LAMBDATAGGING

[AutomateMandatoryTag.py](https://onedrive.live.com/embed?resid=8751035A609F4B69%21984&filename=AutomateMandatoryTag.py&authkey=!AJRU6Mc092bmdQI)

[Class-event-test.json](https://onedrive.live.com/embed?resid=8751035A609F4B69%21985&filename=Class-event-test.json&authkey=!AJytgkNiFb0Go9c)

[auto-update-ec2-ebs.py](https://onedrive.live.com/embed?resid=8751035A609F4B69%21987&filename=auto-update-ec2-ebs.py&authkey=!AMKzBMgi0SDv44s)

**Break the root password and set a new root password to Linux**

There are multiple ways to reset a root password on a Linux machine. In this

scenario, we are going to assume that the best way to reset the password is to

interrupt the boot process, move into the "emergency mode" and force a reset of

the root password

Interrupt the boot process to gain access to the system and reset the root password. Hint: You need to edit through the GRUB menu.

1. Start or reboot a system to get into the boot menu.

2. Press any key to stop the auto selection of a menu item.

3. Ensure the kernel you intend to boot into is highlighted and press the E key to edit the entry.

4. Navigate to the "linux16" kernel line and hit the End key to go to the end of the line.

5. Append rd.break enforcing=0 to the linux16 kernel line.

6. Hit Ctrl + X to continue.

7. The system boots into an emergency mode that has the /sysroot directory mounted as read only.

8. Mount the /sysroot directory with read and write permissions.

#mount –o remount, rw /sysroot

9. Switch into chroot jail and set the /sysroot as the root file system.

#chroot /sysroot

10. Reset the root password.

#passwd root

11. Clean up. Make sure that all unlabled files get relabeled during the boot process for SELinux.

#touch /.autorelabel

12. Exit chroot jail.

#exit

13. Exit the initramfs debug shell.

#exit

**Troubleshooting Notes**

If the password did not change after reboot:

The touch /.autorelabel command was missed or performed incorrectly.

The file system was not mounted as read/write so the changes made were not

persistent.

**Network/Hostname Question**

#hostnamectl set-hostname station.domain11.example.com

#nmcli connection modify eno16777736 ipv4.method manual

#nmcli connection modify eno16777736 ipv4.addresses '172.24.11.10/24 172.24.11.254' #nmcli connection modify eno16777736 ipv4.dns '172.24.11.250' nmcli connection up eno16777736

#nmcli con show eno16777736 | grep ipv4 host server.domain11.example.com

#route -n

**Selinux Question**

Configure SELinux to make it work in enforcing mode

getenforce // view mode

setenforce 1 // set to enforcing mode

vim /etc/selinux/config // permanent modification

selinux=enforcing

:wq

Restart

Then use the sestatus to view

1.Configure a default software repository for your system One YUM has already provided to configure your system on <http://server.domain11.example.com/pub/x86_64/Server>, and can be used normally.

Solutions:

#yum-config-manager --add-repo=http://content.example.com/rhel7.0/x86-64/dvd” is to generate a file vim content.example.com\_rhel7.0\_x86\_64\_dvd.repo,

Add a line gpgcheck=0

#yum clean all

#yum repolist

Almost 4305 packages are right, Wrong Yum Configuration will lead to some following questions cannot be worked out.

2.Adjust the size of the Logical Volume

Adjust the size of the vo Logical Volume, its file system size should be 290M. Make sure that the content of this system is complete. Note: the partition size is rarely accurate to the same size as required, so in the range 270M to 320M is acceptable.

Solution One:

Addition

# df -hT

#lvextend -L +100M /dev/vg0/vo

#Lvscan

#xfs\_growfs /home/

//home is the mounted directory of the LVM,

this step just need to do in the practice environment, and test EXT4 does not need this step.

#resize2fs /dev/vg0/vo

// use this command to update in examination.

#df -hT

Solution Two:

Subtraction

#e2fsck -f /dev/vg0/vo

#umount /home

#resize2fs /dev/vg0/vo

// the final required partition capacity is 100M

#lvreduce -l 100M /dev/vg0/vo

#mount /dev/vg0/vo /home

#df -hT

3.Create User Account

Create the following users, group and group membership:

Adminuser group

User natasha, using adminuser as a sub group

User Harry, also using adminuser as a sub group

User sarah, cannot access the SHELL which is interactive in the system, and is not a member of adminuser,

natasha, Harry, sarah password is redhat.

Solutions:

#groupadd adminuser

#useradd natasha -G adminuser

#useradd Harry -G adminuser

#useradd sarah -s /sbin/nologin

#Passwd user name // to modify password or echo redhat | passwd --stdin user name id natasha

// to view user group.

4.Configure /var/tmp/fstab Permission:

Configure /var/tmp/fstab permission

Copy the file /etc/fstab to /var/tmp/fstab. Configure /var/tmp/fstab permissions as the following:

Owner of the file /var/tmp/fstab is Root, belongs to group root.

