How to build a Kickstart server and push Secure RHEL Installations.

Motivation

I find the practice of “Google engineering” frustrating and rewarding at the same time. There is a lot of disinformation posted on sites around the world, that disinformation is then discovered by search engines, people then come across and repost on their sites. My frustration really stems from people that don’t take the time to validate their source(s) and mindlessly post disinformation. With that stated, I’ve taken the time to glean the correct information and post worthy instructions that are repeatable. I will take the time to say I do enjoy finding new ways to do things on computers.

My assumption if you are reading this is you know how to perform a base install of RedHat Enterprise Linux (RHEL) by yourself and that you have the CDROM/DVD with the RHEL software. Leave this in the CDROM/DVD drive, we will need files off of it. I’m also assuming you have a mount point for the installation media and that it is already mounted. Your root account needs to use Bash for the shell in the examples shown below. If you changed root’s default shell, then type in “bash” and stay in that shell while typing in the examples below.

Install Necessary Services

I’m going to show the install using Yellowdog Updater Modified (YUM), you could use RedHat Package Manager (RPM) to do the same thing. As root, execute the following command:

```
yum install xinetd httpd tftp-server
```

Answer yes with a “Y” and depress the Return key. This will install the necessary software packages for you to work with.

TFTP Customization

I’m not a fan of the base setup of tftp-server. Therefore, I like to clean this up and return to a known good solution. As root, execute the following command:

```
rm -rf /tftpboot/*
```

Now build the new directories:

```
mkdir -p /tftpboot/msgs /tftpboot/pxelinux.cfg /tftpboot/rhel
```

Populate the msgs directory:

```
cd /tftpboot/msgs
cp <CDROM_mount_point>/isolinux/* .
```

You should end up with the following files in the msgs directory:

```
-r--r--r-- 1 root root    2048 Apr  7 12:34 boot.cat
-r--r--r-- 1 root root     439 Apr  7 14:58 boot.msg
```

```
-rw-r--r-- 1 root root     668 Apr  7 14:58 expert.msg
-r--r--r-- 1 root root     871 Apr  7 14:58 general.msg
-r--r--r-- 1 root root 7399936 Apr  7 12:34 initrd.img
-r--r--r-- 1 root root   10648 Apr  7 12:34 isolinux.bin
-r-xr-xr-x 1 root root     364 Apr  7 12:34 isolinux.cfg
-r--r--r-- 1 root root   94600 Apr  7 12:34 memtest
-r--r--r-- 1 root root     817 Apr  7 12:34 options.msg
-r--r--r-- 1 root root     860 Apr  7 14:58 param.msg
-r--r--r-- 1 root root     530 Apr  7 14:58 rescue.msg
-rw-r--r-- 1 root root     545 Apr  7 14:58 snake.msg
-r--r--r-- 1 root root   23107 Apr  7 12:34 splash.lss
-r--r--r-- 1 root root    2659 Apr  7 12:34 TRANS.TBL
-r--r--r-- 1 root root 1932316 Apr  7 12:34 vmlinuz
```

Now populate rhel directory:

```
cd /tftpboot/rhel/
cp <CDROM_mount_point>/images/pxeboot/{initrd.img,vmlinuz} .
```

You should see:

```
-r--r--r-- 1 root root 7399936 Apr  7 12:33 initrd.img
-r--r--r-- 1 root root 1932316 Apr  7 12:33 vmlinuz
```

Get files for the /tftpboot directory:

```
cd /tftpboot/
cp /usr/lib/syslinux/{*.c32,pxelinux.0,memdisk} .
```

Your /tftpboot directory should now look like this:

```
-rw-r--r-- 1 root root  3464 Apr  7 12:49 chain.c32
-rw-r--r-- 1 root root  5540 Apr  7 12:49 ethersel.c32
drwxr-xr-x 3 root root  4096 Apr  7 15:06 linux-install
-rw-r--r-- 1 root root 60904 Apr  7 12:49 mboot.c32
-rw-r--r-- 1 root root 20020 Apr  7 12:46 memdisk
-rw-r--r-- 1 root root 26496 Apr  7 12:49 menu.c32
drwxr-xr-x 2 root root  4096 Apr  7 14:58 msgs
-rw-r--r-- 1 root root 13148 Apr  7 12:48 pxelinux.0
drwxr-xr-x 2 root root  4096 Apr  7 15:12 pxelinux.cfg
drwxr-xr-x 2 root root  4096 Apr  7 12:33 rhel
```

Change directory and edit the following file:

```
cd /tftpboot/pxelinux.cfg/
vi default
```

Now create the default file and populate with the following information:

```
default 2
timeout 30
prompt 1
display msgs/boot.msg
F1 msgs/boot.msg
F2 msgs/general.msg
F3 msgs/expert.msg
F4 msgs/param.msg
F5 msgs/rescue.msg
F7 msgs/snake.msg

label 1
   localboot 1
```

```
label 2
   kernel rhel/vmlinuz
   append initrd=rhel/initrd.img \
          ramdisk_size=32768 \
          ks=http://192.168.139.70/ksfiles/ks.cfg \
          method=http://192.168.139.70/rhel54/ \
          ip=dhcp
```

When done, depress Escape key and type “:wq!”

Use the built in tool, “gethostip” to create the reference from default. E.g.:

```
gethostip 192.168.139.71
```

Produces:

```
192.168.139.71 192.168.139.71 C0A88B47
```

So use the third field for your pointer (this step is critical for each IP that will connect):

```
cp default `gethostip 192.168.139.71 | awk ‘{print $3}’`
```

Edit the tftp service file (/etc/xinetd.d/tftp), it should look like this:

```
service tftp
{
        disable                 = no
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -v -s /tftpboot
        per_source              = 11
        cps                     = 100 2
        max-block-size          = 32768  ## Max size is 65464.
        flags                   = IPv4
}
```

Now, activate the service and set to startup at boot time:

```
service xinetd start
chkconfig –level 345 xinetd on
```

This section is now complete.

DHCP Customization

As the root user, cut and paste the following into the new file /etc/dhcpd.conf:

```
#
#
#
ddns-update-style interim;
ignore client-updates;
deny unknown-clients;
allow bootp;
allow booting;

subnet 192.168.139.0 netmask 255.255.255.0 {
                     option routers      192.168.139.2;
                     option subnet-mask  255.255.255.0;
                     range dynamic-bootp 192.168.139.71 192.168.139.95;
                     default-lease-time  86400;
                     max-lease-time      86400;
                     option time-offset  -5;
}

class "pxeclients" {
     match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
     next-server 192.168.139.70;  #@# this is my tftp server
     filename "pxelinux.0";
}

group {
     host datanode1 { hardware ethernet 00:0c:29:a2:58:18 ; }
     host datanode2 { hardware ethernet 00:0C:29:08:63:19 ; }
}
```

Obviously you will need to change this example subnet and IPs to ones that will work in your environment. You will notice I have a hostname of datanode1 and its corresponding MAC address. I did this so that only these boxes, datanode(1|2) will perform the PXE boot from this DHCP server.

