Internet	logs remote IP addresses with hostnames
atd	scheduling	executes at jobs based on a scheduled time and batch jobs based CPU load
auditd	logging	the Linux auditing system daemon which logs system, software and user-generated events
autofs	file system	automatically mounts file systems at initialization
bluetooth	hardware	bluetooth service
certmonger	web/Internet	maintain up-to-date security certificates
cpufreq, cpufreqd	hardware	configures and scales CPU frequency to reduce possible CPU overheating

Name	Type	Description
crond	scheduling	the daemon for handling cronttab jobs
cups	hardware	service for printing
cvs	system	managing multi-user documents
dhcpd	web/Internet	configure DHCP access
dnsmasq	web/Internet	starts/stops DNS caching
gpm	hardware	mouse driver
haldaemon	hardware	monitors for new or removed hardware
httpd	web/Internet	the Apache web server
iptables, ip6tables	web/Internet	the Linux firewalls
mdadm	file system	manages software for RAID
named	web/Internet	starts/stops the BIND program (DNS)
netfs	file system	allows remote mounting
netplugd	network	monitors network interface
network	network	starts and stops network access
nfs	file system	enables network file system sharing
nscd	network	password and group lookup service

Name	Type	Description
oddjobd	system	fields requests from software that otherwise do not have access to needed Linux operations
postfix	network	mail service
prelude	network	intrusion detection system service
rdisc	network	discovers routers on local subnet
rsync	file system	allows remote mounting of file systems
smartd	hardware	monitors SMART devices, particularly hard drives
snmpd	network	network management protocol for small networks
sshd	network	service to permit ssh access
syslog	logging	system logging
ypbind	network	name server for NIS/YP networks

Services: Starting and Stopping

- You can establish which runlevels a service is started or stopped for in three ways
  - By altering the symbolic links in the rc#.d directories (e.g., change S11auditd to K88auditd)
- Using the chkconfig command
  - Without arguments, it lists for all services the runlevels that the service starts and stops in
  - Use arguments as in --level levelnumber service start/stop
  - Use the Service Configuration Manager (see next slide)
    - this GUI tool does not actually allow you to configure a service, just start or stop or change the runlevels that it starts and stops

