

CentOS Server - Installation

Basic Server Installation

- Server Install Checklist
 - Server Checklist
- Preparation
 - Server Image Installation
 - Add Additional Repositories
- System Update
 - Update With The Latest Update
 - Configure Automatic Updates
 - Configure Network Time Protocol (NTP)
- Process Hardening
 - Restrict Core Dumps
 - Enable Randomized Virtual Memory Region Placement
- OS Hardening
 - Remove Legacy Services
 - Disable Or Remove Server Services
- Firewall Configuration
 - Firewall Configuration
- Remote Administration Via SSH

- Set SSH protocol to 2
- Disable SSH root login
- Set SSH permitemptypasswords to no
- System Integrity and Intrusion Detection
 - Install And Configure Fail2Ban
 - Install and configure AIDE
- Anti-Virus Considerations
 - Install And Enable Anti-Virus Software
 - Configure Daily Scans

Server Install Checklist

Server Checklist

Server Checklist

Step	√	To Do
		Preparation
1		Install the server image
2		Add additional repositories
		System Update
3		Update with the latest updates
4		Configure automatic updates
5		Configure network time protocol (NTP)
		Process Hardening
6		Restrict core dumps
7		Enable randomized virtual memory region placement
		OS Hardening

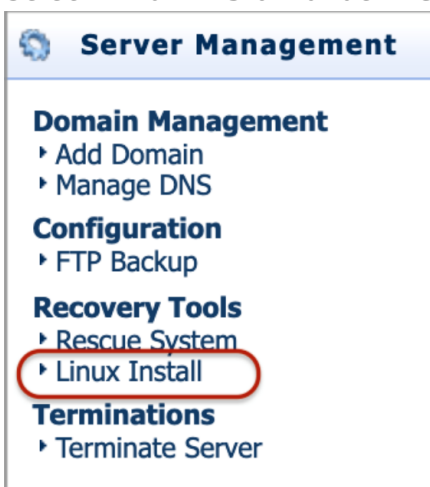
8		Remove legacy services (e.g., telnetserver; rsh, rlogin, rcp; ypserv, ypbind; tftp, tftp-server; talk, talkserver)
9		Disable or remove server services that are not going to be utilized (e.g. FTP, DNS, LDAP, SMB, DHCP, NFS, SNMP, etc.)
		Network Security and Firewall Configuration
10		Firewall Configuration
		Remote Administration Via SSH
11		Set SSH protocol to 2
12		Disable SSH root login
13		Set SSH permitemptypasswords to no
		System Integrity and Intrusion Detection
14		Install and configure Fail2Ban
15		Install and configure AIDE
		Anti-Virus Considerations
16		Install and enable anti-virus software
17		Configure daily scan

Preparation

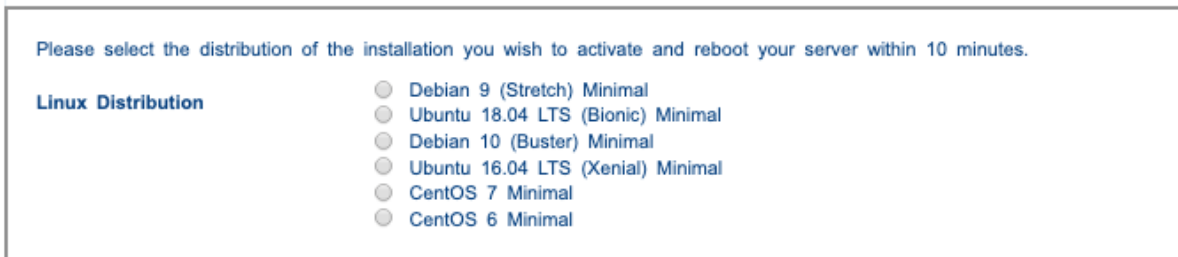
Server Image Installation

Server Image Installation

1. Browse to **konsoleH** and **log in** at Admin level
2. Select or search for your Self-Managed server in the **Hosting Service** tab
3. Select **Linux Install** under **Recovery Tools** from the left-hand menu



