

Swarm Logic

Red Hat Enterprise Linux Vmware Template Build Standards

Prepared By



SWARM LOGIC

INFORMATION SECURITY EXPERTS

Security Classification - Public

Notice:

Copyright **Global Information Security Group P/L trading as Swarm Logic** 2010

This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/> or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

Table of Contents

1.0	DOCUMENT ADMINISTRATION	4
2.0	INTRODUCTION.....	5
2.1	OVERVIEW	5
2.2	STATEMENT OF WARRANTY.....	6
2.3	FEEDBACK	6
3.0	OPERATING SYSTEM INSTALLATION.....	7
3.1	CREATE THE VIRTUAL MACHINE	7
3.2	BASE OPERATING SYSTEM INSTALLATION	7
3.3	POST INSTALL CONFIGURATION	8
3.4	CLEAN UP NETWORK BOOT SCRIPTS.....	8
3.5	INSTALL VMWARE TOOLS.....	8
3.6	CONFIGURE NON-PRIVILEGED USERS	9
3.7	CONFIGURE SSHD	9
3.8	CONFIGURE RHN	9
3.9	INSTALL POSTFIX.....	9
3.10	REMOVE EXCESS PACKAGES.....	10
3.11	CONFIGURE LOG MANAGEMENT.....	10
3.12	ADDITIONAL HARDENING.....	10
3.13	CONFIGURE NTP	12
3.14	CONFIGURE SYSLOG	12
3.15	CONFIGURE FIREWALL	12
3.16	UPDATE SERVER	12
3.17	CONFIGURE AIDE.....	12
3.18	SECURE FILESYSTEMS.....	12
3.19	SECURE USER ACCOUNTS.....	13
3.20	CONFIGURE POSTFIX.....	13
4.0	APPENDICES.....	15
4.1	IPTABLES.....	15
4.2	USER ACCOUNT LOCKDOWN	15

1.0 DOCUMENT ADMINISTRATION

Document History

Version	Name	Changes	Date
1.0	Kurt Heinrich	Original	20/09/10

Distribution List

Version	Name	Issued To	Date

2.0 INTRODUCTION

2.1 OVERVIEW

This document is provided as a courtesy to the community. It is fairly succinct and assumes you are familiar with Vmware, Linux and template style builds.

It provides details of how to create a reasonably secure Vmware template suitable for VI4.

It is considered suitable for hosting services classified "Commercial in Confidence" or similar

It is designed to be used as a Vmware template and therefore provides minimal functionality, it is expected that additional services will be installed and configured in a secure manner.

It is assumed that the technical resource using this build guide to (re)construct the server is familiar with Linux installation procedures, is familiar with most common Linux administration tasks and has a good working knowledge of TCP/IP and network routing. As such detailed technical particulars regarding the reasoning for each step of the build procedure have not been included.

Hardware: Vmware Virtual Machine

Service Tag: N/A

CPU: 1

RAM: 2 GB Ram

Disk: 10 GB

Network: 1 x Gigabit Ethernet

O/S: RHEL 5.4 X64

Software Requirements

Red Hat Enterprise Linux 5.4 X64

These are typical parameters we use for lightly loaded servers. Adjust to suit your own circumstances if required.

This template has been tested on RHEL 5.4 and 5.5 however should work on most versions of RHEL.

This template also assumes you have detailed firewall rules hosted on a dedicated firewall as the iptables rules are relatively loose and only restrict access to a service based on destination port only

This template also assumes you have a central syslog server and an email account to forward all system emails to.

This template will have ssh as the only externally accessible service.

This template is derived from the NSA RHEL security guidelines, any questions regarding what specific commands do are available in that document.

The following are areas for improvement if additional security required;

- Tuning of iptables firewall based on source and destination addresses
- Modification of SELINUX into enforcing mode (SELINUX requires fairly specialist knowledge to maintain)
- AIDE can be configured to run as a cron job to ensure critical system files have not been tampered with
- NTP can be modified to use multiple trusted servers
- Can use LVM if required (we generally use a SAN to provide disk redundancy and performance)

This template is aimed to provide a sample basic build of RHEL suitable for general purpose services such as web or SQL services.