Now, activate the service and set to startup at boot time:

```
service dhcpd start
chkconfig –level 345 dhcpd on
```

This section is now complete.

Apache Customization

Copy your installation media from your CDROM/DVD to this folder:

```
mkdir -p /var/www/html/rhel54
cp <CDROM_mount_point>/* /var/www/html/rhel54
```

Secure the new files:

```
chown -R root:root /var/www/html/rhel54
find /var/www/html/rhel54 -type f | xargs chmod 660
find /var/www/html/rhel54 -type d | xargs chmod 755
```

Now, activate the service and set to startup at boot time:

```
service httpd start
chkconfig –level 345 httpd on
```

This section is now complete.

Kickstart Customization

Create a new directory:

```
mkdir /var/www/html/ksfiles
```

create the ks.cfg file inside the above directory and populate with this content:

```
# Install OS instead of upgrade
install
```

```
# Use text mode install
text
# Network information
network --bootproto=dhcp --device=eth0 --onboot=on
# System language
lang en_US
langsupport --default en_US
# System keyboard
keyboard us
mouse
# System timezone
timezone --isUtc America/New_York
#Root password
rootpw --iscrypted <enc_passwd_here>
#platform=x86, AMD64, or Intel EM64T
# System authorization information
auth  --useshadow  --enablemd5
# SELinux configuration
selinux --disabled
# Firewall configuration
firewall --disabled
# don't enter installation key
key --skip


# Run the Setup Agent on first boot
firstboot --disable

# Installation logging level
logging --level=info

# Use network installation
url --url=http://192.168.139.70/rhel54/

# X Window System configuration information
xconfig  --defaultdesktop=GNOME --depth=32 --resolution=1280x1024 --
startxonboot

# Reboot after installation
reboot


# Clear the Master Boot Record
zerombr
# Partition clearing information
clearpart --all --initlabel
# Disk partitioning information ------>  these numbers were made for my 40GB
hard drive
part /boot  --asprimary  --bytes-per-inode=4096 --fstype="ext3" --size=200
part swap   --asprimary  --bytes-per-inode=4096 --fstype="swap" --size=2048
part /      --asprimary  --bytes-per-inode=4096 --fstype="ext3" --size=4096
part /usr                --bytes-per-inode=4096 --fstype="ext3" --size=8192
part /home               --bytes-per-inode=4096 --fstype="ext3" --size=4096
part /tmp                --bytes-per-inode=4096 --fstype="ext3" --size=2048
part /var                --bytes-per-inode=4096 --fstype="ext3" --size=10240
part /var/log/audit --bytes-per-inode=4096 --fstype="ext3" --size=2048
part /opt --bytes-per-inode=4096 --fstype="ext3" --size=4096     --grow
```

```
# System bootloader configuration
bootloader --location=mbr --append="elevator=anticipatory"

# add a few users for administration:
user --name=masterfoo  --groups=wheel --homedir=/home/masterf --
password=<enc_passwd_here> --iscrypted --shell=/bin/bash --uid=1600

#
%packages --resolvedeps
… the whole file is in the Appendix.
```

To get the root and any user passwords encrypted, use these two commands:

```
read –s PASSWORD
openssl passwd –1 $PASSWORD
```

Place the encrypted password(s) into your ks.cfg file. Don't use plain text because anyone with network access can read the ks.cfg file.

I could have placed a ton of lockdowns into the bash script in the %post section, however I opted out because I don't know if it would break your server. I recommend going to http://cisecurity.org and download their Linux hardening guides. You can copy and paste from those into your bash scripts. Test, test and test with these on development servers before trying on any production servers.

I favor using the IBM approach and having all of my third party software loaded under /opt. You may have different requirements, so modify as necessary. In fact, it would be advantageous to install and run this graphical tool, "system-config-kickstart". Then create your bash script and paste on the end of your new ks.cfg file.

Testing

Browser

Open your favorite browser and go to <your> ip address, as in: http://192.168.139.70/rhel54/

Make sure you can see your installation files listed here.

Virtual Machine

I opened my <hostname>.vmx and retrieved the MAC address and placed in /etc/dhcpd.conf.

I then deleted the hard drive on each test and re-added it to vmware workstation. I then booted up and let the new VM find the dhcp server and start the load process.

Final Thoughts

I've learned a lot about Kickstart installs of RHEL with this paper. Hopefully you've learned some valuable information and your install works as smoothly as mine.

Appendix:

/etc/dhcpd.conf:

```
#
#
#
ddns-update-style interim;
ignore client-updates;
deny unknown-clients;
allow bootp;
allow booting;

subnet 192.168.139.0 netmask 255.255.255.0 {
                     option routers      192.168.139.2;
                     option subnet-mask  255.255.255.0;
                     range dynamic-bootp 192.168.139.71 192.168.139.95;
                     default-lease-time  86400;
                     max-lease-time      86400;
                     option time-offset  -5;
}

class "pxeclients" {
     match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
     next-server 192.168.139.70;  #@# this is my tftp server
     filename "pxelinux.0";
}

group {
     host datanode1 { hardware ethernet 00:0c:29:a2:58:18 ; }
     host datanode2 { hardware ethernet 00:0C:29:08:63:19 ; }
}
```

/tftpboot/pxelinux.cfg/default:

```
default 2
timeout 30
prompt 1
display msgs/boot.msg
F1 msgs/boot.msg
F2 msgs/general.msg
F3 msgs/expert.msg
F4 msgs/param.msg
F5 msgs/rescue.msg
F7 msgs/snake.msg

label 1
   localboot 1

label 2
   kernel rhel/vmlinuz
   append initrd=rhel/initrd.img \
          ramdisk_size=32768 \
          ks=http://192.168.139.70/ksfiles/ks.cfg \
          method=http://192.168.139.70/rhel54/ \
          ip=dhcp
```