File /var/tmp/fstab cannot be executed by any user

User natasha can read and write /var/tmp/fstab

User Harry cannot read and write /var/tmp/fstab

All other users (present and future) can read /var/tmp/fstab

#cp /etc/fstab /var/tmp/fstab

#chown root:root /var/tmp/fstab

#chmod –x /var/tmp/fstab

#setfacl –m u:natasha:rw /var/tmp/fstab

#setfacl –m u:Harry:--- /var/tmp/fstab

#setfacl –m d:u:o:r-- /var/tmp/

#getfacl /var/tmp/fstab

5. Configure a cron Task

User natasha must configure a cron job, local time 14:23 runs and executes: \*/bin/echo hiya every day.

#crontab -e -u natasha

23 14 \* \* \* /bin/echo hiya

#crontab -l -u natasha // View

#Systemctl enable crond

#Systemcdl restart crond

6. Create a Shared Directory Create a shared directory /home/admins, make it has the following characteristics: /home/admins belong to group adminuser

This directory can be read and written by members of group adminuser

Any files created in /home/ admin, group automatically set as adminuser.

Solutions:

#mkdir /home/admins

#chgrp -R adminuser /home/admins

#chmod g+w /home/admins

#chmod g+s /home/admins

1. Change the current hostname to station1.mydomain.com

To complete the proceeding task, you need to perform the following steps

a. Execute the following command to change the hostname

#hostnamectl set-hotsname station1.mydomain.com

b. Execute the following command to verify that the new hostname has been set #hostname

1. Complete the following user and group management tasks:

• Create a directory named /SalesDocs

• Allow Peter and Constance user accounts to share documents in the /SalesDocs directory using a group named sales.

• Both the users can read, write, and remove each other’s documents in this directory.

• Users that are not members of the sales group cannot access the documents of the /SalesDocs directory

To complete the preceding tasks, you need to perform the following steps:

a. Run the following command to create the directory named /SalesDocs

 #mkdir /SalesDocs

b. Execute the following command to create the group named sales.

 #groupadd sales

c. Run the following the command to set the group membership on /SalesDocs directory #chgrp sales /SalesDocs

d. Execute the following command to set the permission for the /SalesDocs directory #chmod 2770 /SalesDocs

e. Run the following commands to add Peter and Constance user accounts to sales group #usermod –aG sales Peter #usermod –aG sales Constance

f. Run the following command to verify the group permissions.

#ll /

1. Create a cron job with the following conditions:

• Should run as root user

• Should start at 10:07PM every day

• Should write a report of the daily system resource consumption under the /var/log/syreport1.log file

To complete this task, you need to perform the following steps:

a. Execute the following command to edit or add a cron job

 #crontab –e

Note: Add the following line:

07 22 \* \* \* /usr/bin/sar –A > /var/log/syreport1.log

b. Execute the following command to restart the crond service

 #systemctl restart crond

c. Execute the following commands to list the cron jobs:

#crontab –l

1. Create user David with UID 500 and set password as Pa55word.

#useradd -u 500 David

#passwd David

1. Extend the swap space with 500 MB , don’t remove the existing swap. It should be available even after reboot.

#fdisk /dev/sda

Choose hex code 82 for swap

#mkswap /dev/sda7

#swapon /dev/sda7

#swapon –s #blkid /dev/sda7 (copy UUID)

#vim /etc/fstab

UUID=XXXXXXX swap swap defaults 0 0

#swapon –s (To verify)

1. Create 250 MB partition and format it with EXT4 and mount it permanently at /data

#fdisk /dev/sda

Press ‘n’ ……

Now press ‘t’ for changing partition type.

Hex code:8e

Press l to confirm partition

Press w

#partprobe /dev/sda

Tip: if you creating partition for the fist time, create it as an extended partition for all the available space and then from it, you can create more different partition. #pvcreate /dev/sda4 /dev/sda5

#vgcreate datavg /dev/sda4 /dev/sda5

 #lvcreate –L 250M –n datalv datavg

 #mkfs.ext4 /dev/datavg/datalv

#mkdir /data

#vi /etc/fstab

/dev/datavg/datalv /data ext4 defaults 0 0

Assignment: work with Tatiana  with the week

1. Add a disk in your VM
2. Check the difference between

**Troubleshooting Commands and Sources of Useful Information**

1. **Useful Information**
2. **Log Files:** Log files are often the first place to look for troubleshooting information. Whenever a service or server is experiencing an issue, checking the log files for errors can often answer many questions quickly.
3. **Command Log Files:** The following table is a short list of common log files and a description of what you can find within them. This list is specific to what you can find in Re Hat Linux 7, and while other distributions might follow similar conventions, there’s no guarantee.

