

# Unix Server Set-Up Configurations

Revised: JEU, 23<sup>rd</sup> October 2001

webmaster@ukmotorsport.com

## **Scope**

This document sets-out a standard for the generic set-up of a Unix machine that is intended for any role. It does not cover the specifics of bespoke application set-ups. It is intended that the machine will be able to function as part of an Intranet, Extranet or be added to the Intranet with or without a firewall implied.

## **Overview of Process**

1. Unpack hardware, record part numbers and serial numbers etc.
2. Decide disk partitioning scheme
3. Install Operating system, invoke partitioning scheme and configure network connectivity
4. Install Patches
5. Apply Unix Armor script
6. Increase Logging Levels
7. Install Standard (Unix) Utilities
8. Carry out Miscellaneous Configuration Tasks
9. Install Housekeeping Scripts and Cronjobs
10. Configure RAID if applicable
11. Install Applications (covered elsewhere)

## **Detailed Description of Process**

1. Unpacking, Inventory etc.
  - Receive goods against delivery note and confirm schedule
  - Unpack goods and do whatever we normally do when we receive new product such as recording hardware information, labeling the server.
  - Confirm that the warranty agreements are in place against serial numbers.
  - Connect physical hardware requirements and power-up machine.
2. Disk Partitioning
  - Plan the disk partitioning based on generic guidelines combined with site-specific requirements. Swap space should be included with the guideline of swap space = physical memory x 2. Make sure that the plan allows for estimated traffic and growth in content for around three years. Partition the disks according to a formula to be as yet agreed:
3. Operating system
  - Fully install OS to agreed version (hopefully current latest but probably Solaris 2.7: the decision will need to be based this decision on any applications, which limit the version of the OS (such as Broadvision).

- Invoke previously planned disk partitioning scheme.
- Configure any ethernet interfaces using advice from the network team as to what IP addresses are available.
- Carry out required tasks to get machine on LAN:
  1. Decide hostname using scheme if provided. It is important to get this right at this stage and not at a further one!
  2. Configure `/etc/nsswitch.conf`
  3. Configure `/etc/hosts` (this should include the **minimum** of entries: DNS should be used for lookups rather than entries in the hosts file.)
  4. Configure `/etc/defaultrouter` (e.g. if the base address of new machine is 192.168.\$.25 then the entry in this file *usually* should be 192.168.\$.1)
- Create alias for each IP address on interface in `/etc/hosts`. Create appropriate `/etc/hostname.hme0.$` files where \$ is the last quadrant of the IPV4 address. The reasoning for this is that management of multiple IP addresses via `/sbin/ifconfig` is made very much more convenient. Make sure all addresses are up on the interface and listening.
- Reboot and test

#### 4. Install OS Patch Set

- Install Sun approved patch set. These comes from the latest SunSolve patch cluster from the most recent SunSolve CD or <http://sunsolve.sun.co.uk/>
- Reboot and test

#### 5. Apply Unix Armor Script

- Install required libraries etc for SSH compliant telnetd and ftpd wrapper binaries.
- Install and run `armor` that wraps TCP/IP services: **see separate documentation on this topic. DO NOT reboot until the following checks are carried out:**
- The `/etc/hosts.allow` file should minimally contain the following **before** the machine is rebooted:
 

```
ALL: <yourdomain>.co.uk :ALLOW
ALL: 192.168.52. :ALLOW
```
- Add admin user account with a GID of 10 (which is the GID of the default staff group) and label as " Admin Account". This provides a clean non-privileged account to go with the privileged root account. This is useful for testing and is a primary, non-privileged point of telnet access especially for remote machines.
- Add admin user to wheel group in `/etc/group` (the primary GID for the admin user will be that of the staff group which should be 10) and make sure that the admin user can su to root (need to log out and back in to test).
- Reboot the machine and check that you can login and su.
- Remove any extra unnecessary services not removed by the `armor` process. Using `netstat -a | grep LISTEN` is it possible to see what TCP/IP & UDP ports are in a LISTEN state for inbound requests. Many of these are superfluous (and therefore provide a security risk) and should be turned off. In each case

stop the service and then rename from SXXblah to off.SXXblah. Examples of these (are written in the armor script) include:

