

??????

Home ??

???? Home ??

?? User ? Home ?????????????????????????????

????????????????

```
cd /home
cp -a user1/ user1_new/
```

????????????????

```
cd /home
cp -a user1/.[^.]* user1_new/
```

???????? Home ??

```
cp -r /etc/skel /home/user1
chown -R user1.group1 /home/user1
chmod 0700 /home/user1
```

??? /home ????????

“ Answer: ?(?)??????????? SELinux ???????????? SELinux ???????????

```
# ls -ld /home
drwxr-xr-x. 2 root root 4096 Mar 28 2017 /home

# ls -Zd /home
drwxr-xr-x. root root system_u:object_r:home_root_t:s0 /home
```

????? Home ??

```
mkhomedir_helper <username>
```

???????

?????? share_test??? team ????????????????

```
groupadd team
mkdir /worktmp/share_test
chgrp team /worktmp/share_test
chmod 2775 /worktmp/share_test
usermod -aG team i04181
```

?? PATH

PATH ?????? bin ??

~/.bashrc :

```
# Custom PATH
case :$PATH: in
    */home/$USER/bin:*) ;;
    *) PATH=/home/$USER/bin:$PATH ;;
esac
```

```
[ -z "$(sed -n '@usr/local/bin@p' <<< $PATH)" ] && PATH=/usr/local/bin:$PATH
```

Custom Prompt

```
# Kali-like Custom PROMPT
PS1="\[\033[38;5;209m\] └─\[\033[38;5;141m\]u\[\033[38;5;209m\]@\[\033[38;5;105m\]\h\[\033[38;5;231m\]:\nw\[\033[38;5;209m\]\[\033[33m\]\$(GIT_PS1_SHOWUNTRACKEDFILES=1 GIT_PS1_SHOWDIRTYSTATE=1\n__git_ps1)\[\033[00m\]\n\[\033[38;5;209m\] └─\[\033[38;5;209m\]$\[\033[37m\] "
```

Solution: __git_ps1 command not found

```
curl -o ~/.git-prompt.sh https://raw.githubusercontent.com/git/git/master/contrib/completion/git-prompt.sh
echo 'source ~/.git-prompt.sh' >> ~/.bashrc
```

?? Zombie ??(defunct)

One may deal with zombie processes in any one of the following ways:

- Fix the parent process to make it execute `wait(2)` on child process exit
- Kill the parent process of the zombie
- Reboot system
- Ignore it

?? zombie processes

```
ps aux |grep "defunct"
ps aux |grep Z

# How many Zombie process running on your server
ps aux | awk {'print $8'}|grep -c Z

# List the PID of Zombie
ps aux | awk '{ print $8 " " $2 }' | grep -w Z
```

Kill zombie process

```
# find the parent process list
pstree -paul

kill -9 <PARENT-PID>
```

RHEL Documents:

- [What_is_a_zombie_\(defunct\)_process.pdf](#)
- [How_to_kill_Zombie_Defunct_process.pdf](#)

?? & Auditing ??

```
# Parse /var/log/secure
grep "authentication failure" /var/log/secure | awk '{ print $13 }' | cut -b7- | sort | uniq -c

# Login failed attempts
lastb -F
lastb -F <username>
```

Check Linux Login History

```
#!/bin/bash
#Filename: intruder_detect.sh
```

#Description: Check Linux Login History

AUTHLOG=/var/log/secure

if [[-n \$1]];

then

 AUTHLOG=\$1

 echo Using Log file : \$AUTHLOG

fi

Collect the failed login attempts

FAILED_LOG=/tmp/failed.\$\$log

egrep "Failed pass" \$AUTHLOG > \$FAILED_LOG

Collect the successful login attempts

SUCCESS_LOG=/tmp/success.\$\$log

egrep "Accepted password|Accepted publickey|keyboard-interactive" \$AUTHLOG > \$SUCCESS_LOG

extract the users who failed

failed_users=\$(cat \$FAILED_LOG | awk '{ print \$(NF-5) }' | sort | uniq)

extract the users who successfully logged in

success_users=\$(cat \$SUCCESS_LOG | awk '{ print \$(NF-5) }' | sort | uniq)

extract the IP Addresses of successful and failed login attempts

failed_ip_list="\$(egrep -o "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" \$FAILED_LOG | sort | uniq)"

success_ip_list="\$(egrep -o "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" \$SUCCESS_LOG | sort | uniq)"

Print the heading

printf "%-10s|%-10s|%-10s|%-15s|%-15s|s\n" "Status" "User" "Attempts" "IP address" "Host" "Time range"

Loop through IPs and Users who failed.

