open-shift(okd) installaion and documentation

https://opensource.com/article/18/11/local-okd-cluster-linux
#######################################
tripwire-tool

https://www.unixmen.com/install-tripwire-intrusion-det-such-file-or-directory/

######################################

file and directorys integrity
if any one changes any file

https://www.cyberciti.biz/tips/linux-audit-files-to-see-who-made-changes-to-a-file.html
https://www.digitalocean.com/community/tutorials/how-to-write-custom-system-audit-rules-on-centos-7#prerequisites
https://www.scip.ch/en/?labs.20150604
https://www.thegeekdiary.com/how-to-use-auditd-to-monitor-a-file-deletion-in-linux/
http://linux.die.net/man/8/auditd
http://linux.die.net/man/8/aureport
http://linux.die.net/man/8/pam_tty_audit
http://www.sudo.ws
https://duckduckgo.com/?q=log+_bash_+commands&ia=qa
https://www.newnettechnologies.com/what-are-the-recommended-audit-policy-settings-for-linux.html#file-deletion-events-by-users >>>>>> important for audit rules

###############################

for tcpdump related topics

https://linoxide.com/linux-how-to/14-tcpdump-commands-capture-network-traffic-linux/

############################

advanced command restriction in linux with rbash

https://www.ostechnix.com/how-to-limit-users-access-to-the-linux-system/

###
for hipaa information

https://www.fullmedia.com/a-beginners-guide-to-hipaa-compliant-websites
https://medium.com/@oceanbcreative/hipaa-compliance-for-app-web-based-health-platforms-aa4872f88e35
https://medium.com/@MedStack/hipaa-tips-for-developers-hipaa-compliant-servers-3f8951b94bc3
https://www.manageengine.com/products/eventlog/hipaa-compliance-reports.html
##