4. Select the distribution of the **installation** that you wish to activate



5. Select **Activate** on the top right-hand side
6. **Reboot** your server within 10 minutes via the RMM / IPMI device
7. During the server startup process, you have the option to reconfigure your RAID (TruServ Commerce only) via the RAID controller bios.
8. The server will boot into the OS installation environment you selected in step 4
9. Follow the onscreen prompts to install your OS and configure your disks and partition layout
10. Once the install is complete your server will reboot into your installed OS and will be accessible
11. Access your server with the user(s) configured via SSH (some Linux distributions do not allow root logins by default over SSH).

Add Additional Repositories

Install additional repositories

Additional Repositories

1. Using the commands below, install the Epel and PHP repositories:

```
yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm  
yum install http://rpms.remirepo.net/enterprise/remi-release-7.rpm
```

MySQL Repository

Replace MariaDB with MySQL

1. Navigate to <https://dev.mysql.com/downloads/repo/yum/>
2. Select the correct package corresponding to the version running on the server and click download.
3. Scroll down to 'No thanks, just start my download' and right click on the link.
4. Click 'Copy link address.'
5. Run the command below to install the MySQL repository.

```
yum localinstall 'link address copied from MySQL website'
```

Enable the correct release series

1. Manually edit the '/etc/yum.repos.d/mysql-community.repo' file with your favorite text editor.
2. Specify enabled=0 to disable a subrepository, or enabled=1 to enable a subrepository, see example below to enable MySQL 5.6 and disable MySQL 5.7 series.

```
# Enable to use MySQL 5.6 & Disabled MySQL 5.7  
[mysql56-community]  
name=MySQL 5.6 Community Serverbaseurl=http://repo.mysql.com/yum/mysql-5.6-
```

```
community/el/6/$basearch/  
enabled=1  
gpgcheck=1  
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-mysql  
[mysql57-community]  
name=MySQL 5.7 Community Serverbaseurl=http://repo.mysql.com/yum/mysql-5.7-  
community/el/6/$basearch/  
enabled=0  
gpgcheck=1gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
```

Note: When sub repositories for more than one release series are enabled, the latest series will be used by Yum.

System Update

Update With The Latest Update

Updating packages

1. Run the command below and press 'y' at the prompt. After the update has finished, restart the server.

```
yum update
```

Configure Automatic Updates

Setting Up Automatic Updates

Install yum-cron

1. Install yum-cron, the package that allows us to do automatic updates

```
yum -y install yum-cron
```

Configure yum-cron for auto-update

1. Edit the file /etc/yum/yum-cron.conf and change the options below

```
apply_updates = no
```

```
to
```

```
apply_updates = no
```

```
emit_via = stdio
```

```
to
```

```
emit_via = email
```

```
email_to =
```

```
to
```

```
email_to = sys admin email address
```

Verify that the service is running

1. Verify that the service is running with the command

```
systemctl status yum-cron.service
```

The output should look similar to

```
# /bin/systemctl status yum-cron.service
yum-cron.service - Run automatic yum updates as a cron job
   Loaded: loaded (/usr/lib/systemd/system/yum-cron.service; enabled)
   Active: active (exited) since sab 2014-08-09 00:37:16 CEST; 16h ago
   Process: 830 ExecStart=/bin/touch /var/lock/subsys/yum-cron (code=exited, status=0/SUCCESS)
   Main PID: 830 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/yum-cron.service
```

If the service is stopped, start it with the following command

```
systemctl start yum-cron.service
```

Configure Network Time Protocol (NTP)

Install NTP Daemon

1. Install NTPd with the following command

```
yum -y install ntp
```

Configure Firewall

1. Add NTP service to the 'allow' rules and reload the firewall to apply changes

```
firewall-cmd --add-service=ntp --permanent
```

```
firewall-cmd --reload
```