2.2 STATEMENT OF WARRANTY

THESE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT

2.3 FEEDBACK

We welcome your feedback at info@swarm-logic.com

3.0 OPERATING SYSTEM INSTALLATION

3.1 CREATE THE VIRTUAL MACHINE

- Open virtual centre
- Right click the Vmware host and select create new Virtual Machine
- Select typical
- Set the name as appropriate (RHEL__54_X64_Template or similar)
- Set the datastore as appropriate
- Set the operating system to Redhat Enterprise Linux 5 64 bit
- Set the hard disk size to 10GB
- Select thin provisioning
- Click edit virtual machine settings
- Set the memory to 2GB
- Set the number of processors to 1
- Click finish
- Either Connect the DVD to the ISO via a client device or datastore ISO image.
- Power on the virtual machine and open the console
- Depending on timing you may need to reboot the machine to pick up the DVD if it's attached as a client device.

3.2 BASE OPERATING SYSTEM INSTALLATION

- At the boot: prompt enter linux text and allow the server to boot
- Select 'Skip' to bypass the media test.
- Click 'Next' on the introduction screen to begin installation. Click the next button on the next screens after entering the settings outlined below.
- **Language Selection:** English
- **Keyboard Configuration:** U.S. English
- **Installation Number:** Select skip and acknowledge message
- Acknowledge the warning about the HDD being unreadable
- **Disk Partitioning Setup:** Select create custom layout
- Select and delete any existing partitions. Create the new partitions as follows.

Mount	Size	Format
swap	2047Mb	swap
/	4096Mb	ext3
/var	rest of disk	ext3
- **Boot Loader Configuration:** Accept default values. This will install GRUB as the default boot loader.
- **Network Configuration:**
 - Configure eth0? Click Yes.
 - Configure the following settings
 - Select Enable IPV4
 - Select Manual Address Conf

- Set the IP address as appropriate
- Set the hostname as appropriate, this should be the FQDN (host.example.com rather than just host)
- Set the default gateway as appropriate
- Set the DNS server address as appropriate
- Disable ipv6
- **Time Zone Selection:** Australia/Sydney
- **Set Root Password:** Set the root password
- **Package Installation Options:** Deselect all recommended package groups and select customise software selection
- **Package Group Selection:**
 - Deselect all except the following
 - Applications\Editors
 - Base System\Base
- Click next
- **About to Install:** Select Next to begin installation.
- The installation will now format the system and install the selected packages.
- Disconnect the client DVD device once prompted to reboot
- Re-boot the server when prompted. Click 'Reboot'.
- Login to the server as the root user to continue the configuration.

3.3 POST INSTALL CONFIGURATION

- Run the firewall configuration tool
- Enable the security Level (local iptables firewall)
- Enable SE linux in permissive mode
- Click OK
- Click exit

3.4 CLEAN UP NETWORK BOOT SCRIPTS

- Vi /etc/sysconfig/network-scripts/ifcfg-eth0
- Remove the line referencing a MAC address
- Save the file and reboot
- Confirm networking starts without errors

3.5 INSTALL VMWARE TOOLS

- Right click on the virtual machine and select install VMware tools
- mount /dev/cdrom /mnt
- cd /mnt
- rpm -i VMwaretools-4.xxxx.i386.rpm
- vmware-config-tools.pl
- Accept all the installation defaults
- umount /mnt
- reboot

3.6 CONFIGURE NON-PRIVILEGED USERS

- Add the required non-privileged users at the command prompt with the following commands;
useradd admin or as appropriate
- # passwd <username>
Changing password for user <username>.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
- Repeat the process to add additional users.

3.7 CONFIGURE SSHD

- Uncomment and modify the following SSH configuration options;
vi /etc/ssh/sshd_config
Port 22
Protocol 2
PermitRootLogin no
PermitEmptyPasswords no
X11Forwarding no
Banner /etc/issue
- # service sshd restart

3.8 CONFIGURE RHN

- rhn_register
- click next
- enter the username as appropriate
- enter the password as appropriate
- leave the profile as default, click next
- click next
- click next
- click next
- click OK once registered to confirm subscription
- click finish

3.9 INSTALL POSTFIX

- # yum install system-switch-mail
- Download as required
- # yum install postfix
- Download as required
- # system-switch-mail nox and select postfix
- Click OK
- Click finish
- Accept the GPG key