qa-server release

website ....> /home/drucareqa/qa/Root
python ui.py qa-website

microui ....> /home/drucareqa/qa/microui
python ui.py qa-microui

app 1.6 ....> /home/drucareqa/qa/app
python ui.py qa-app

```
new 7 ........................>  /home/drucareqa/qa/new
python  ui.py   qa-new



###########################################
for  ssh certificate  authentication
https://www.youtube.com/watch?v=gxpGtopzdhk

commands to create  ssh  certificate

ssh-keygen    -f  test-ca

cp publickey  /etc/ssh/

vi /etc/ssh/sshd_config
TrustedUserKeys /etc/ssh/test.ca

##########################
user-malli  db  server
https://www.google.com/chart?chs=200x200&chld=M|
0&cht=qr&chl=otpauth://totp/malli@devdb.dru.care%3Fsecret
%3DBGXOXI7ER43DC5HCAVBKMTPTAY%26issuer%3Ddevdb.dru.care
Your new secret key is: BGXOXI7ER43DC5HCAVBKMTPTAY
Your verification code is 523896
Your emergency scratch codes are:
  99017398
  25707289
  96923203
  10583261
  37831789

##############################
user-malli  chat  server

https://www.google.com/chart?chs=200x200&chld=M|
0&cht=qr&chl=otpauth://totp/malli@chat.dru.care%3Fsecret
%3DQ7RRKC6CNPQUZV6YWT2C2B5FWA%26issuer%3Dchat.dru.care
Your new secret key is: Q7RRKC6CNPQUZV6YWT2C2B5FWA
Your verification code is 515584
Your emergency scratch codes are:
  31918664
  57304709
  54667247
  70938598
  61308471

###########################
user-malli   elk  server
https://www.google.com/chart?chs=200x200&chld=M|
0&cht=qr&chl=otpauth://totp/malli@elk.dru.care%3Fsecret
%3DJNHAVML7BWG3NPAKNSSR3EYYRU%26issuer%3Delk.dru.care
Your new secret key is: JNHAVML7BWG3NPAKNSSR3EYYRU
Your verification code is 843486
Your emergency scratch codes are:
  97398645
  41802738
  59594068
  55701401
  13257381

###############################
user- malli  dev  server
```

```
https://www.google.com/chart?chs=200x200&chld=M|
0&cht=qr&chl=otpauth://totp/malli@dru.test01%3Fsecret
%3DEHNV64YJ2QPDLZKPTMWKGETNGA%26issuer%3Ddru.test01
Your new secret key is: EHNV64YJ2QPDLZKPTMWKGETNGA
Your verification code is 594722
Your emergency scratch codes are:
  51942261
  46931749
  71181137
  77740127
  86984570

###########################

###########################
malli-user  qa  server
  https://www.google.com/chart?chs=200x200&chld=M|
0&cht=qr&chl=otpauth://totp/malli@qa.dru.care%3Fsecret
%3D6752X33LLUHTP5EWQXLEQADWC4%26issuer%3Dqa.dru.care

Your new secret key is: 6752X33LLUHTP5EWQXLEQADWC4
Your verification code is 291093
Your emergency scratch codes are:
  84711692
  97585982
  37842349
  29526823
  34877767

#########
shell-scripting  pdf  slides  url

https://www.slideshare.net/polarahul/linux-shell-scripting-tutorial-45352341?
fbclid=IwAR36vVGZHgB2UftOlPbMzmXWsjBrrE-I6Y9Xl2Kocu3x_VUhNVzQ_GqlMTk

###################
elk-server  grok  pattrens

https://github.com/logstash-plugins/logstash-patterns-
core/blob/master/patterns/grok-patterns
###################
docker issues

https://stackoverflow.com/questions/47506171/start-ssh-using-systemctl-inside-
the-docker-container
https://stackoverflow.com/questions/50393525/failed-to-get-d-bus-connection-
operation-not-permitted

#######################

#for shell scripting advanced concepts

https://www.softwaretestinghelp.com


#######################################################
finding ip from  pid

https://stackoverflow.com/questions/8167537/finding-the-ip-from-the-pid
########################################
https://www.quora.com/How-do-I-become-hadoop-administrator
###################################
converstion of hexadecimal to  ip and port
```

```
https://www.browserling.com/tools/hex-to-ip

https://www.hexdictionary.com/hex/01BB/

###################################
for to increase bash historysize and    to add time stamp to that history

https://www.rootusers.com/17-bash-history-command-examples-in-linux/
####################################
openssl req -new -x509 -nodes -out pub.crt -keyout pub.key  -days 90

for https(nginx) server purpose
#############################
google time sysnchronaization commands

https://www.dyclassroom.com/reference-server/how-to-sync-linux-server-time-with-ntp-network-time-protocol-server
###########
if dns failed then applied commands

vim /etc/resolv.conf

nameserver 8.8.8.8
nameserver 8.8.4.4
###############
vim /etc/hosts

192.168.2.146  malli.example.com

systemctl restart systemd-hostnamed

######################

###################
setting grub password to get rid of phyisical access

grub2-mkpasswd-pbdkf2

vim /etc/grub.d/40_custom

in this configuration file we have to make entry like follows..

set superusers="root"
password_pbkdf2 root (shift+insert)

grub2-mkconfig -o /boot/grub2/grub.cfg

note: before doing this backup of above mentioned two configuration files must be taken
##########################################

delete all the empty lines in a file

#sed '/^$/ d' file.txt

delete all the "#symbol" lines in a file

#sed '/^#/ d' file.txt


############################

#cat /var/log/secure  | grep sshd | grep Accepted | awk '{print $11}'
#cat /var/log/secure  | grep sshd | grep Disconnected | awk '{print $11}'
```

```
#cat /var/log/secure  | grep sshd | grep Rejected  | awk  '{print $11}'

########################
```

allowing multipule ports at time by using for loop

```
cat > file
121
123
8080
80
# for i in `cat tst` ; do firewall-cmd --permanent  --add-port=$i/tcp ; done ; firewall-cmd --reload ; firewall-cmd  --list-all
#  for i in `cat tst` ; do firewall-cmd  --permanent --remove-port=$i/tcp ; done ; firewall-cmd  --reload ; firewall-cmd --list-all
```

for particular Zones also

```
# for i in `cat tst` ; do firewall-cmd --permanent --zone=public --add-port=$i/tcp ; done ; firewall-cmd  --reload ; firewall-cmd  --list-all
```

if do not mention any zone by default it will consider "public zone"

```
############################
```

to get colour coding in yaml file use following code in .vimrc

```
# autocmd FileType yaml setlocal ai ts=2 sw=2 colorcolumn=1,3,5,7,9,11


################################################################################
#####################################################
```