Edit ntp.conf File

1. Change/add the /etc/ntp.conf by removing current time servers and adding new time servers

Change from

```
# hetzner ntp servers
server ntp1.hetzner.de iburst
server ntp2.hetzner.com iburst
server ntp3.hetzner.net iburst
```

to

```
# hetzner ntp servers
```

```
# server ntp1.hetzner.de iburst
# server ntp2.hetzner.com iburst
# server ntp3.hetzner.net iburst
```

Add the following time servers

=====

```
server 0.pool.ntp.org
server 1.za.pool.ntp.org
server 2.africa.pool.ntp.org
```

Start And Check NTP service

1. Start NTP service and check to see if it is active

Start and enable NTPd

=====

```
systemctl start ntpd
systemctl enable ntpd
```

Check to see if service is enabled

=====

```
ntpq -p
```

Process Hardening

Restrict Core Dumps

Ensure core dumps are restricted

1. Edit the `/etc/security/limits.conf` and `/etc/sysctl.conf` files, adding the lines below

```
/etc/security/limits.conf
```

```
=====
```

```
* hard core 0
```

```
/etc/sysctl.conf
```

```
=====
```

```
fs.suid_dumpable = 0
```

Active kernel parameter

1. Active the kernel parameter by running the following command

```
sysctl -w fs.suid_dumpable=0
```

Enable Randomized Virtual Memory Region Placement

Randomized virtual memory region placement

1. Add the line below to the `/etc/sysctl.conf` file

```
kernel.randomize_va_space = 2
```

OS Hardening

Remove Legacy Services

The removal of legacy services

Check for legacy services

1. To check for legacy services, use the command the below

```
chkconfig --list
```

You should get an output similar to

```
Note: This output shows SysV services only and does not include native
systemd services. SysV configuration data might be overridden by native
systemd configuration.

If you want to list systemd services use 'systemctl list-unit-files'.
To see services enabled on particular target use
'systemctl list-dependencies [target]'.

netconsole    0:off  1:off  2:off  3:off  4:off  5:off  6:off
network       0:off  1:off  2:on   3:on   4:on   5:on   6:off
```

Disable legacy services

1. Confirm the necessity of the service and disable if not necessary with the below command

```
chkconfig "service name" off
```

I.e to disable netconsole

```
=====
```

```
chkconfig netconsole off
```

Disable Or Remove Server Services

Disable or remove server services that are not going to be utilized (e.g. FTP, DNS, LDAP, SMB, DHCP, NFS, SNMP, etc.)

Display a list of services available

1. To display a list of services available use the command the below

```
systemctl -t service
```

This will display something similar to

UNIT	LOAD	ACTIVE	SUB	DESCRIPTION
auditd.service	loaded	active	running	Security Auditing Service
clamd@scan.service	loaded	active	running	clamd scanner (scan) daemon
crond.service	loaded	active	running	Command Scheduler
dbus.service	loaded	active	running	D-Bus System Message Bus
fail2ban.service	loaded	active	running	Fail2Ban Service
firewalld.service	loaded	active	running	firewalld - dynamic firewall daemon
getty@tty1.service	loaded	active	running	Getty on tty1
httpd.service	loaded	active	running	The Apache HTTP Server
irqbalance.service	loaded	active	running	irqbalance daemon

Disable unnecessary services

1. Stop and turn OFF auto-start services not needed

```
systemctl stop "service name"
systemctl disable "service name"
```

I.e. to stop and disable the Postfix service

=====

```
systemctl stop postfix
```

```
systemctl disable postfix
```

Firewall Configuration

Firewall Configuration

Configuring The Firewall

Start and enable the firewall

1. To start and enable the firewall use the commands below

```
systemctl start firewalld  
systemctl enable firewalld
```

Get an overview

Default Zone

1. Find the default zone. The default zone is usually public

```
firewall-cmd --get-default-zone
```

```
root@aza2-jhb-azandi /home/aza_admin # firewall-cmd --get-default-zone  
public  
root@aza2-jhb-azandi /home/aza_admin #
```