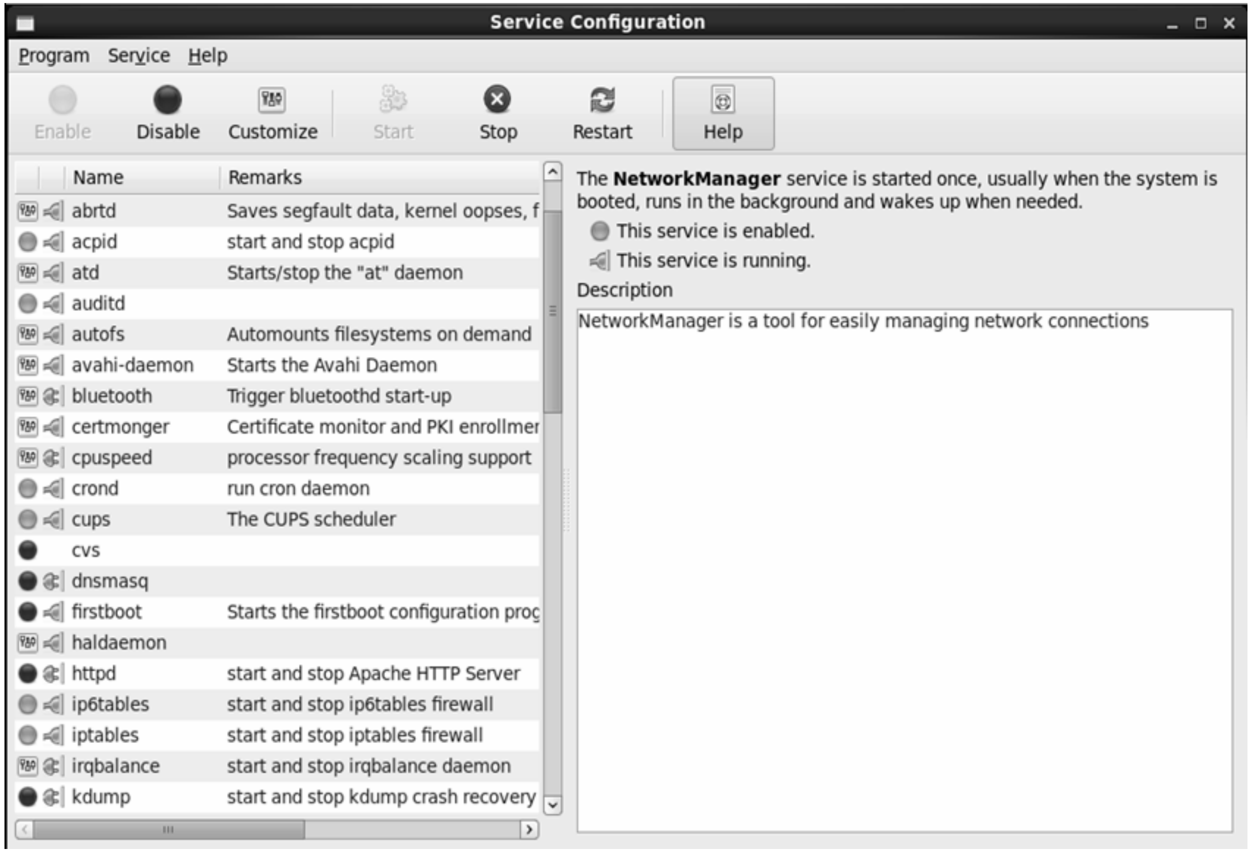
Services: Starting and Stopping

Select a service

Click on Start, Stop, Restart

Click Enable/Disable to indicate that the service should be started or stopped for this runlevel

Select Customize to change start/stop runlevels (only permits runlevels 2-5)



Name	Remarks
abrtd	Saves segfault data, kernel oopses, f
acpid	start and stop acpid
atd	Starts/stop the "at" daemon
auditd	
autofs	Automounts filesystems on demand
avahi-daemon	Starts the Avahi Daemon
bluetooth	Trigger bluetoothd start-up
certmonger	Certificate monitor and PKI enrollmer
cpuspeed	processor frequency scaling support
crond	run cron daemon
cups	The CUPS scheduler
cvs	
dnsmasq	
firstboot	Starts the firstboot configuration proc
haldaemon	
httpd	start and stop Apache HTTP Server
ip6tables	start and stop ip6tables firewall
iptables	start and stop iptables firewall
irqbalance	start and stop irqbalance daemon
kdump	start and stop kdump crash recovery

The **NetworkManager** service is started once, usually when the system is booted, runs in the background and wakes up when needed.

This service is enabled.

This service is running.

Description

NetworkManager is a tool for easily managing network connections

Services: Starting and Stopping

- You can start and stop services from the command line
  - /sbin/service servicename command
    - command is one of start, stop, restart, status
  - Or /etc/init.d/servicename command as in /etc/init.d/auditd start
  - If you are in /etc/init.d, you can also do this as ./auditd start
- The files in /etc/init.d are not the services but are scripts used to start and stop services
  - We explore some portions of the atd script next

Services: a Closer Look

- auditd – the Linux auditing system daemon
  - Logs entries based on activities that match rules defined in auditd's rule file (/etc/sysconfig/audit.rules)
  - Rules use options to specify the type of event and specific criteria as shown in the table below

Syntax	Meaning
-D	Delete any previously defined rules
-b #	# is a number, establish # buffers, e.g., -b 1024
-f #	Set failure flag to # (0 is silent, 1 is print failure messages, 2 is panic or halt the system)
-w directory	Log attempts to access the directory
-w filename	Log attempts to access the file
-w filename –p [rwxa]*	Log attempts to read file (r), write to file (w), execute file (x), or change file's attributes (a). The * indicates that any combination of the options r, w, x, and a can be listed.
-a action,list –S syscall –F field=value	Log system calls; action is either always or never, list is one of task, entry, exit, user or exclude. The –S option allows you to specify a Linux operation such as chmod, mkdir or mount. The –F option allow you to fine-tune the match by testing some system or user parameters such as EUID