/var/www/html/ksfiles/ks.cfg:

```
< # Install OS instead of upgrade
install
# Use text mode install
text
# Network information
network --bootproto=dhcp --device=eth0 --onboot=on
# System language
lang en_US
langsupport --default en_US
# System keyboard
keyboard us
mouse
# System timezone
timezone --isUtc America/New_York
#Root password
rootpw --iscrypted <enc_passwd_here>
#platform=x86, AMD64, or Intel EM64T
# System authorization information
auth  --useshadow  --enablemd5
# SELinux configuration
selinux --disabled
# Firewall configuration
firewall --disabled
# don't enter installation key
key --skip


# Run the Setup Agent on first boot
firstboot --disable

# Installation logging level
logging --level=info

# Use network installation
url --url=http://192.168.139.70/rhel54/

# X Window System configuration information
xconfig  --defaultdesktop=GNOME --depth=32 --resolution=1280x1024 --
startxonboot

# Reboot after installation
reboot


# Clear the Master Boot Record
zerombr
# Partition clearing information
clearpart --all --initlabel
# Disk partitioning information ------>  these numbers were made for my 40GB
hard drive
part /boot      --asprimary     --bytes-per-inode=4096   --fstype="ext3"
--size=200
part swap       --asprimary     --bytes-per-inode=4096   --fstype="swap"
--size=2048
```

```
part /          --asprimary     --bytes-per-inode=4096   --fstype="ext3"
--size=4096
part /usr                       --bytes-per-inode=4096   --fstype="ext3"
--size=8192
part /home                      --bytes-per-inode=4096   --fstype="ext3"
--size=4096
part /tmp                       --bytes-per-inode=4096   --fstype="ext3"
--size=2048
part /var                       --bytes-per-inode=4096   --fstype="ext3"
--size=10240
part /var/log/audit             --bytes-per-inode=4096   --fstype="ext3"
--size=2048
part /opt                       --bytes-per-inode=4096   --fstype="ext3"
--size=4096     --grow


# System bootloader configuration
bootloader --location=mbr --append="elevator=anticipatory"

# add a few users for administration:
user --name=masterf \
     --groups=wheel \
     --homedir=/home/masterf \
     --password=<enc_passwd_here> \
     --iscrypted \
     --shell=/bin/bash \
     --uid=1600

#
%packages --resolvedeps
@admin-tools
@base
@base-x
@core
@editors
@engineering-and-scientific
@gnome-desktop
@graphical-internet
@kde-desktop
@java
@legacy-software-support
@mail-server
@network-server
@server-cfg
@system-tools
@text-internet
@web-server


## Packages I want to make sure are installed.
aide
amanda
arpwatch
audit
autoconf
automake
bison-runtime
```

```
boost
bzip2
checkpolicy
cpio
curl
device-mapper-multipath
dhcp
diffstat
diffutils
dos2unix
doxygen
dstat
dtach
dump
elfutils
elfutils-devel
elfutils-devel.i386
elfutils-devel-static
elfutils-devel-static.i386
elfutils-libelf
elfutils-libelf-devel
elfutils-libelf-devel.i386
elfutils-libelf-devel-static
elfutils-libelf-devel-static.i386
elfutils-libelf.i386
elfutils-libs
elfutils-libs.i386
fipscheck
flex
fuse
fuse-libs.i386
fuse-libs.x86_64
gcc
gd
gdb
gedit
gettext
gnuplot
gtk+
httpd
iptraf
kernel
kernel-doc
kernel-headers
keyutils
libpng
libtool
logrotate
logwatch
lsof
lsscsi
lynx
m4
nedit
netlabel_tools
ntp
openssh-askpass
```

```
openssh-clients
openssh-server
openssl
oprofile
oprofile-gui
parted
pcre
perl
perl-HTML-Parser
perl-XML-Twig
php
php-pear
policycoreutils-newrole
postfix
psutils
python
python-devel
python-docs
python-elementtree
python-imaging
python-iniparse
python-lcms
python-ldap
python-numeric
python-pyblock
python-setuptools
python-sqlite
python-tools
python-urlgrabber
pyxf86config
rpm-build
rsyslog
ruby
ruby-devel.x86_64
ruby-docs
ruby-irb
ruby-libs.i386
ruby-libs.x86_64
ruby-mode
ruby-rdoc
ruby-ri
ruby-tcltk
screen
setools
star
strace
stunnel
subversion
sudo
syslinux
sysstat
time
tree
trousers
units
unix2dos
unixODBC.i386
unixODBC.x86_64
unixODBC-devel.i386
unixODBC-devel.x86_64
unzip
wget
valgrind
vim-common
vim-enhanced
vim-X11
vlock
xinetd
yum
yum-keys
yum-list-data
yum-security
yum-utils
yum-verify
zenity
zip

## For Oracle 11gR2 installs:
binutils
compat-libstdc++-33
compat-libstdc++-33.i386
elfutils-libelf
elfutils-libelf-devel
gcc
gcc-c++
gdbm
gdbm.i386
glibc
glibc.i686
glibc-common
glibc-devel
glibc-devel.i386
glibc-headers
ksh
libaio
libaio.i386
libaio-devel
libaio-devel.i386
libgcc
libgcc.i386
libstdc++
libstdc++.i386
libstdc++-devel
make
numactl
numactl.i386
numactl-devel
numactl-devel.i386
sysstat
util-linux


## Packages I want to exclude
#
```

```
-anacron
-aspell
-aspell-en
-autofs
-avahi
-blas
-bluez-gnome
-bluez-hcidump
-bluez-utils
-bluez-utils-cups
-byacc
-cadaver
-cdecl
-cdparanoia
-coolkey
-crash
-cscope
-ctags
-dia
-doxygen
-elinks
-emacs
-emacs-leim
-emacspeak
-ethereal
-ethereal-gnome
-evolution
-fbset
-fetchmail
-finger
-gaim
-gcc-g77
-gcc-java
-gimp
-gimp-data-extras
-gimp-gap
-gimp-help
-gimp-print-plugin
-gnome-games
-gnomemeeting
-gnome-pilot
-httpd-manual
-httpd-suexec
-indent
-irda-utils
-isdn4k-utils
-java-1.4.2-gcj-compat
-kernel-devel
-kernel-hugemem-devel
-kernel-smp-devel
-lapack
-lm_sensors
-mutt
-net-snmp-libs
-NetworkManager
-NetworkManagerDispatcher
-nfs-utils
```

```
-nmap
-octave
-OpenIPMI
-openldap-clients
-oprofile
-perl-Crypt-SSLeay
-perl-LDAP
-perl-XML-Dumper
-perl-XML-Encoding
-perl-XML-Grove
-perl-XML-LibXML
-perl-XML-LibXML-Common
-perl-XML-NamespaceSupport
-perl-XML-Parser
-perl-XML-SAX
-perl-XML-Twig
-php
-php-ldap
-php-mysql
-planner
-portmap
-psgml
-python-ldap
-rcs
-rdist
-readahead
-rhythmbox
-rsh
-samba-client
-sane-frontends
-sendmail
-sendmail-cf
-setools
-slrn
-spamassassin
-splint
-squid
-system-config-httpd
-system-config-samba
-talk
-tcpdump
-telnet
-texinfo
-tftp
-tog-pegasus
-tog-pegasus-devel
-tux
-units
-valgrind
-valgrind-callgrind
-vino
-vnc
-vnc-server
-webalizer
-wireless-tools
-wpa_supplicant
-xcdroast
```

```
-xchat
-xdelta
-xsane
-xsane-gimp
-ypbind
-yum-updatesd
-zisofs-tools
-zsh

## Pre install commands/scripts
%pre

## Post install commands/scripts
%post
################################################