create admin new user using git bash in centos mechine:
===

```
1.create ec2 instance
2.save filename.pem file in your pc
3.go to file location-->right click-->click on "git bash here"
4.ssh -i "db-testing.pem" centos@ec2-13-232-115-66.ap-south-1.compute.amazonaws.com  [change root to centos user]
5.sudo -s [change to root user]
6.enable port-22 and PasswordAuthentication - yes
  *vi /etc/ssh/sshd_config
  *service sshd restart/systemctl restart sshd
7.adduser username
8.passwd username[enter and confirm password]
9.usermod -aG wheel username[members of the wheel group have sudo privileges]
10.su - username[Test sudo access on new user account]
11.sudo ls -la /root[only accessible to the root user.]

12.timedatectl set-timezone Asia/Kolkata changing time zone
```

from linux server:

```
ssh -p 15951 -i pem-file-name.pem centos@10.0.0.89
```

dbuser {Dru@999}

logs:
====

```
tail -222f /logs/report.json
```

```
executing command in remote-server:
===================================
ssh -p portno username@IP/dns command
ssh -p 15951 drucareqa@10.0.2.103 'python test.py veer'     [asks pwd]
sshpass -p 'pwd'  ssh -p 15951 drucareqa@10.0.2.103 'python test.py veer'
[passing pwd in command using sshpass]



copying directory to remote server:
===================================
scp -P portno -r path/to/directory  username@IP:/destination/path
scp -P 15951 -r ./deploy veer.n@13.233.123.16:/home/veer.n/      [deploy
directory is copied into destination]

copying file to remote server:
===================================
scp -P portno path/to/file username@IP:/destination/path
scp -P 15951 file.txt veer.n@13.233.123.16:/home/veer.n/       [deploy directory
is copied into destination]

memory information:
==================
df -h  ------------------------[free disk space]
du -h  ------------------------[used disk space]
du -h /opt/app/jarbackup-------[size of any directory]
du -sh  <foldername>
free -h -----------------------[free ram space]
sudo du -h / | sort -rh | head -10

http://fuzzyblog.io/blog/docker/2017/08/30/running-out-of-disc-space-with-
docker.html

timedatectl set-timezone Asia/Kolkata changing time zone

exporting a port in centos:
===========================
rootusers.com/how-to-open-a-port-in-centos-7-with-firewalld/
www.rootusers.com
How To Open A Port In CentOS 7 With Firewalld

contos java installation:
===========================

yum check-update
yum upgrade
yum clean all
yum install nano wget curl net-tools lsof bash-completion

wget --no-cookies --no-check-certificate --header "Cookie: gpw_e24=http%3A%2F
%2Fwww.oracle.com%2Ftechnetwork%2Fjava%2Fjavase%2Fdownloads%2Fjdk8-downloads-
2133151.html; oraclelicense=accept-securebackup-cookie;"
"download.oracle.com/otn-pub/java/jdk/8u201-
b09/42970487e3af4f5aa5bca3f542482c60/jdk-8u201-linux-x64.rpm"
download.oracle.com
Unauthorized Request

sudo sh -c "echo export JAVA_HOME=/usr/java/jdk1.8.0_201-amd64/jre >>
/etc/environment"

#############################

=======
on 1st day of every month::::::::::cron job:::::::::::::[0 0 1 * *
/usr/bin/python /home/drucareqa/logszip/logszipping.py]

mail file----------------------/var/mail/$USERNAME or /var/spool/mail/username
file location-----------------/etc/crontab
logs--------------------------/var/log/cron

/usr/lib/cron/cron.allow
/usr/lib/cron/cron.deny
```

permissions for root user:
=========================

for giving permissions on few commands add below line to "sudoers" file by using "sudo visudo" command

```
->username ALL = NOPASSWD: /usr/bin/mv, /usr/sbin/service, /usr/bin/kill
->username ALL=(ALL) NOPASSWD:ALL  ------------[permissions on all commands]
```

15. Remove Unneeded Services

```
 ss -tulpn
 # systemctl list-units -t service
 # yum remove service-name
```

27. Lock Accounts

```
 lock:
 # passwd -l username ---------------user cannot login
 # usermod -L username
 unlock:
 # passwd -u username
 # usermod -U username
```

28.Prevent Accounts Shell Access:[/usr/sbin/nologin or /bin/false]

```
 # usermod -s /bin/false username-----------------------user cannot login
 or
 # useradd -s /usr/sbin/nologin username

 # chage -d 0 username[ immediate password expiration (user must change password on next login)]
```

Disable SSH Root Login:

```
 #vi /etc/ssh/sshd_config----->PermitRootLogin no
 #systemctl restart sshd
```