Display Allowed Services

1. Display the allowed services of the zone

```
firewall-cmd --list-service --zone=external
```

By default, "public" zone is applied with a NIC and dhcpv6-client and ssh are allowed.

```
root@aza2-jhb-azandi /home/aza_admin # firewall-cmd --list-service --zone=public  
dhcpv6-client http https ssh  
root@aza2-jhb-azandi /home/aza_admin #
```

Display Services Defined By Default

1. To list all service defined by default use the command below

```
firewall-cmd --get-services
```

It should give you an output similar to

```
[root@dlp ~]# firewall-cmd --get-services
amanda-client bacula bacula-client dhcp dhcpv6 dhcpv6-client dns ftp high-availability http https imaps ipp
ipp-client ipsec kerberos kpasswd ldap ldaps libvirt libvirt-tls mdns mountd ms-wbt mysql nfs ntp openvpn
pmcd pmproxy pmwebapi pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba samba-client smtp ssh
telnet tftp tftp-client transmission-client vnc-server wbem-https
```

Add/Remove services

1. Add or Remove allowed services. The change will be back after rebooting the system. If you change settings permanently, add the "--permanent" option.

```
# for example, add http (the change will be valid at once)
[root@dlp ~]# firewall-cmd --add-service=http
success
[root@dlp ~]# firewall-cmd --list-service
dhcpv6-client http ssh

# for example, remove http
[root@dlp ~]# firewall-cmd --remove-service=http
success
[root@dlp ~]# firewall-cmd --list-service
dhcpv6-client ssh

# for example, add http permanently. (this permanent case, it's necessary to reload the Firewallld to enable the change)
[root@dlp ~]# firewall-cmd --add-service=http --permanent
success
[root@dlp ~]# firewall-cmd --reload
success
[root@dlp ~]# firewall-cmd --list-service
dhcpv6-client http ssh
```

Add/Remove Ports

1. Add or remove allowed ports

```
# for example, add TCP 465
[root@dlp ~]# firewall-cmd --add-port=465/tcp
success
[root@dlp ~]# firewall-cmd --list-port
465/tcp

# for example, remove TCP 465
[root@dlp ~]# firewall-cmd --remove-port=465/tcp
success
[root@dlp ~]# firewall-cmd --list-port

# for example, add TCP 465 permanently
[root@dlp ~]# firewall-cmd --add-port=465/tcp --permanent
success
[root@dlp ~]# firewall-cmd --reload
success
[root@dlp ~]# firewall-cmd --list-port
465/tcp
```

Add/Remove Prohibited ICMP Types

1. Add or remove prohibited ICMP types

```
# for example, add echo-request to prohibit it
[root@dlp ~]# firewall-cmd --add-icmp-block=echo-request
success
[root@dlp ~]# firewall-cmd --list-icmp-blocks
echo-request

# for example, remove echo-request
[root@dlp ~]# firewall-cmd --remove-icmp-block=echo-request
success
[root@dlp ~]# firewall-cmd --list-icmp-blocks

# display ICMP types
[root@dlp ~]# firewall-cmd --get-icmptypes
destination-unreachable echo-reply echo-request parameter-problem redirect
router-advertisement router-solicitation source-quench time-exceeded
```

Remote Administration Via SSH

Set SSH protocol to 2

Set SSH protocol to 2

SSH has two protocols it may use, protocol 1 and protocol 2. The older protocol 1 is less secure and should be disabled unless you know that you specifically require it.

1. Open the sshd config

```
vi /etc/ssh/sshd_config
```

2. Add or amend as shown below

```
# Protocol 2,1  
Protocol 2
```

3. Restart the sshd service

```
systemctl restart sshd.service
```

Disable SSH root login

Disabling root login via SSH

Disabling SSH root login will add an extra layer of security. It would be more secure to brute force attacks or in case your password is stolen.