#
#   This is where all of your lockdowns go.
#   Go to:  http://www.cisecurity.org/
#   for Linux hardening recommendations.
#
%post --log=/root/post-kickstart.log

#!/usr/bin/bash

rpm --import /usr/share/rhn/RPM-GPG-KEY

################ Login Banner ################

cat <<-EOF > /etc/issue

                    Authorized Use Only.
Transactions may be monitored. By continuing past this point,
        you expressly consent to this monitoring.

EOF

cat /etc/issue >> /etc/issue.net
cat /etc/issue >> /etc/motd

################ File and folder Permissions/Ownerships ################
# Create any files that are not yet found
touch /var/log/audit/audit.log
touch /var/log/cron

# Change Permissions of all files in /etc/skel and /var/log
find /etc/skel -type f -exec chmod 644 '{}' \;
find /var/log/ -type f -exec chmod 640 '{}' \;
find /etc/skel -type f -exec chown root '{}' \;

# Start changing permissions and owners around
chmod -R 700 /etc/cron.daily
chmod -R 700 /etc/cron.hourly
chmod -R 700 /etc/cron.monthly
chmod -R 700 /etc/cron.weekly
chmod -R 700 /var/crash
chgrp -R root /etc/news/*
chown -R root /etc/news/*
```

```
chmod 600 /boot/grub/grub.conf
chmod 644 /etc/{environment}
chgrp root /etc/{profile,bashrc,environment}
chown root /etc/{profile,bashrc,environment}
chmod 444 /etc/{profile,bashrc}
chmod 644 /etc/aliases
chown root /etc/aliases
chmod 400 /etc/at.allow
chown root:root /etc/at.allow
chmod 600 /etc/at.deny
chown root:root /etc/at.deny
chmod 600 /etc/audit/audit.rules
chmod 600 /etc/audit/auditd.conf
chmod 400 /etc/cron.allow
chown root:root /etc/cron.allow
chgrp root /etc/cron.d
chmod 750 /etc/cron.d
chown root /etc/cron.d
chown root /etc/cron.d/*
chgrp root /etc/cron.daily
chmod 750 /etc/cron.daily
chown root /etc/cron.daily
chown root /etc/cron.daily/*
chmod 600 /etc/cron.deny
chown root:root /etc/cron.deny
chgrp root /etc/cron.hourly
chmod 750 /etc/cron.hourly
chown root /etc/cron.hourly
chown root /etc/cron.hourly/*
chgrp root /etc/cron.monthly
chmod 750 /etc/cron.monthly
chown root /etc/cron.monthly
chown root /etc/cron.monthly/*
chgrp root /etc/cron.weekly
chmod 750 /etc/cron.weekly
chown root /etc/cron.weekly
chown root /etc/cron.weekly/*
chmod 400 /etc/crontab
chmod 444 /etc/csh.cshrc
chmod 444 /etc/csh.login
chmod 600 /etc/cups/client.conf
chmod 600 /etc/cups/cupsd.conf
chmod 644 /etc/exports
chown root /etc/exports
chmod 600 /etc/ftpusers
chown root /etc/ftpusers
chmod 444 /etc/hosts
chmod 600 /etc/inittab
chmod 600 /etc/lilo.conf
chmod 640 /etc/login.defs
chmod 444 /etc/mail/sendmail.cf
chmod 600 /etc/news/hosts.nntp
chmod 600 /etc/news/hosts.nntp.nolimit
chmod 600 /etc/news/nnrp.access
chmod 600 /etc/news/passwd.nntp
chown root /etc/passwd
chgrp root /etc/rc.d/init.d/*
```

```
chmod ug-s /etc/rc.d/init.d/*
chmod 755 /etc/rc.d/init.d/*
chown root /etc/rc.d/init.d/*
chmod 744 /etc/rc.d/init.d/auditd
chmod 740 /etc/rc.d/init.d/iptables
chmod 600 /etc/rc.d/rc.local
chmod 600 /etc/rc.local
chgrp root /etc/samba/smb.conf
chmod 644 /etc/samba/smb.conf
chown root /etc/samba/smb.conf
chgrp root /etc/securetty
chmod 400 /etc/securetty
chown root /etc/securetty
chmod 750 /etc/security
chgrp root /etc/security/access.conf
chmod 640 /etc/security/access.conf
chown root /etc/security/access.conf
chmod 600 /etc/security/console.perms
chmod 600 /etc/security/console.perms.d/50-default.perms
chmod 444 /etc/services
chown root /etc/services
chmod 400 /etc/shadow
chown root /etc/shadow
chmod 444 /etc/shells
chmod 600 /etc/skel/.bashrc
chown root:sys /etc/snmp/snmpd.conf
chgrp root /etc/sysctl.conf
chmod 600 /etc/sysctl.conf
chown root /etc/sysctl.conf
chgrp root /etc/syslog.conf
chmod 600 /etc/syslog.conf
chown root /etc/syslog.conf
chmod 440 /etc/xinetd.conf
chmod 755 /etc/xinetd.d
chmod 700 /root
chmod 400 /root/{.bashrc,.bash_profile,.cshrc,.tcshrc}
chmod 740 /sbin/iptables
chgrp root /usr/bin/smbpasswd
chmod 600 /usr/bin/smbpasswd
chown root /usr/bin/smbpasswd
chmod 644 /usr/share/doc/
chmod 740 /usr/share/logwatch/scripts/services/iptables
chmod 644 /usr/share/man/
chown root:root /var/crash
chmod 600 /var/log/faillog
chmod 700 /var/log/audit
chmod 640 /var/log/audit/*
chown root:root /var/log/btmp
chmod 600 /var/log/btmp
chmod 600 /var/log/cron
chmod 600 /var/log/dmesg
chmod 400 /var/log/lastlog
chmod 640 /var/log/maillog
chown root /var/log/maillog
chmod 600 /var/log/messages
chmod 600 /var/log/secure
chmod 600 /var/log/wtmp
```

```
chown root:root /var/log/wtmp
chmod 755 /var/spool/at/spool
chown root:root /var/spool/at/spool
chgrp root /var/spool/cron
chmod 750 /var/spool/cron
chown root /var/spool/cron
chown root /var/spool/cron/*

sed -i "/umask/ c\umask 022" /etc/bashrc
sed -i "/umask/ c\umask 022" /etc/csh.cshrc

##################### Delete Unecessary Users #####################
/usr/sbin/userdel shutdown
/usr/sbin/userdel halt
/usr/sbin/userdel sync
/usr/sbin/userdel ftp
/usr/sbin/userdel news
/usr/sbin/userdel operator
/usr/sbin/userdel games
/usr/sbin/userdel gopher
/usr/sbin/userdel nfsnobody

##################### Turn Additional Services off #####################
/sbin/chkconfig acpid off
/sbin/chkconfig anacron off
/sbin/chkconfig apmd off
/sbin/chkconfig atd off
/sbin/chkconfig autofs off
/sbin/chkconfig avahi-daemon off
/sbin/chkconfig bluetooth off
/sbin/chkconfig cups off
/sbin/chkconfig irda off
/sbin/chkconfig lm_sensors off
/sbin/chkconfig nfslock off
/sbin/chkconfig portmap off
/sbin/chkconfig rawdevices off
/sbin/chkconfig rhnsd off
/sbin/chkconfig rpcgssd off
/sbin/chkconfig rpcidmapd off
/sbin/chkconfig rpcsvcgssd off
/sbin/chkconfig sendmail off
/sbin/chkconfig setroubleshoot off
/sbin/chkconfig xfs off
/sbin/chkconfig xinetd off

# Set the default run level to 3
perl -p -i -e 's/^.*id:.:initdefault:$/id:3:initdefault:/g' /etc/inittab

#############################################################################
########                                                             ########
########                Finished all Security Configurations         ########
########                                                             ########
#############################################################################
```