3.10 REMOVE EXCESS PACKAGES

- Remove the unwanted packages that are installed by default with the following command;
rpm -e <package name>
- Or # yum erase <package name> (follows dependencies)
Where <package name> is on of the following list;
- yum erase ppp autofs rdate rsh rdist sendmail mdadm acpid ipsec-tools wpa_supplicant bluez-gnome xorg-x11-xfs nss-tools desktop-file-utils bluez-libs jwhois rsync finger cups-libs net-snmp-libs stunnel ypbind quota smartmontools nfs-utils lftp audiofile flac nc xorg-x11-server-utils gphoto2 nss_ldap samba-common irda-utils busybox foomatic tftp-server docbook-dttds avahi cdrecord redhat-release-notes-5Server-29 talk nscd dhclient dhcpv6-client xinetd gnome-doc-utils xorg-x11-fonts-ISO8859-1-75dpi xorg-x11-xkb-utils mkisofs libX11 libXmu libXxf86vm libXcursor libXres libXdamage xorg-x11-font-utils libXfixes libXrandr libXt libXScrnSaver neon pango xorg-x11-utils hicolor-icon-theme xkeyboard-config gnome-mime-data xorg-x11-filesystem anacron

3.11 CONFIGURE LOG MANAGEMENT

- Edit /etc/logrotate.conf to rotate logs weekly and retain 26 weeks of compressed logs.

```
weekly
rotate 26
create
compress
```

3.12 ADDITIONAL HARDENING

- Modify /etc/issue to read
***** This service is for authorised clients only *****

* WARNING: It is a criminal offence to: *
* i. Obtain access to data without authority *
* (Penalty 2 years imprisonment) *
* ii Damage, delete, alter or insert data without authority *
* (Penalty 10 years imprisonment) *

- Update /etc/motd and /etc/issue.net to be the same as /etc/issue
- Modify /etc/default/useradd and change SHELL=/bin/bash to SHELL=/bin/nologin
- Remove all temporary files that were used during install
- Disable excess services

```
chkconfig atd off
chkconfig gpm off
chkconfig haldaemon off
chkconfig kudzu off
chkconfig mcstrans off
chkconfig setroubleshoot off
chkconfig readahead_early off
chkconfig ip6tables off
chkconfig lvm2-monitor off
chkconfig netfs off
chkconfig pcscd off
chkconfig portmap off
chkconfig rhnsd off
chkconfig yum-updatesd off
```

- view suid/guid/world writeable files
Find / -perm -4000 -ls > /root/suid-list
Find / -perm -2000 -user root -ls > /root/sgid-list
Find / -perm -0002 -type f -ls > /root/worldwriteable
- Check that none of these are a potential vulnerability
- Vi /etc/sysctl.conf, add the following lines

```
#Allow pings
net.ipv4.icmp_echo_ignore_all = 0

#Ignore broadcast pings
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

```
#TCP Syncookies
net.ipv4.tcp_syncookies = 1
```

```
#No ICMP redirect
net.ipv4.conf.all.accept_redirects = 0
```

```
#Enforce packet defragging
net.ipv4.ip_always_defrag = 1
```

```
#Bogus error message protection
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

```
#IP Spoof protection
net.ipv4.conf.all.rp_filter = 1
```

```
#Log Martians
net.ipv4.conf.all.log_martians = 1
```

```
#Increase maximum number of concurrent connections for iptables
net.ipv4.ip_conntrack_max = 65536
```

- # vi /etc/modprobe.conf

- Add the following lines above the vmware tools section
alias net-pf-10 off
alias ipv6 off

NB , Vmware tools may modify these lines if placed below the vmware tools section and re-enable IPV6

3.13 CONFIGURE NTP

- Yum install ntp
- Vi /etc/ntp.conf
- Remove the default servers and add the FQDN of your trusted NTP server as the only time server(s)
- Remove the references to ipv6 restriction lists
- Modify the default restrict line to read
- restrict default notrust kod nomodify notrap nopeer noquery
- Chkconfig –level 3 ntpd on
- Service ntpd start

3.14 CONFIGURE SYSLOG

- Vi /etc/syslog.conf
- Add the following lines
 - # copy everything to central server
 - *.* @192.168.1.200 (ie IP address of central syslog server)

3.15 CONFIGURE FIREWALL

- Vi /etc/sysconfig/iptables
- Edit the file as per the appendix

3.16 UPDATE SERVER

- Perform a yum update

3.17 CONFIGURE AIDE

- Yum install aide
- aide –init
- cp /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
- aide – check (confirm there are no errors)
- store a copy of the database file on another server

3.18 SECURE FILESYSTEMS

- Vi /etc/fstab
- For all additional partitions such as /var that are not root modify the file to include the following
- LABEL=/var /var ext3 defaults,nosuid,nodev,noexec 1 2
- Eg append after defaults ,nosuid,nodev,noexec
- This will reduce the risk of these filesystems being exploited maliciously
- Vi /etc/modprobe.conf and add the following lines above the vmware tools entries
 - install cramfs /bin/true
 - install freevxfs /bin/true
 - install jffs2 /bin/true
 - install hfs /bin/true
 - install hfsplus /bin/true
 - install squashfs /bin/true
 - install udf /bin/true
- This prevents these filesystems being used