/var/log/message: General message and system related stuff

/var/log/auth.log: Authenication logs

/var/log/kern.log: Kernel logs

/var/log/cron.log: Crond logs (cron job)

/var/log/maillog: Mail server logs

/var/log/qmail/ : Qmail log directory (more files inside this directory)

/var/log/httpd/: Apache access and error logs directory

/var/log/lighttpd: Lighttpd access and error logs directory

/var/log/boot.log : System boot log

/var/log/mysqld.log: MySQL database server log file

/var/log/secure: Authentication log

/var/log/utmp or /var/log/wtmp : Login records file

/var/log/yum.log: Yum log files

/var/log/faillog – Contains user failed login attemps.

/var/log/secure - This log file contains authentication related messages items such as ssh, user creation and sudo violations and  privilege educations.

For many issues, one of the first files to review is /var/log/messages log

B**. Troubleshooting Commands**

1. Gathering General Information:
2. #w -show who logged on and what they are doing
3. #rpm -q -a -listing all packages installed
4. #df -report file system space usage. The df command is very useful command when troubleshooting file system issues. The df command is used to output space utilization for mounted file systems (#df -h).
5. #df -i -showing available inodes
6. #free -display memory utilization
7. #grep Available /proc/meminfo
8. #ps -report a snapshot of current running processes
9. VIII.#ps -elf -printing every process in a long format
10. #ps -U postfix -l -printing a specific user’s processes
11. #ps -p 1236 -l - printing a process by process ID

**2. Networking:**

1. #netstat -na -printing network connections (print the existing established network connections.if the -a (all) flag is used, the output will also include listening ports ).
2. #netstat -nlp - -tcp -printing all ports listening for TCP connections
3. #ifstat -review interface statistics. When it comes to network, there are about four metrics that can be used to measure throughput: Received packets (number of packets received by interface); Sent Packets (number of packets sent out by the interface); Received data (amount of data received by the interface), and sent data (amount of data sent by the interface)

**3. Performance:**

1. #iotop -a simple top-like i/o monitor
2. #iostat -report I/O and CPU statistics. While iotop shows what processes are utilizing I/O, iostat shows what devices are being utilized.
3. #vmstat -report virtual memory statistics. Where iostat is used to report statistics about disk I/O performance, vmstat is used to report statistics about memory usage and performance.
4. #vmstat - - stats
5. #sar -collect, report or save system activity information. The you print without any flag, it will print the current day’s CPU statistics.
6. #sar -f /var/log/sa/sal3 -use the -f flag to run sar against a specified file.
7. #top -a single command to look for everything. Look for the overall systems performance using top. Details are updated every 3 seconds if ran without any flag
8. VIII.#cat /proc/cpuinfo -determining the number of CPUs available
9. #lscpu -another way to look for CPU info
10. #ps -Drill down deeper on individual processes with ps
11. #ps -lf 3000
12. #free -looking at free and used memory
13. XIII.# free -m
14. XIV.#grep “Out of memory” /var/log/messages
15. #vmstat -monitoring memory allocation and swapping
16. XVI.#vmstat -n 10 5
17. XVII.#iostat -CPU and device input/output statistics
18. XVIII.#iostat -x 10 3
19. XIX.#sar -d -show disk statistics for today

• R: running or runnable, it is just waiting for the CPU to process it

• S: Interruptible sleep, waiting for an event to complete, such as input from the terminal

• D: Uninterruptible sleep, processes that cannot be killed or interrupted with a signal, usually to make them go away you have to reboot or fix the issue

• Z: Zombie, we discussed in a previous lesson that zombies are terminated processes that are waiting to have their statuses collected

• T: Stopped, a process that has been suspended/stopped

#ps -elf | grep “ D “

#ps -elf - - forest

#iotop -a top like command for disk i/o

4**. Troubleshooting a web application:**

1. #ps -elf | grep mysql (validating the database service)
2. #rpm -qa | egrep “(maria/mysql)”. The egrep is similar to grep. However, it accepts search strings in the form of regular expressions
3. #rpm -aq | grep php -validating php
4. #ps -elf | grep php
5. #ls -la /var/www/html

**5. Testing Connectivity**

#telnet [db.example.com](http://db.example.com/) 3306

#ping [db.example.com](http://db.example.com/)

#ping .[google.com](http://google.com/" \t "_blank)

**6. Troubleshooting DNS**

Checking DNS with dig

#dig [db.example.com](http://db.example.com/)

#dig @8.8.8.8 [db.example.com](http://db.example.com/)

Looking up DNS with nslookup

#nslookup [db.example.com](http://db.example.com/)

#nslook [db.example.com](http://db.example.com/) 8.8.8.8

7. Verifying that Iptables is running

#ps -elf grep iptables

#service iptable status

#systemctl status iptables.service

8. Show Iptables Rules Enforce

#iptable -L -n

#iptable -L nv

9. File Systems Errors and Recovery

#cat /proc/mounts

#fdisk -l -to lost available partitions

#mount | grep /boot

#mount | grep “data”

#lsof (to print all open files

#ls -r | grep /boot

#fsck /dev/sda1 -check the filesystem for consistency

#fsck -y /dev/sda1 -automatically repair the issues found by passing in the -y flag