/etc/httpd/conf/httpd.conf:

```
#
# This is the main Apache server configuration file.  It contains the
# configuration directives that give the server its instructions.
# See URL:http://httpd.apache.org/docs-2.2/ for detailed information.
# In particular, see
# URL:http://httpd.apache.org/docs/2.2/mod/directives.html
# for a discussion of each configuration directive.
#
#
# Do NOT simply read the instructions in here without understanding
# what they do.  They're here only as hints or reminders.  If you are unsure
# consult the online docs. You have been warned.
#
# The configuration directives are grouped into three basic sections:
#  1. Directives that control the operation of the Apache server process as a
#     whole (the 'global environment').
#  2. Directives that define the parameters of the 'main' or 'default'
server,
#     which responds to requests that aren't handled by a virtual host.
#     These directives also provide default values for the settings
#     of all virtual hosts.
#  3. Settings for virtual hosts, which allow Web requests to be sent to
#     different IP addresses or hostnames and have them handled by the
#     same Apache server process.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path.  If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so "logs/foo.log"
# with ServerRoot set to "/etc/httpd" will be interpreted by the
# server as "/etc/httpd/logs/foo.log".
#

### Section 1: Global Environment
#
# The directives in this section affect the overall operation of Apache,
# such as the number of concurrent requests it can handle or where it
# can find its configuration files.
#

#
# Don't give away too much information about all the subcomponents
# we are running.  Comment out this line if you don't mind remote sites
# finding out what major optional modules you are running
ServerTokens OS

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# NOTE!  If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the LockFile documentation
# (available at <URL:http://httpd.apache.org/docs-
2.0/mod/core.html#lockfile>);
```

```
# you will save yourself a lot of trouble.
#
# Do NOT add a slash at the end of the directory path.
#
ServerRoot "/etc/httpd"

#
# PidFile: The file in which the server should record its process
# identification number when it starts.
#
PidFile "/var/run/httpd.pid"

#
# Timeout: The number of seconds before receives and sends time out.
#
TimeOut 45

#
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive on

#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 80

#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
KeepAliveTimeout 15

##
## Server-Pool Size Regulation (MPM specific)
##

# prefork MPM
# StartServers: number of server processes to start
# MinSpareServers: minimum number of server processes which are kept spare
# MaxSpareServers: maximum number of server processes which are kept spare
# MaxClients: maximum number of server processes allowed to start
# MaxRequestsPerChild: maximum number of requests a server process serves
<IfModule prefork.c>
StartServers 5
MinSpareServers 5
MaxSpareServers 10
ServerLimit 15
MaxClients 15
MaxRequestsPerChild 2000
</IfModule>

# worker MPM
# StartServers: initial number of server processes to start
# MaxClients: maximum number of simultaneous client connections
# MinSpareThreads: minimum number of worker threads which are kept spare
# MaxSpareThreads: maximum number of worker threads which are kept spare
# ThreadsPerChild: constant number of worker threads in each server process
# MaxRequestsPerChild: maximum number of requests a server process serves
<IfModule worker.c>
StartServers         4
MaxClients         150
MinSpareThreads     25
MaxSpareThreads     75
ThreadsPerChild     250
MaxRequestsPerChild  0
</IfModule>

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, in addition to the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#
#Listen 12.34.56.78:80
Listen *:80

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO
you
# have to place corresponding `LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by `httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule auth_digest_module modules/mod_auth_digest.so
LoadModule authn_file_module modules/mod_authn_file.so
LoadModule authn_alias_module modules/mod_authn_alias.so
LoadModule authn_anon_module modules/mod_authn_anon.so
LoadModule authn_dbm_module modules/mod_authn_dbm.so
LoadModule authn_default_module modules/mod_authn_default.so
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule authz_user_module modules/mod_authz_user.so
LoadModule authz_owner_module modules/mod_authz_owner.so
LoadModule authz_groupfile_module modules/mod_authz_groupfile.so
LoadModule authz_dbm_module modules/mod_authz_dbm.so
LoadModule authz_default_module modules/mod_authz_default.so
LoadModule ldap_module modules/mod_ldap.so
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
LoadModule include_module modules/mod_include.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule logio_module modules/mod_logio.so
LoadModule env_module modules/mod_env.so
LoadModule ext_filter_module modules/mod_ext_filter.so
LoadModule mime_magic_module modules/mod_mime_magic.so
LoadModule expires_module modules/mod_expires.so
LoadModule deflate_module modules/mod_deflate.so
LoadModule headers_module modules/mod_headers.so
LoadModule usertrack_module modules/mod_usertrack.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule mime_module modules/mod_mime.so
LoadModule dav_module modules/mod_dav.so
LoadModule status_module modules/mod_status.so
LoadModule autoindex_module modules/mod_autoindex.so
LoadModule info_module modules/mod_info.so
LoadModule dav_fs_module modules/mod_dav_fs.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule negotiation_module modules/mod_negotiation.so
LoadModule dir_module modules/mod_dir.so
LoadModule actions_module modules/mod_actions.so
LoadModule speling_module modules/mod_speling.so
LoadModule userdir_module modules/mod_userdir.so
LoadModule alias_module modules/mod_alias.so
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule cache_module modules/mod_cache.so
LoadModule suexec_module modules/mod_suexec.so
LoadModule disk_cache_module modules/mod_disk_cache.so
LoadModule file_cache_module modules/mod_file_cache.so
LoadModule mem_cache_module modules/mod_mem_cache.so
LoadModule cgi_module modules/mod_cgi.so
LoadModule version_module modules/mod_version.so

#
# The following modules are not loaded by default:
#
#LoadModule cern_meta_module modules/mod_cern_meta.so
#LoadModule asis_module modules/mod_asis.so

#
# Load config files from the config directory "/etc/httpd/conf.d".
#
Include conf.d/*.conf

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information (ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus off

#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd as.