3.19 SECURE USER ACCOUNTS

- Run the commands under the user account lockdown appendix to secure the system accounts
- Vi /etc/login.defs and modify the following parameters
 - PASS_MAX_DAYS 60
 - PASS_MIN_DAYS 7
 - PASS_MIN_LEN 8
 - PASS_WARN_AGE 7
- Enforce complex passwords
- Vi /etc/pam.d/system-auth
 - Locate the line password requisite pam_cracklib.so try_first_pass retry=3
 - And change it to
 - password requisite pam_passwdqc.so min=disabled,disabled,16,12,8
- Configure UMASK
 - Vi /etc/bashrc and change all instances of UMASK to UMASK 077

3.20 CONFIGURE POSTFIX

- Vi /etc/postfix/main.cf
 - Add the following lines
- ```
default_process_limit = 100
smtpd_client_connection_count_limit = 10
smtpd_client_connection_rate_limit = 30
queue_minfree = 20971520
header_size_limit = 51200
message_size_limit = 10485760
smtpd_recipient_limit = 100
```

smtpd\_banner = \$myhostname ESMTP

- configure roots email to be forwarded centrally
- vi /etc/aliases
- add the following line at the bottom of the file
  - root: admin@yourdomain.com
- save the file and run the command newaliases

### **3.21 CONFIGURE AS TEMPLATE**

- Shutdown the machine.
- Once its powered off right click and select convert to template

### **3.22 CREATE VMWARE CUSTOMISATION SPECIFICATION**

- Select management\customisation specifications manager
- Select new
- Set the operating system to Linux
- Set the name as appropriate eg RHEL\_54\_x64\_V1.0
- Set the description as appropriate
- Click next
- Select use the virtual machine name for the computer name
- Set the domain name as appropriate (eg domain suffix example.com)
- Set the location as appropriate and ensure the hardware clock is set to UTC
- For network select custom settings
- Set the general tab to prompt user for an IP address when the specification is used
- Set the subnet mask and default gateway as appropriate, click next
- Set the primary DNS as appropriate
- Set the DNS search path to be the same as the domain name you entered earlier
- Click finish

## 4.0 APPENDICES

### 4.1 IPTABLES

```
Firewall configuration written by system-config-securitylevel
Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j
ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j
ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

### 4.2 USER ACCOUNT LOCKDOWN

```
usermod -L bin
usermod -L daemon
usermod -L adm
usermod -L lp
usermod -L sync
usermod -L shutdown
usermod -L halt
usermod -L mail
usermod -L news
usermod -L uucp
usermod -L operator
usermod -L games
usermod -L gopher
usermod -L ftp
usermod -L nobody
usermod -L vcsa
usermod -L pcap
usermod -L rpc
usermod -L mailnull
usermod -L smmsp
usermod -L sshd
usermod -L dbus
```

```
usermod -L avahi
usermod -L haldaemon
usermod -L avahi-autoipd
usermod -L ntp
usermod -L xfs
usermod -L postfix
usermod -s /sbin/nologin bin
usermod -s /sbin/nologin daemon
usermod -s /sbin/nologin adm
usermod -s /sbin/nologin lp
usermod -s /sbin/nologin sync
usermod -s /sbin/nologin shutdown
usermod -s /sbin/nologin halt
usermod -s /sbin/nologin mail
usermod -s /sbin/nologin news
usermod -s /sbin/nologin uucp
usermod -s /sbin/nologin operator
usermod -s /sbin/nologin games
usermod -s /sbin/nologin gopher
usermod -s /sbin/nologin ftp
usermod -s /sbin/nologin nobody
usermod -s /sbin/nologin vcsa
usermod -s /sbin/nologin pcap
usermod -s /sbin/nologin rpc
usermod -s /sbin/nologin mailnull
usermod -s /sbin/nologin smmsp
usermod -s /sbin/nologin sshd
usermod -s /sbin/nologin dbus
usermod -s /sbin/nologin avahi
usermod -s /sbin/nologin haldaemon
usermod -s /sbin/nologin avahi-autoipd
usermod -s /sbin/nologin ntp
usermod -s /sbin/nologin xfs
usermod -s /sbin/nologin postfix
```