Allowing Users:

add below property to allow particular users in "/etc/ssh/sshd_config" file

```
 {AllowUsers username1 username2}
 #systemctl restart sshd

 /var/log/secure
```

password aging/expiration:

```
      chage -M 30 uesrname(gammadev,betadev,deltadev,alphadev)
      chage -M -1 uesrname-----disabling expiration
```

##################################

netConnectivity:

Remember from open project if mails cant be send, there seems a internet issue in the server. To restore internet connectivity, do the below things.

```
$ source /root/.bash_profile
$caa -d
```

```
Do these things as root user. Check if internet connectivity works.


Rocket chat:
------------
/etc/init.d/rocketchat_all start


community.openproject.com/projects/docker/work_packages/24378/activity

Use the command docker exec -it <container name> /bin/bash to get a bash shell
in the container
Generically, use docker exec -it <container name> <command> to execute whatever
command you specify in the container.

################################################

unmount a device:https://www.webhostinghero.com/blog/how-to-unmount-filesystems-
or-partitions-in-centos-linux/
================
1.The first step is to find out which disks and volumes are mapped to which
directories.
  lsblk
  2.in order to unmount a device, you must be Ã¢â□¬Å□standing outsideÃ¢â□¬ its
block device descriptor or mount point
    umount /var/lib/docker
    3.lsblk


    mounting hard disk:
    ===================
    1.mkfs.xfs /dev/xvdb
    2.mount -t xfs /dev/xvdb /var/lib/dockers
    3.open /etc/fstab
      add the entry ---------- /dev/xvdb /var/lib/docker xfs defaults 0 0

      cyberciti.biz/faq/centos-linux-6-7-changing-timezone-command-line/


#########################################

>Download the activemq gzip file to the Unix machine, using either a browser or
a tool, i.e., wget, scp, ftp, etc. for example:
  wget http://archive.apache.org/dist/activemq/5.15.3/apache-activemq-5.15.3-
bin.tar.gz
>Extract the files from the gzip file into a directory of your choice. For
example:
         tar zxvf activemq-x.x.x.tar.gz -C /target/directory
      i.e: tar zxvf apache-activemq-5.15.3-bin.tar.gz -C /var/activemq/
           mv /var/apache-activemq-*/ /var/activemq/
>If the ActiveMQ start-up script is not executable, change its permissions. The
ActiveMQ script is located in the bin directory. For example:
     cd [activemq_install_dir]/bin
     chmod 755 activemq
>now create activemq.service file[Using Systemd service will ensure that
ActiveMQ will start automatically at boot time and failures]
  vi  /etc/systemd/system/activemq.service



>Now populate the activemq.service file with the following content.
-------------------------------------------
[Unit]
Description=ActiveMQ service
```

```
After=network.target

[Service]
Type=forking
ExecStart=/var/activemq/bin/activemq start
ExecStop=/var/activemq/bin/activemq stop
User=root
Group=root
Restart=always
RestartSec=9
StandardOutput=syslog
StandardError=syslog
SyslogIdentifier=activemq

[Install]
WantedBy=multi-user.target
----------------------------------------------
>systemctl start activemq
> To configure ActiveMQ to automatically start at boot time, use.
  systemctl enable activemq
>systemctl status activemq

>Using Admin Web Panel of activemq
  http://Your_Server_IP:8161/admin
>If you have firewalld installed, you will have to allow port 8161 through the
firewall. Run the following command for same.

   firewall-cmd --zone=public --permanent --add-port=8161/tcp
   firewall-cmd --reload

   The initial username and password for Apache ActiveMQ are admin and admin.
Once you are logged in, you will see the following interface.



###########################################
#######################
 backuping  module ....

1. backup /usr/share  directory to /root/usr.tar.gz  (or)  /root/usr.tgz
2. backup /usr/share  directory to /root/usr.tar.bz2
3. backup /usr/share  directory to /root/usr.tar.xz


answers ...

1. tar czvf  /root/usr.tar.gz   /usr/share  (or)  tar czvf  /root/usr.tgz
/usr/share
1. tar cjvf  /root/usr.tar.bz2  /usr/share    (small 'j')
1. tar cJvf  /root/usr.tar.xz   /usr/share    (capital 'J')



############################



#utmpdump /var/run/utmp | grep  malli  | sed -n '2 p' | awk -F " " '{print
$5$6,$13,$14,$15,$16,$17,$18,$19}'


###########################
```