#   . On SCO (ODT 3) use "User nouser" and "Group nogroup".
#   . On HPUX you may not be able to use shared memory as nobody, and the
#     suggested workaround is to create a user www and use that user.
#  NOTE that some kernels refuse to setgid(Group) or semctl(IPC_SET)
#  when the value of (unsigned)Group is above 60000;
#  don't use Group #-1 on these systems!
#
User apache
Group apache

### Section 2: 'Main' server configuration
#
# The directives in this section set up the values used by the 'main'
# server, which responds to any requests that aren't handled by a
# <VirtualHost> definition.  These values also provide defaults for
# any <VirtualHost> containers you may define later in the file.
#
# All of these directives may appear inside <VirtualHost> containers,
# in which case these default settings will be overridden for the
# virtual host being defined.
#

#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed.  This address appears on some server-generated pages, such
# as error documents.  e.g. admin@your-domain.com
#
ServerAdmin W3bMistress@SecuredNetwork.lan

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work.  See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
ServerName kickstart

#
# UseCanonicalName: Determines how Apache constructs self-referencing
# URLs and the SERVER_NAME and SERVER_PORT variables.
# When set "Off", Apache will use the Hostname and Port supplied
# by the client.  When set "On", Apache will use the value of the
# ServerName directive.
#
UseCanonicalName on

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
```

```
DocumentRoot "/var/www/html"

#
# UserDir: The name of the directory that is appended onto a user's home
# directory if a ~user request is received.
#
# The path to the end user account 'public_html' directory must be
# accessible to the webserver userid.  This usually means that ~userid
# must have permissions of 711, ~userid/public_html must have permissions
# of 755, and documents contained therein must be world-readable.
# Otherwise, the client will only receive a "403 Forbidden" message.
#
# See also: http://httpd.apache.org/docs/misc/FAQ.html#forbidden
#
<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    UserDir "disable"

    #
    # To enable requests to /~user/ to serve the user's public_html
    # directory, use this directive instead of "UserDir disable":
    #
    #UserDir public_html

</IfModule>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
# The index.html.var file (a type-map) is used to deliver content-
# negotiated documents.  The MultiViews Option can be used for the
# same purpose, but it is much slower.
#
DirectoryIndex

#
# AccessFileName: The name of the file to look for in each directory
# for access control information.  See also the AllowOverride directive.
#
AccessFileName .htaccess

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
</Files>

#
# TypesConfig describes where the mime.types file (or equivalent) is
# to be found.
#
TypesConfig "/etc/mime.types"

#
# DefaultType is the default MIME type the server will use for a document
# if it cannot otherwise determine one, such as from filename extensions.
# If your server contains mostly text or HTML documents, "text/plain" is
# a good value.  If most of your content is binary, such as applications
# or images, you may want to use "application/octet-stream" instead to
# keep browsers from trying to display binary files as though they are
# text.
#
DefaultType text/plain

#
# The mod_mime_magic module allows the server to use various hints from the
# contents of the file itself to determine its type.  The MIMEMagicFile
# directive tells the module where the hint definitions are located.
#
<IfModule mod_mime_magic.c>
#   MIMEMagicFile /usr/share/magic.mime
    MIMEMagicFile conf/magic
</IfModule>

#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
# nameserver.
#
HostNameLookups Off

#
# EnableMMAP: Control whether memory-mapping is used to deliver
# files (assuming that the underlying OS supports it).
# The default is on; turn this off if you serve from NFS-mounted
# filesystems.  On some systems, turning it off (regardless of
# filesystem) can improve performance; for details, please see
# http://httpd.apache.org/docs-2.0/mod/core.html#enablemmap
#
#EnableMMAP off

#
# EnableSendfile: Control whether the sendfile kernel support is
# used to deliver files (assuming that the OS supports it).
# The default is on; turn this off if you serve from NFS-mounted
# filesystems.  Please see
# http://httpd.apache.org/docs-2.0/mod/core.html#enablesendfile
#
#EnableSendfile off

#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "/var/log/httpd/error_log"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent


#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here.  Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
# CustomLog logs/access_log common
CustomLog logs/access_log combined

#
# If you would like to have agent and referer logfiles, uncomment the
# following directives.
#
#CustomLog logs/referer_log referer
#CustomLog logs/agent_log agent

#
# If you prefer a single logfile with access, agent, and referer information
# (Combined Logfile Format) you can use the following directive.
#
#CustomLog logs/access_log combined

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (error documents, FTP directory listings,
# mod_status and mod_info output etc., but not CGI generated documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
#
ServerSignature on

#
```

```
# Aliases: Add here as many aliases as you need (with no limit). The format
is
# Alias fakename realname
#
# Note that if you include a trailing / on fakename then the server will
# require it to be present in the URL.  So "/icons" isn't aliased in this
# example, only "/icons/".  If the fakename is slash-terminated, then the
# realname must also be slash terminated, and if the fakename omits the
# trailing slash, the realname must also omit it.
#
# We include the /icons/ alias for FancyIndexed directory listings.  If you
# do not use FancyIndexing, you may comment this out.
#
Alias /icons/ "/var/www/icons/"

#
# This should be changed to the ServerRoot/manual/.  The alias provides
# the manual, even if you choose to move your DocumentRoot.  You may comment
# this out if you do not care for the documentation.
#
# 05/23/05: This is now provided via a separate package called httpd-manual
# which comes with an own manual alias
#Alias /manual "/var/www/manual"

<IfModule mod_dav_fs.c>
    # Location of the WebDAV lock database.
    DAVLockDB /var/lib/dav/lockdb
</IfModule>

#
# ScriptAlias: This controls which directories contain server scripts.
# ScriptAliases are essentially the same as Aliases, except that
# documents in the realname directory are treated as applications and
# run by the server when requested rather than as documents sent to the
client.
# The same rules about trailing "/" apply to ScriptAlias directives as to
# Alias.
#
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"

<IfModule mod_cgid.c>