1. Create a non-root user

```
adduser username  
passwd username
```

2. Open the ssh configuration file with your editor.

```
vi /etc/ssh/sshd_config
```

3. Add the line "PermitRootLogin no." Or uncomment the line "#PermitRootLogin yes" and change yes to no.

```
#LoginGraceTime 2m  
#PermitRootLogin yes  
#StrictModes yes  
#MaxAuthTries 6  
#MaxSessions 10  
PermitRootLogin no
```

4. Save and exit the file.
5. Restart the ssh service

```
systemctl restart sshd.service
```

Set SSH peremptypasswords to no

Set SSH peremptypasswords to no

1. Open the ssh configuration file with your editor.

```
vi /etc/ssh/sshd_config
```

2. Add or amend as shown below

```
PermitEmptyPasswords no
```

3. Restart the sshd service

```
systemctl restart sshd.service
```

System Integrity and Intrusion Detection

Install And Configure Fail2Ban

Installation

1. Run the command below to install Fail2Ban

```
yum install fail2ban fail2ban-systemd
```

Configuration

1. Copy the "jail.conf" file and re-save it with the name "jail.local"

```
cp -pf /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

2. Edit the jail.local and add your local IP address onto the **ignoreip** line

```
[ DEFAULT ]
```

```
# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will not
# ban a host which matches an address in this list. Several addresses can be
# defined using space separator.
```

```
ignoreip = 127.0.0.1
```

```
# Override /etc/fail2ban/jail.d/00-firewalld.conf:
```

```
banaction = iptables-multiport
```

```
# "bantime" is the number of seconds that a host is banned.
```

```
bantime = 600
```

```
# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
```

```
findtime = 600
```

```
# "maxretry" is the number of failures before a host get banned.  
maxretry = 5
```

Add a jail file to protect SSH access

1. Create a new file called sshd.local

```
| touch /etc/fail2ban/jail.d/sshd.local && chmod +x /etc/fail2ban/jail.d/sshd.local |
```

2. Edit the file and add the lines below

```
vi /etc/fail2ban/jail.d/sshd.local
```

Add these lines to the file

```
=====
```

```
[sshd]  
enabled = true  
port = ssh  
#action = firewallcmd-ipset  
logpath = %(sshd_log)s  
maxretry = 5  
bantime = 86400
```

Enable and start the FAIL2BAN service

1. Run the following commands to enable and start the Fail2Ban service

```
systemctl enable fail2ban  
systemctl start fail2ban
```

Install and configure AIDE

Install and configure Host Based IDS (Intrusion Detection System) "AIDE"

1. Install AIDE

```
yum -y install aide
```

2. Configure AIDE and initialize database. It's possible to use AIDE with default config but if you'd like to customize settings, change configuration file like follows. Setting rules are written near 26-84 lines, refer to them.

```
[root@dlp ~]# vi /etc/aide.conf

# for example, change setting of monitoring /var/log
/var/log    p+u+g+i+n+acl+selinux+xattrs

# initialize database
[root@dlp ~]# aide --init

AIDE, version 0.15.1

### AIDE database at /var/lib/aide/aide.db.new.gz initialized.

# copy generated DB to master DB
[root@dlp ~]# cp -p /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

3. Execute checking

```
[root@dlp ~]# aide --check

# if there is no unmatched, it displays "Okay"

AIDE, version 0.15.1

### All files match AIDE database. Looks okay!

# try to change a file and check again
[root@dlp ~]# chmod 640 /root/anaconda-ks.cfg
[root@dlp ~]# aide --check

# detected differences like follows
```

AIDE 0.15.1 found differences between database and filesystem!!