1. /etc/rc2.d/S74xntpd
  2. /etc/rc2.d/S73cachefs.daemon
  3. /etc/rc2.d/S73nfs.client
  4. /etc/rc2.d/S99dtlogin (anyone using CDE will need this however). If you stop this service whilst the console is using it, the machine will hang. Log out on the console, stop the service, mv S99dtlogin and restart the machine.
  5. /etc/rc2.d/S85power
  6. /etc/rc2.d/S80lp
  7. /etc/rc2.d/S74autofs
  8. /etc/rc3.d/S15nfs.server
  9. /etc/rc3.d/S79snmpdx
  10. /etc/rc3.d/S77dmi
  11. /etc/rc2.d/S70uucp
  12. /etc/rc2.d/S76nscd
- Reboot and test.
6. Increase Logging Levels
- Edit /etc/syslog.conf and uncomment the lines containing the auth.login and mail.debug entries and do a /etc/rc2.d/S74syslog stop; /etc/rc2.d/S74syslog start command. This increases logging levels for authenticated logins.
  - Edit /etc/rc2.d/S72inetsvc and change the bottom-line from /usr/sbin/inetd -s to /usr/sbin/inetd -s -t This increases the level of TCP/IP logging from a security perspective. Do a /usr/sbin/shutdown -g60 -i6 -y. This is a dangerous thing to do with a live box! (Armor does this anyway).
7. Install Standard (Unix) Utilities
- ftp to /var/spool/pkg the following package from <http://www.sunfreeware.com/>
    1. gzip, and install this first inorder to gunzip the following:
    2. top : performance monitoring
    3. lsof : process/file diagnostics
    4. traceroute : network diagnosis
    5. snort : intrusion detection package
    6. dig : DNS diagnosis
    7. pine : handy email client
    8. Perl: needed for Perl scripts in cgi-bin (*only* for http and development servers)
    9. bash : popular alternative shell
    10. tcsh : alternative shell
    11. m4: macro processor
    12. plus others, according to requirements.
  - Install the above (accepting the default locations) and add symbolic links (using /usr/bin/ln -s) to each binary from /usr/local/bin/
  - Install the sysinfo utility available from <http://www.magnicomp.com/sysinfo/> Add symbolic link from the main binary to /usr/local/bin/ The purpose of this

binary is to provide a whole heap of kernel information normally accessible using several commands with unmemorable syntaxes. The basic install procedure for sysinfo is:

1. Download the appropriate binary from above for the version of Solaris.
2. Untar into /opt/
3. Rename sysinfo-version-number-XXXX to sysinfo
4. Edit /etc/sysinfo.cf and add "ConfDir /opt/sysinfo/config"
5. Run with /opt/sysinfo/sysinfo
6. Make a symbolic link from /usr/local/bin to /opt/sysinfo/sysinfo

### Carry out Miscellaneous Configuration Tasks

- As the root user, execute `catman -w&` to produce the man `-k` indexes.
- Modify /etc/motd to include details of location (ISP, room, rack) hardware and functionality
- As root, touch /etc/notrouter and reboot to stop machine being used as a router. Check that it has worked with `/usr/sbin/ndd /dev/ip ip_forwarding: answer should be 0`. *This ought to be the out-of-the-box default but it's worth doing anyway.* This is not appropriate for a machine acting as a firewall.
- Edit /etc/hosts so that the localhost entry is at the end of the line containing the loopback address. This is useful for the syslog process.
- Append /etc/services.extra to the foot of /etc/services so that all items found from `netstat -a | grep LISTEN` are accounted for and labelled apart from multifarious Oracle, and BV ports.
- Add .forward files for all interactive accounts, especially those that own any crontab tasks. Each .forward file should contain the entry `youraccount@yourdomain.co.uk`. This will send cron messages to your inbox.
- Set the shell for each interactive user according to preference (DO NOT alter roots' shell) although a standard shell should probably be agreed: /usr/local/bin/bash is recommended.
- Create /etc/shells and include in it all the shells required for any users wishing to use ftp. Don't forget any "false" shells required for chroot jail functionality. Probably we need:
  1. /sbin/sh : This should always be root's shell
  2. /bin/csh
  3. /bin/false : This should be the shell for chroot jail ftp accounts
  4. /bin/ksh
  5. /bin/sh
  6. /usr/local/bin/bash
  7. /usr/local/bin/tcsh
- Comment out the crontab entries for the UUCP as they do-nothing useful: they do things that were useful in the days of newsgroup propagation by UUCP
- Add `-X /tmp/sendmail.log` to the line which starts /usr/lib/sendmail in /etc/rc2.d/S88sendmail This logs all sendmail transactions and is useful in case of spam attacks etc. For a site employing the BroadVision mails

gateway this log file could grow enormously (because BV sends a “HELO” command every minute) and also a site with heavy email traffic: this needs monitoring. You will need to issue an `/etc/rc2.d/S88sendmail stop;/etc/rc2.d/S88sendmail start` command to restart sendmail. At some point a decision should be made as to if sendmail should be running. If not, issue an `/etc/rc2.d/S88sendmail stop` command and rename `/etc/rc2.d/S88sendmail` to `/etc/rc2.d/off.S88sendmail`

- If sendmail is needed then we need to agree a standard configuration:
- Uncomment all the crontab entries for the sys user. This is required to enable system performance monitoring (other things are required. Edit `/etc/rc2.d/S21perf` and remove #'s as appropriate. Stop and start the S21perf service.: ).
- edit `/etc/group` so that the entries are consistent (i.e. group memberships)

#### 9. Install Housekeeping Scripts and Cronjobs

- Make `/usr/local/alpha` directory and populate with our standard maintenance and alert scripts:
- Set-up and test crontab tasks for root and any other out-of-the-box user accounts and the admin account.

#### 10. Configure RAID

#### 11. Install Applications