#
# Additional to mod_cgid.c settings, mod_cgid has Scriptsock <path>
# for setting UNIX socket for communicating with cgid.
#
#Scriptsock            logs/cgisock
</IfModule>

#
# Redirect allows you to tell clients about documents which used to exist in
# your server's namespace, but do not anymore. This allows you to tell the
# clients where to look for the relocated document.
# Example:
# Redirect permanent /foo http://www.example.com/bar

#
# Directives controlling the display of server-generated directory listings.
```

```
#

#
# IndexOptions: Controls the appearance of server-generated directory
# listings.
#
IndexOptions FancyIndexing VersionSort NameWidth=*

#
# AddIcon* directives tell the server which icon to show for different
# files or filename extensions.  These are only displayed for
# FancyIndexed directories.
#
AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip

AddIconByType (TXT,/icons/text.gif) text/*
AddIconByType (IMG,/icons/image2.gif) image/*
AddIconByType (SND,/icons/sound2.gif) audio/*
AddIconByType (VID,/icons/movie.gif) video/*

AddIcon /icons/binary.gif .bin .exe
AddIcon /icons/binhex.gif .hqx
AddIcon /icons/tar.gif .tar
AddIcon /icons/world2.gif .wrl .wrl.gz .vrml .vrm .iv
AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
AddIcon /icons/a.gif .ps .ai .eps
AddIcon /icons/layout.gif .html .shtml .htm .pdf
AddIcon /icons/text.gif .txt
AddIcon /icons/c.gif .c
AddIcon /icons/p.gif .pl .py
AddIcon /icons/f.gif .for
AddIcon /icons/dvi.gif .dvi
AddIcon /icons/uuencoded.gif .uu
AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl
AddIcon /icons/tex.gif .tex
AddIcon /icons/bomb.gif core
AddIcon /icons/back.gif ..
AddIcon /icons/hand.right.gif README
AddIcon /icons/folder.gif ^^DIRECTORY^^
AddIcon /icons/blank.gif ^^BLANKICON^^

#
# DefaultIcon is which icon to show for files which do not have an icon
# explicitly set.
#
DefaultIcon /icons/unknown.gif

#
# AddDescription allows you to place a short description after a file in
# server-generated indexes.  These are only displayed for FancyIndexed
# directories.
# Format: AddDescription "description" filename
#
#AddDescription "GZIP compressed document" .gz
#AddDescription "tar archive" .tar
#AddDescription "GZIP compressed tar archive" .tgz
```

```
#
# ReadmeName is the name of the README file the server will look for by
# default, and append to directory listings.
#
# HeaderName is the name of a file which should be prepended to
# directory indexes.
ReadmeName README.html
HeaderName HEADER.html

#
# IndexIgnore is a set of filenames which directory indexing should ignore
# and not include in the listing.  Shell-style wildcarding is permitted.
#
IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t

#
# DefaultLanguage and AddLanguage allows you to specify the language of
# a document. You can then use content negotiation to give a browser a
# file in a language the user can understand.
#
# Specify a default language. This means that all data
# going out without a specific language tag (see below) will
# be marked with this one. You probably do NOT want to set
# this unless you are sure it is correct for all cases.
#
# * It is generally better to not mark a page as
# * being a certain language than marking it with the wrong
# * language!
#
# DefaultLanguage nl
#
# Note 1: The suffix does not have to be the same as the language
# keyword --- those with documents in Polish (whose net-standard
# language code is pl) may wish to use "AddLanguage pl .po" to
# avoid the ambiguity with the common suffix for perl scripts.
#
# Note 2: The example entries below illustrate that in some cases
# the two character 'Language' abbreviation is not identical to
# the two character 'Country' code for its country,
# E.g. 'Danmark/dk' versus 'Danish/da'.
#
# Note 3: In the case of 'ltz' we violate the RFC by using a three char
# specifier. There is 'work in progress' to fix this and get
# the reference data for rfc1766 cleaned up.
#
# Catalan (ca) - Croatian (hr) - Czech (cs) - Danish (da) - Dutch (nl)
# English (en) - Esperanto (eo) - Estonian (et) - French (fr) - German (de)
# Greek-Modern (el) - Hebrew (he) - Italian (it) - Japanese (ja)
# Korean (ko) - Luxembourgeois* (ltz) - Norwegian Nynorsk (nn)
# Norwegian (no) - Polish (pl) - Portugese (pt)
# Brazilian Portuguese (pt-BR) - Russian (ru) - Swedish (sv)
# Simplified Chinese (zh-CN) - Spanish (es) - Traditional Chinese (zh-TW)
#
AddLanguage ca .ca
AddLanguage cs .cz .cs
AddLanguage da .dk
AddLanguage de .de
AddLanguage el .el
AddLanguage en .en
AddLanguage eo .eo
AddLanguage es .es
AddLanguage et .et
AddLanguage fr .fr
AddLanguage he .he
AddLanguage hr .hr
AddLanguage it .it
AddLanguage ja .ja
AddLanguage ko .ko
AddLanguage ltz .ltz
AddLanguage nl .nl
AddLanguage nn .nn
AddLanguage no .no
AddLanguage pl .po
AddLanguage pt .pt
AddLanguage pt-BR .pt-br
AddLanguage ru .ru
AddLanguage sv .sv
AddLanguage zh-CN .zh-cn
AddLanguage zh-TW .zh-tw

#
# LanguagePriority allows you to give precedence to some languages
# in case of a tie during content negotiation.
#
# Just list the languages in decreasing order of preference. We have
# more or less alphabetized them here. You probably want to change this.
#
LanguagePriority en ca cs da de el eo es et fr he hr it ja ko ltz nl nn no pl
pt pt-BR ru sv zh-CN zh-TW

#
# ForceLanguagePriority allows you to serve a result page rather than
# MULTIPLE CHOICES (Prefer) [in case of a tie] or NOT ACCEPTABLE (Fallback)
# [in case no accepted languages matched the available variants]
#
ForceLanguagePriority Prefer Fallback

#
# Specify a default charset for all content served; this enables
# interpretation of all content as UTF-8 by default.  To use the
# default browser choice (ISO-8859-1), or to allow the META tags
# in HTML content to override this choice, comment out this
# directive:
#
AddDefaultCharset UTF-8

#
# AddType allows you to add to or override the MIME configuration
# file mime.types for specific file types.
#
#AddType application/x-tar .tgz

#
# AddEncoding allows you to have certain browsers uncompress
# information on the fly. Note: Not all browsers support this.
# Despite the name similarity, the following Add* directives have nothing
# to do with the FancyIndexing customization directives above.
#
#AddEncoding x-compress .Z
#AddEncoding x-gzip .gz .tgz

# If the AddEncoding directives above are commented-out, then you
# probably should define those extensions to indicate media types:
#
AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz

#
# AddHandler allows you to map certain file extensions to "handlers":
# actions unrelated to filetype. These can be either built into the server
# or added with the Action directive (see below)
#
# To use CGI scripts outside of ScriptAliased directories:
# (You will also need to add "ExecCGI" to the "Options" directive.)
#
#AddHandler cgi-script .cgi

#
# For files that include their own HTTP headers:
#
#AddHandler send-as-is asis

#
# For type maps (negotiated resources):
# (This is enabled by default to allow the Apache "It Worked" page
#  to be distributed in multiple languages.)
#
AddHandler type-map var

