**AMI build and OS Hardening**

CENTOS 7

|  |  |
| --- | --- |
| Version | Version-2.0 |
| Date | 31-OCT-2017 |
| Status | Revised / Approval |
| Owner | Sandeep Ravipati |
|  |  |
|  |  |

Table of Contents

[1 Introduction 3](#_Toc163282787)

[1.1 Purpose 3](#_Toc163282788)

[1.2 Glossary 3](#_Toc163282789)

[2 “AMI build out and hardening- Linux Servers” 3](#_Toc163282790)

2.1 NOTE Further Changes / Modifications 4

[References](#_Toc163282791) 4

Introduction

## Purpose

To have a better hardening Rules on Tightening OS Level Security Rules to make the Environment robust and stable avoiding any Fixes.

## Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| OS Hardening | To make the AWS Infra / Servers more secure & Robust with OS Rules. |

# “Real Content”

**Introduction:**

This document helps you to understand the process which CIS team will follow for hardening a Linux server.

**Scope:**

The scope is only limited to CIS Team.

**AMI Details:**

|  |  |  |  |
| --- | --- | --- | --- |
| **AMI ID** | **OS Version Details** | **Virtualization Type** | **Provider** |
| **ami-d099aec6** | CENTOS 7 | HVM | OPEN Source / Shared Support Services |
| NONE | RHEL 7 | HVM | Redhat, INC |

**Process:**

1. Servers should be launched in Respective Public & Private subnets. and have the internet access through Internet & NAT Gateways surpass the Traffic 🡪 allowing only 80 and 443 to 0.0.0.0/0 outbound as Default
2. Resize the root partition to 30GB, because Amazon by default comes with 5/10GB of root partition size which will not be sufficient
3. Perform the OS Patch update from the Yum Updates before creating the base Image
   1. To install the plugin run: yum install yum-security
   2. To list all updates that are security relevant, and get a return code on whether there are security updates use: yum --security check-update
   3. To apply updates that are security relevant use: yum --security update
4. Disable the SSH protocol version 1 from the ssh configuration.

# The default requires explicit activation of protocol 1

Protocol 2 (Uncomment Protocol 2 /etc/sshd/sshd\_config)

* 1. service sshd restart
  2. service sshd status

1. Verify & Update the D2A DNS Server settings : /etc/resolv.conf; By default, VPC instances will take the DNS settings from the VPC DHCP Option Sets, make sure that your DHCP Options entries are correctly configured.

Cat /etc/resolv.conf

# Generated by NetworkManager

Search ec2.internal

nameserver 10.158.32.2

1. Uninstall the unused/unnecessary services if any.

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep auth

authconfig-6.2.8-30.el7.x86\_64

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep nis

libunistring-0.9.3-9.el7.x86\_64

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep nfs

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep smb

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep nmb

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep ypserv

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep tux

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep postgres

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep firewalled

https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/6/html/security\_guide/sect-security\_guide-server\_security-disable-source-routing

sysctl net.ipv4.conf.all.accept\_source\_route

1. Install and Enable the sysstat package for System Activity Report

(https://www.itadminstrator.com/2016/12/how-to-install-and-configure-sysstat.html)

* 1. yum list installed sysstat
  2. yum install sysstat -y -q && yum list installed sysstat -q
  3. systemctl enable sysstat
  4. systemctl start sysstat && systemctl status sysstat -l

1. Install and Enable the psacct which will help us monitoring the user activities reports

Enable/disable/start/stop process accounting (psacct)

* 1. yum install psacct -y
  2. sudo service psacct start
  3. sudo service psacct status
  4. ac -d (Display the statistics for total login time)

1. Disable any xinetd services you do not absolutely require by setting "disable=yes" in /etc/xinetd.d/\*. : sudo service xinetd stop; sudo chkconfig xinetd off

To verify pass -1 and -2

core@ip-10-158-35-146 ~ $ ssh -i att\_staging.pem -1 ec2-user@10.158.39.154

Protocol major versions differ: 1 vs. 2

core@ip-10-158-35-146 ~ $ ssh -i att\_staging.pem -2 ec2-user@10.158.39.154

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* SSH D2A Security \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Last login: Thu Jun 21 13:46:19 2018 from ip-10-158-35-146.ec2.internal

1. Use netstat -tunlp command to check what network services are running/listening, stop the unused services using service and chkconfig commands.

Below services are running, Is there any unused service ?

[root@ip-10-158-39-154 xinetd.d]# netstat -tunlp

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 15069/sshd

tcp 0 0 127.0.0.1:25 0.0.0.0:\* LISTEN 1662/master

tcp6 0 0 :::22 :::\* LISTEN 15069/sshd

tcp6 0 0 ::1:25 :::\* LISTEN 1662/master

udp 0 0 0.0.0.0:32541 0.0.0.0:\* 557/dhclient

udp 0 0 0.0.0.0:68 0.0.0.0:\* 557/dhclient

udp 0 0 127.0.0.1:323 0.0.0.0:\* 516/chronyd

udp6 0 0 ::1:323 :::\* 516/chronyd

udp6 0 0 :::45235 :::\* 557/dhclient

1. Enable the Auto Service Start for: SSH, Network.

If you want the daemon to start automatically at the boot time, type:

* 1. chkconfig sshd on

1. Display SSH D2A Security Warning Banner before login: Use the /etc/motd or

/etc/ssh/sshd\_config file Banner field.

