Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Home > Faq > Redhat and friends > Security

Linux Default Services Which Are Enabled at Boot

Posted by Vivek Gite <vivek@nixcraft.com>

Can you provide a guidance on default CentOS / Fedora / RHEL / Redhat enterprise Linux services which are enabled at boot time by a default? Can you provide set of recommendations for all default services and which to keep for performance and security and which to turn off?

[1]

You need to minimize software to minimize vulnerability. This provides the best possible protection against vulnerable software.

[2]

Determine Which Services Are Enabled At Boot

Type the following command:

```
# service --status-all [3]
# chkconfig --list | grep '3:on'
```

Sample outputs:

```
acpid           0:off 1:off 2:on 3:on 4:on 5:on 6:off
anacron         0:off 1:off 2:on 3:on 4:on 5:on 6:off
atd             0:off 1:off 2:off 3:on 4:on 5:on 6:off
auditd          0:off 1:off 2:on 3:on 4:on 5:on 6:off
cpuspeed        0:off 1:on 2:on 3:on 4:on 5:on 6:off
crond           0:off 1:off 2:on 3:on 4:on 5:on 6:off
dkms_autoinstaller 0:off 1:off 2:on 3:on 4:on 5:on 6:off
haldaemon       0:off 1:off 2:off 3:on 4:on 5:on 6:off
ip6tables       0:off 1:off 2:on 3:on 4:on 5:on 6:off
irqbalance      0:off 1:off 2:on 3:on 4:on 5:on 6:off
kudzu           0:off 1:off 2:off 3:on 4:on 5:on 6:off
lm_sensors      0:off 1:off 2:on 3:on 4:on 5:on 6:off
mcstrans        0:off 1:off 2:on 3:on 4:on 5:on 6:off
messagebus      0:off 1:off 2:off 3:on 4:on 5:on 6:off
microcode_ctl   0:off 1:off 2:on 3:on 4:on 5:on 6:off
netfs           0:off 1:off 2:off 3:on 4:on 5:on 6:off
network         0:off 1:off 2:on 3:on 4:on 5:on 6:off
ntpd            0:off 1:off 2:on 3:on 4:on 5:on 6:off
rawdevices      0:off 1:off 2:off 3:on 4:on 5:on 6:off
readahead_early 0:off 1:off 2:on 3:on 4:on 5:on 6:off
restorecond     0:off 1:off 2:on 3:on 4:on 5:on 6:off
sendmail        0:off 1:off 2:on 3:on 4:on 5:on 6:off
setroubleshoot  0:off 1:off 2:off 3:on 4:on 5:on 6:off
smartd          0:off 1:off 2:on 3:on 4:on 5:on 6:off
snmpd           0:off 1:off 2:on 3:on 4:on 5:on 6:off
sshd            0:off 1:off 2:on 3:on 4:on 5:on 6:off
syslog          0:off 1:off 2:on 3:on 4:on 5:on 6:off
sysstat         0:off 1:off 2:on 3:on 4:on 5:on 6:off
yum-updatesd    0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

The first column is the name of service which is enabled at boot. It can be disabled using the chkconfig command [4] or ntsysv command [3]:

```
chkconfig serviceName off
service serviceName stop
```

OR

```
ntsysv [5]
```

Service Status

All services can be in any one of the following status at a time:

1. **Disabled** : Disable the service if possible (e.g., NFS and portmap) .
2. **Enabled** : Leave the service enabled (e.g. Power management, and Networking etc).
3. **Configure**: This is essential service and you need to configure so that server works correctly. The service must be configured properly for security and performance (e.g., various servers, Iptables, SELinux, and IP6tables etc).
4. **Remove**: This is not status but you can delete the service (e.g., rsh, vsftpd, X Servers or any other unwanted insecure services).

Recommend Actions on Default Services

Service	Description	Action
acpid	Advanced Configuration and Power Interface event daemon	Enable
anacron	Anacron is like cron, but it does not assume that the machine is running continuously. Hence, it can be used on machines that aren't running 24 hours a day, to control daily, weekly, and monthly jobs that are usually controlled by cron.	Disable on servers
apmd	Advanced Power Management Subsystem (old system). If the server is capable of ACPI support, disable this service	Disable if possible
auditd	The Linux Auditing System	Enable and configure
atd	atd runs jobs queued by at	Enable and configure
autofs	The automount(8) program is used to manage mount points for autofs, the inlined Linux automounter. You can mount NFS, USB, DVD/CD, and CIFS via /etc/fstab.	Disable
avahi-daemon and avahi-dnsconfd	The Avahi mDNS/DNS-SD daemon implementing Apple's ZeroConf architecture (also known as "Rendezvous" or "Bonjour").	Disable
bluetooth and hidd	Bluetooth services for service discovery, authentication, Human Interface Devices (hidd), etc	Disable [6]
cpuspeed	This service monitors the system's idle percentage and reduces or raises the CPUs' clock speeds and voltages accordingly to minimize power consumption when idle and maximize performance when needed	Enable
crond	Service to execute scheduled commands via crond daemon.	Enable and configure
cups	Common unix printing system service	Disable if possible
dc_client & dc_client	Startup script for the Distcache SSL Session Cache Client and server proxy. Disable if you do not need cache proxy.	Disable if possible
dnsmasq	the DNS caching server. Enable if your ISP or remote DNS caching server is pretty slow.	Enable
dkmdkms_autoinstallers	dkms is a framework which allows kernel modules to be dynamically built for each kernel on your system in a simplified and organized fashion.	Disable if possible
firstboot	RHLE specific service. It does a few configuration following successful installation of the operating system.	Disable
gpm	A cut and paste utility and mouse server service for virtual consoles.	Disable
haldaemon	This service is used for collecting and maintaing information about hardware from several sources. This is only used for X and desktop apps. Disable it on servers.	Disable
hplip	A service for non-PostScript HP printer. Disable it on servers.	Disable
irda	IrDA(TM) (Infrared Data Association) is an industry standard for wireless, infrared communication between devices. IrDA speeds range from 9600 bps to 4 Mbps, and IrDA can be used by many modern devices including laptops, LAN	Disable if possible

	adapters, PDAs, printers, and mobile phones.	
iscsi & iscsid	iscsi service logs into iSCSI targets needed at system startup (i.e. iscsi client). iscsid will start and stop iSCSI daemon. Use this if you've iscsi based storage.	Disable if possible
iptables & ip6tables	IPv4 and IPv6 firewall service.	Enable [7] and configure
irqbalance	The irqbalance service will distribute interrupts across the cpus on a multiprocessor system with the purpose of spreading the load.	Enable
isdn	Provides the Internet connectivity using an ISDN modem.	Disable if not using an ISDN modem.
kdump	Kernel crash dump analyzer. This service is useful for kernel hackers and device driver development or testing new kernel feature. Dsable the service on production boxes.	Disable
kudzu	RHEL specific hardware detection service. This is required on desktop or laptop where end users can add a new hardware but not on servers.	Disable
lm_sensors	lm_sensors is used for monitoring motherboard sensor values.	Disable
lvm2-monitor	Starts and stops dmeventd monitoring for lvm2. If you are not using LVM2 (Linux volume manager) based storage disable it.	Disable
mcstrans	Starts the SELinux Context Translation System daemon. This is site specific SELinux requirements.	Disable if possible
mdmonitor	software RAID monitoring and management service. If you are not using software RAID disable it. This is not required for hardware RAID setup as they comes with their own programs.	Disable if possible
messagebus	This service broadcasts notifications of system events and other messages (D-bus). Turn it on for bluetooth, X Windows and desktop systems.	Disable
microcode ctl	Script to apply cpu microcode for Intel IA32 processor. If you are not using Intel IA32 processor disable it.	Disable
netfs, nfslock, rpcgssd, rpcidmapd, and portmap	Mount and configure Linux network network filesystems (NFS). If you are not using NFS client/server technology disable it.	Disable if possible
network	A service to activates/deactivates all network interfaces configured to start at boot time.	Enable
pcscd	The PC/SC smart card sevice is a resource manager for the PC/SC lite and Musclecard frameworks. It coordinatescommunications with smart card readers, smart cards, and cryptographic tokens that are connected to the system.If Smart Cards are not in use on the system, disable this service:	Disable
readahead_early and readahead_later	This sevice provide one-time caching of files belonging to a few boot services. It does not provide any boosting. Just disable it.	Disable
restorecond	This service restores the correct security context for SELinux.	Enable
rhnsd	This service handles the task of connecting periodically to the RHN servers to check for updates, notifications and perform system monitoring tasks according to the service level that your server is subscribed for. Disable this service and use yum-updatesd service.	Disable
sendmail	Use to start sendmail server.	Enable and configure
smartd	Self Monitoring and Reporting Technology (SMART) Daemon for hard disks.	Enable and configure
setroubleshoot	This service starts the SELinux Troubleshooting daemon. It will send notification tothe desktop user of SELinux access denied messages in a user-friendly fashion.	Disable
sshd	The openssh server. If you need remote login enable it. You must enable this on all servers so that you can login and configure everything.	Enable [8]
syslog	Syslog is the facility by which many other Linux daemons use to log messages to various system log files. It is a good idea to always run syslog.	Enable
xfs	X Windows font server. Disable it on servers.	Disable

yum-updatesd	Update notification daemon for system packages.	Enable [9]

Remove Outdated Insecure Services

Is there a mission-critical reason for users to access the system via the **insecure protocols** such as ftp, NIS and telnet? The following services are obsolete services and must be deleted for security:

1. **inetd and xinetd** : This is not installed by default. But, it it is installed just delete it. Consider **switching to more secure services** which provide the needed functionality.
2. **telnet-serve**r : Delete insecure telnet remote login, use OpenSSH server and ssh client to get back into the server.
3. **rsh-server** : Delete insecure rlogin, rsh, or rcp commands. Use scp and ssh commands from the OpenSSH.
4. **ypserv & ypbind** : Remote outdated NIS, consider using OpenLDAP or Fedora / Redhat directory server.
5. **tftp-server** : Remove outdated and insecure TFTP server software.

Configure Required Services

Other services need to be installed and configr as and when required:

1. **httpd**: The Apache web server.
2. **php-cgi**: The php server.
3. **bind9 (named)**: The DNS server.
4. **ntpd** : The time network based time client/server.
5. **snmpd** : The net-snmp server.
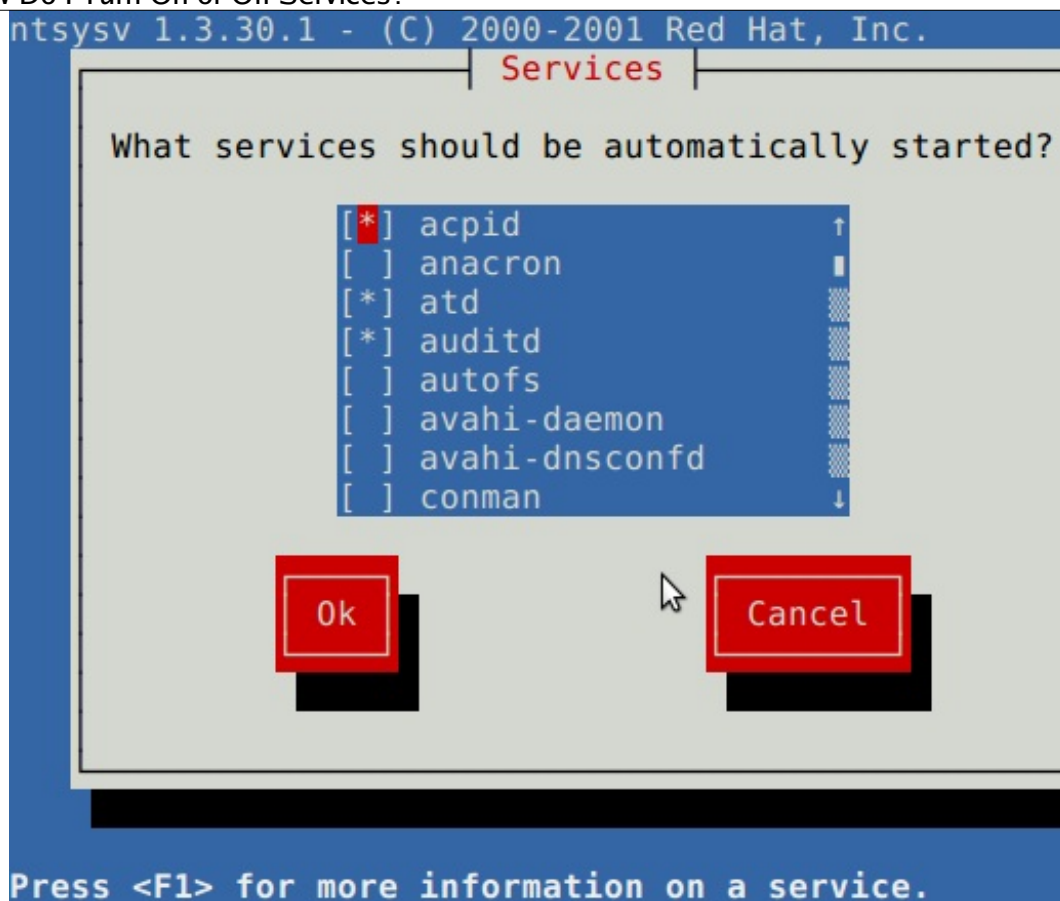6. **squid** : The squid proxy and web caching server.

How Do I Turn On or Off Services?

Use the ntsysv application which is a simple interface for configuring runlevel services which are also configurable through chkconfig command:

```
# ntsysv
```

OR

```
# chkconfig serviceName off
```

[10]

Fig.01: ntsysv in action

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our daily email newsletter or weekly newsletter to make sure you don't miss a single tip/tricks. Alternatively, subscribe via RSS/XML feed.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/linux-default-services-which-are-enabled-at-boot/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/redhat-and-friends/**
[2] Image: **http://www.cyberciti.biz/faq/category/centos/**
[3] service --status-all: **http://www.cyberciti.biz/faq/check-running-services-in-rhel-redhat-fedora-centoslinux/**
[4] chkconfig command: **http://www.cyberciti.biz/faq/rhel5-update-rcd-command/**
[5] ntsysv: **http://www.cyberciti.biz/faq/tag/ntsysv-command/**
[6] Disable: **http://www.cyberciti.biz/faq/linux-disable-bluetooth-host-controller-interface-daemon/**
[7] Enable: **http://www.cyberciti.biz/faq/rhel-fedorta-linux-iptables-firewall-configuration-tutorial/**
[8] Enable: **http://www.cyberciti.biz/tips/linux-unix-bsd-openssh-server-best-practices.html**
[9] Enable: **http://www.cyberciti.biz/faq/red-hat-centos-fedora-send-package-update-notification-via-email/**
[10] Image: **http://www.cyberciti.biz/faq/linux-default-services-which-are-enabled-at-boot/ntsysv-services-rhel-fedora-centos-linux/**