Start timestamp: 2015-06-17 19:55:20

Summary:

Total number of files:	39039
Added files:	0
Removed files:	0
Changed files:	1

Changed files:

changed: /root/anaconda-ks.cfg

Detailed information about changes:

File: /root/anaconda-ks.cfg

Perm	: -rw-----	, -rw-r-----
Ctime	: 2015-05-24 02:22:04	, 2015-06-19 11:55:15
ACL	: old = A:	

user::rw-
group:---
other:---

D: <NONE>
new = A:

user::rw-
group:r--
other:---

D: <NONE>

Update AIDE database

1. If there is no problem even if some differences are detected, then update database like follows

```
[root@dlp ~]# aide --update
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2015-06-17 19:56:31

Summary:
  Total number of files:      39039
  Added files:                0
  Removed files:              0
  Changed files:              1

-----
Changed files:
-----

changed: /root/anaconda-ks.cfg
.....
.....

# update database
[root@dlp ~]# cp -p /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

Add Cron job and email logs

1. Add in Cron if check regularly. Log file [/var/log/aide/aide.log] is updated every time and if there is no difference, it is updated with zero byte, so if you's like to save log files, it needs to create a shell script or send results via email or others

```
# for example, add daily check in Crontab and send results via email

[root@dlp ~]# vi /etc/cron.d/aide
00 01 * * * /usr/sbin/aide --update | mail -s 'Daily Check by AIDE' root
```

Anti-Virus Considerations

Install And Enable Anti-Virus Software

Clamav installation

Preparation for ClamAV installation

1. Ensure that the EPEL repository has been installed

```
yum -y install epel-release
```

```
yum clean all
```

ClamAV installation

1. Run the command below to install ClamAV

```
yum -y install clamav-server clamav-data clamav-update clamav-filesystem clamav clamav-scanner-systemd clamav-devel clamav-lib clamav-server-systemd
```

Configuring ClamAV

1. Remove "Example" string from the configuration file

```
sed -i -e "s/^Example/#Example/" /etc/clamd.d/scan.conf
```

2. Edit scan.conf

```
Open scan.conf for editing
```

```
=====
```

```
vi /etc/clamd.d/scan.conf
```

Look for and the change line from

```
=====
```

```
#LocalSocket /var/run/clamd.scan/clamd.sock
```

to

```
LocalSocket /var/run/clamd.scan/clamd.sock
```

Configure FreshClam

1. Remove "Example" string from ClamAV's freshclam update engine configuration file

```
sed -i -e "s/^Example/#Example/" /etc/freshclam.conf
```

2. Run the virus definition database update

```
freshclam
```

Start and enable Clamd services

1. Use the following commands to start and enable Clamd services

```
systemctl start clamd@scan
```

```
systemctl enable clamd@scan
```

Configure Daily Scans

Configure ClamAV for daily scans

1. Create and edit the file `clamscan_daily` in the folder `/etc/cron.daily`

```
Create clamscan_daily
=====

vi /etc/cron.daily

=====

Add below to file changing the option

EMAIL_FROM="from email address";
EMAIL_TO="to email address";
DIRTOSCAN="list of directories";

as required
=====

#!/bin/bash
LOGFILE="/var/log/clamav/clamav-$(date +%Y-%m-%d).log";
EMAIL_MSG="Please see the log file attached.";
EMAIL_FROM="from email address";
EMAIL_TO="to email address";
DIRTOSCAN="list of directories";

for S in ${DIRTOSCAN}; do
    DIRSIZE=$(du -sh "$S" 2>/dev/null | cut -f1);

    echo "Starting a daily scan of \"$S\" directory.
    Amount of data to be scanned is \"$DIRSIZE\".";

    clamscan -ri "$S" >> "$LOGFILE";
```

```
# get the value of "Infected lines"
MALWARE=$(tail "$LOGFILE"| grep Infected| cut -d" " -f3);

# if the value is not equal to zero, send an email with the log file attached
if [ "$MALWARE" -ne "0" ];then
# using heirloom-mailx below
echo "$EMAIL_MSG"| mail -a "$LOGFILE" -s "Malware Found" -r "$EMAIL_FROM" "$EMAIL_TO";
fi
done

exit 0
```