#
# Filters allow you to process content before it is sent to the client.
#
# To parse .shtml files for server-side includes (SSI):
# (You will also need to add "Includes" to the "Options" directive.)
#
AddType text/html .shtml
AddOutputFilter INCLUDES .shtml

#
# Action lets you define media types that will execute a script whenever
# a matching file is called. This eliminates the need for repeated URL
# pathnames for oft-used CGI file processors.
# Format: Action media/type /cgi-script/location
# Format: Action handler-name /cgi-script/location
#

#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
```

```
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#

#
# Putting this all together, we can internationalize error responses.
#
# We use Alias to redirect any /error/HTTP_<error>.html.var response to
# our collection of by-error message multi-language collections.  We use
# includes to substitute the appropriate text.
#
# You can modify the messages' appearance without changing any of the
# default HTTP_<error>.html.var files by adding the line:
#
#   Alias /error/include/ "/your/include/path/"
#
# which allows you to create your own set of files by starting with the
# /var/www/error/include/ files and
# copying them to /your/include/path/, even on a per-VirtualHost basis.
#

Alias /error/ "/var/www/error/"

<IfModule mod_negotiation.c>
<IfModule mod_include.c>
    <Directory "/var/www/error">
        AllowOverride None
        Options IncludesNoExec
        AddOutputFilter Includes html
        AddHandler type-map var
        Order allow,deny
        Allow from all
        LanguagePriority en es de fr
        ForceLanguagePriority Prefer Fallback
    </Directory>

#    ErrorDocument 400 /error/HTTP_BAD_REQUEST.html.var
#    ErrorDocument 401 /error/HTTP_UNAUTHORIZED.html.var
#    ErrorDocument 403 /error/HTTP_FORBIDDEN.html.var
#    ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
#    ErrorDocument 405 /error/HTTP_METHOD_NOT_ALLOWED.html.var
#    ErrorDocument 408 /error/HTTP_REQUEST_TIME_OUT.html.var
#    ErrorDocument 410 /error/HTTP_GONE.html.var
#    ErrorDocument 411 /error/HTTP_LENGTH_REQUIRED.html.var
#    ErrorDocument 412 /error/HTTP_PRECONDITION_FAILED.html.var
#    ErrorDocument 413 /error/HTTP_REQUEST_ENTITY_TOO_LARGE.html.var
#    ErrorDocument 414 /error/HTTP_REQUEST_URI_TOO_LARGE.html.var
#    ErrorDocument 415 /error/HTTP_UNSUPPORTED_MEDIA_TYPE.html.var
#    ErrorDocument 500 /error/HTTP_INTERNAL_SERVER_ERROR.html.var
#    ErrorDocument 501 /error/HTTP_NOT_IMPLEMENTED.html.var
#    ErrorDocument 502 /error/HTTP_BAD_GATEWAY.html.var
#    ErrorDocument 503 /error/HTTP_SERVICE_UNAVAILABLE.html.var
#    ErrorDocument 506 /error/HTTP_VARIANT_ALSO_VARIES.html.var

</IfModule>
```

```
</IfModule>

#
# The following directives modify normal HTTP response behavior to
# handle known problems with browser implementations.
#
BrowserMatch "Mozilla/2" nokeepalive
BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0
BrowserMatch "RealPlayer 4\.0" force-response-1.0
BrowserMatch "Java/1\.0" force-response-1.0
BrowserMatch "JDK/1\.0" force-response-1.0

#
# The following directive disables redirects on non-GET requests for
# a directory that does not include the trailing slash.  This fixes a
# problem with Microsoft WebFolders which does not appropriately handle
# redirects for folders with DAV methods.
# Same deal with Apple's DAV filesystem and Gnome VFS support for DAV.
#
BrowserMatch "Microsoft Data Access Internet Publishing Provider" redirect-
carefully
BrowserMatch "MS FrontPage" redirect-carefully
BrowserMatch "^WebDrive" redirect-carefully
BrowserMatch "^WebDAVFS/1.[0123]" redirect-carefully
BrowserMatch "^gnome-vfs/1.0" redirect-carefully
BrowserMatch "^XML Spy" redirect-carefully
BrowserMatch "^Dreamweaver-WebDAV-SCM1" redirect-carefully

#
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
# Change the ".example.com" to match your domain to enable.
#
#<Location /server-status>
#    SetHandler server-status
#    Order deny,allow
#    Deny from all
#    Allow from .example.com
#</Location>
<Location />
AddOutputFilterByType DEFLATE text/html text/plain text/css text/xml
application/x-javascript
</Location>

#
# Allow remote server configuration reports, with the URL of
#  http://servername/server-info (requires that mod_info.c be loaded).
# Change the ".example.com" to match your domain to enable.
#
#<Location /server-info>
#    SetHandler server-info
#    Order deny,allow
#    Deny from all
#    Allow from .example.com
#</Location>

#
```

```
# Proxy Server directives. Uncomment the following lines to
# enable the proxy server:
#
#<IfModule mod_proxy.c>
#ProxyRequests On
#
#<Proxy *>
#    Order deny,allow
#    Deny from all
#    Allow from .example.com
#</Proxy>

#
# Enable/disable the handling of HTTP/1.1 "Via:" headers.
# ("Full" adds the server version; "Block" removes all outgoing Via: headers)
# Set to one of: Off | On | Full | Block
#
#ProxyVia On

#
# To enable a cache of proxied content, uncomment the following lines.
# See http://httpd.apache.org/docs/2.2/mod/mod_cache.html for more details.
#
#<IfModule mod_disk_cache.c>
#   CacheEnable disk /
#   CacheRoot "/var/cache/mod_proxy"
#<IfModule>
#

#</IfModule>
# End of proxy directives.

### Section 3: Virtual Hosts
#
# VirtualHost: If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most configurations
# use only name-based virtual hosts so the server doesn't need to worry about
# IP addresses. This is indicated by the asterisks in the directives below.
#
# Please see the documentation at
# <URL:http://httpd.apache.org/docs-2.2/vhosts/>
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-S' to verify your virtual host
# configuration.

#
# Use name-based virtual hosting.
#

# Where do we put the lock and pif files?
LockFile "/var/lock/httpd.lock"
CoreDumpDirectory "/etc/httpd"

# Defaults for virtual hosts

# Logs
```

```
#
# Virtual hosts
#

# Virtual host Default Virtual Host
<VirtualHost *>
        ServerSignature email
        DirectoryIndex  index.php index.html index.htm index.shtml
        LogLevel  warn
        HostNameLookups off
</VirtualHost>

#
# Each directory to which Apache has access can be configured with respect
# to which services and features are allowed and/or disabled in that
# directory (and its subdirectories).
#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

<Directory "/">
        Options FollowSymLinks
        AllowOverride None
</Directory>

<Directory "/var/www/html">
        Options Indexes Includes FollowSymLinks
        AllowOverride None
        Allow from all
        Order allow,deny
</Directory>

<Directory "/var/www/icons">
        Options Indexes MultiViews
        AllowOverride None
        Allow from all
        Order allow,deny
</Directory>

<Directory "/var/www/cgi-bin">
        Options ExecCGI

        AllowOverride None
        Allow from all


        Order allow,deny
</Directory>
```