Uncomment banner /etc/issue in /etc/ssh/sshd\_config

Write the banner in the file /etc/issue

sudo /etc/init.d/ssh restart

Logout and login again to see the message

core@ip-10-158-35-146 ~ $ ssh -i att\_staging.pem ec2-user@10.158.39.154

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* SSH D2A Security \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. Change the parameters in /etc/sysctl.conf for kernel hardening.
   1. Enable TCP SYN Cookie Protection - net.ipv4.tcp\_syncookies = 1
   2. Disable IP Source Routing - net.ipv4.conf.all.accept\_source\_route = 0
   3. Disable **ICMP Redirect** Acceptance - net.ipv4.conf.all.accept\_redirects = 0
   4. Enable IP Spoofing Protection - net.ipv4.conf.all.rp\_filter = 1
   5. Enable Ignoring Broadcasts Request - net.ipv4.icmp\_echo\_ignore\_broadcasts = 1
   6. Enable Logging of Spoofed **Packets, Source** Routed Packets, Redirect Packets - net.ipv4.conf.all.log\_martians = 1

To reload the vaules run below command

sysctl –system

and cross verify using below commands

[root@ip-10-158-39-154 ec2-user]# sysctl -a | grep net.ipv4.tcp\_syncookies

net.ipv4.tcp\_syncookies = 1

[root@ip-10-158-39-154 ec2-user]# sysctl -a | grep net.ipv4.conf.all.accept\_source\_route

net.ipv4.conf.all.accept\_source\_route = 0

[root@ip-10-158-39-154 ec2-user]# sysctl -a | grep net.ipv4.conf.all.accept\_redirects

net.ipv4.conf.all.accept\_redirects = 0

[root@ip-10-158-39-154 ec2-user]# sysctl -a | grep net.ipv4.conf.all.rp\_filter

net.ipv4.conf.all.rp\_filter = 1

[root@ip-10-158-39-154 ec2-user]# sysctl -a | net.ipv4.icmp\_echo\_ignore\_broadcasts

bash: net.ipv4.icmp\_echo\_ignore\_broadcasts: command not found

[root@ip-10-158-39-154 ec2-user]# sysctl -a | grep net.ipv4.icmp\_echo\_ignore\_broadcasts

net.ipv4.icmp\_echo\_ignore\_broadcasts = 1

[root@ip-10-158-39-154 ec2-user]# sysctl -a | grep net.ipv4.conf.all.log\_martians

net.ipv4.conf.all.log\_martians = 1

1. Enable the telnet and traceroute tools for connectivity check with other hosts

yum install telnet-server telnet

systemctl start telnet.socket

systemctl enable telnet.socket

*Created symlink from /etc/systemd/system/sockets.target.wants/telnet.socket to /usr/lib/systemd/system/telnet.socket.*

systemctl status telnet.socket

*telnet.socket - Telnet Server Activation Socket*

*Loaded: loaded (/usr/lib/systemd/system/telnet.socket; enabled; vendor preset: disabled)*

*Active: active (listening) since Thu 2018-06-21 07:33:47 EDT; 26s ago*

For traceroute

yum install traceroute -y

which traceroute

1. Make sure /var/log/wtmp file exists to record the login/logout of the users and server reboots, if not create one with the touch command : touch /var/log/wtmp

ls /var/log/wtmp

/var/log/wtmp

1. Increase ulimit open files to 65536

No changes done.

***[Thomas, Shanthi] I will leave it as default for now. It is recommended to reduce it to reduce possibilities of a DOS attack at the OS level. But changing it without proper studying of apps can be disastrous***

1. Ensure that your AMI does not include any general user accounts without passwords or user accounts with default passwords.
2. Remove all the default sudoers details except for root user

I’d emove ec2-user and %wheel from this file.

1. Make sure no AWS Keys are placed in it.
2. Clean up all the SSH Access Keys from the system
3. Clean up the /tmp and any application, customer data in any other directories
4. Remove any custom users created as part of the AMI
5. Change the Time zone of the base Instance to EST time zone

No changes done

[ec2-user@ip-10-158-39-154 etc]$ date

Thu Jun 21 09:01:20 EDT 2018

***[Thomas, Shanthi]*** Thi sis a don’t care – really not part of hardening.

1. Clean up the bash history
2. Take clean AMI backup with the Reboot option enabled
3. Manage the AMIs accordingly as per the guidelines mentioned in the AMI management process. (This we will share separately)

## NOTE:

**IAM & Further Deep Dive Modifications**

1. Have enabled a separate LVM Partition for /home   
   🡪 To Encrypt user’s data & move them to S3 location as backup.
2. PORT Restriction will be done from Security Group on AWS  
   🡪 AWS [EC2 instance] & IP Tables at OS Level.
3. All Services [rlogin, SMTP, ypbind, vsftpd, httpd, Postgress, Docker, nfs & other]   
   🡪 will not be running and not installed by default.
4. ACL is based on requirement, Group Permissions & Sudo need to categorize based on   
   usage & requirements used by team [who all will access the servers]

# References

|  |  |
| --- | --- |
| **[1]** |  |
| [2] |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Change History** | | | | |
| **Version** | **Date** | **Change from Previous** | **Name** | **Status** |
| 2.0 |  | Document Revised | Sandeep Ravipati | Approved |