for ip in \$failed_ip_list;

do

 for user in \$failed_users;

 do

 # Count failed login attempts by this user from this IP

 attempts=`grep \$ip \$FAILED_LOG | grep " \$user " | wc -l`

 if [\$attempts -ne 0]

 then

```

first_time=`grep $ip $FAILED_LOG | grep " $user " | head -1 | cut -c-16`
time="$first_time"
if [ $attempts -gt 1 ]
then
    last_time=`grep $ip $FAILED_LOG | grep " $user " | tail -1 | cut -c-16`
    time="$first_time -> $last_time"
fi
HOST=$(host $ip 8.8.8.8 | tail -1 | awk '{ print $NF }' )
printf "%-10s|%-10s|%-10s|%-15s|%-15s|%-s\n" "Failed" "$user" "$attempts" "$ip" "$HOST" "$time";
fi
done
done

for ip in $success_ip_list;
do
    for user in $success_users;
    do
        # Count successful login attempts by this user from this IP
        attempts=`grep $ip $SUCCESS_LOG | grep " $user " | wc -l`

        if [ $attempts -ne 0 ]
        then
            first_time=`grep $ip $SUCCESS_LOG | grep " $user " | head -1 | cut -c-16`
            time="$first_time"
            if [ $attempts -gt 1 ]
            then
                last_time=`grep $ip $SUCCESS_LOG | grep " $user " | tail -1 | cut -c-16`
                time="$first_time -> $last_time"
            fi
            HOST=$(host $ip 8.8.8.8 | tail -1 | awk '{ print $NF }' )
            printf "%-10s|%-10s|%-10s|%-15s|%-15s|%-s\n" "Success" "$user" "$attempts" "$ip" "$HOST" "$time";
            fi
        done
    done

rm -f $FAILED_LOG
rm -f $SUCCESS_LOG

```

System Audit

```
# Install Audit
yum install audit
systemctl start auditd

# Authentication Report
# To get authentication report for all the attempts which was made
aureport -au -i | more
# To get authentication report for all the success attempts which was made
aureport -au -i --success | more
# To get authentication report for all the failed attempts which was made
aureport -au -i --failed | more
# To get success login information
aureport -l --success | more
# To get failed login information
aureport -l --failed | more
# To get success login summary report for all the success attempts which was made
aureport -l --success --summary -i | more
```

Check if a RHEL system is vulnerable to a specific CVE

```
# rpm -q --changelog [package-name] | grep [CVE-NUMBER]
rpm -q --changelog openssl | grep CVE-2021-3450
rpm -q --changelog openssl | grep CVE
rpm -q --changelog openssl | grep CVE-2021

# Using yum command
yum install yum-plugin-security
yum update yum
yum updateinfo info --cve CVE-2021-3445
```

Auditd

- [AUDITD RECOMMENDED CONFIGURATION ON REDHAT OR CENTOS LINUX FOR SYSTEM AUDITING](#)
- [Linux ?? pam_tty_audit ?? SSH ??????????????](#)
- [Auditd?Linux ??????????????](#)
- The [psacct](#) package contains several utilities for monitoring process activities, including ac, lastcomm, accton and sa.

Auditing tool for UNIX/Linux like - Lynis

- <https://cisofy.com/>
- [How to Do Security Auditing of Linux System Using Lynis Tool](#)

rsh

rsh server

```
# install on CentOS 6/7
yum install rsh-server

# Startup the service on CentOS 6
chkconfig rsh on
chkconfig rlogin on
service xinetd reload

# Startup the service on CentOS 7
systemctl start rsh.socket
systemctl start rlogin.socket
systemctl start rexec.socket
systemctl enable rsh.socket
systemctl enable rlogin.socket
systemctl enable rexec.socket
```

strace ????

```
# Trace the command
strace df -h

# Trace the process ID
strace -p 33259

# Get Summary of Linux Process
strace -c -p 3569

# Print Instruction Pointer During System Call
strace -i df -h

# Show Time of Day For Each Trace Output Line
strace -t df -h
```

```
# Print Command Time Spent in System Calls
```

```
strace -T df -h
```

```
# Trace Only Specific System Calls
```

```
strace -e trace=write df -h
```

```
strace -p 3569 -e poll
```

?? suspend, hibernation

```
# disable the following systemd targets
```

```
sudo systemctl mask sleep.target suspend.target hibernate.target hybrid-sleep.target
```

```
sudo systemctl restart systemd-logind.service
```

```
# Then reboot the system and log in again
```

```
# Verify if the changes have been effected using the command
```

```
sudo systemctl status sleep.target suspend.target hibernate.target hybrid-sleep.target
```

```
# To re-enable the suspend and hibernation modes, run the command
```

```
sudo systemctl unmask sleep.target suspend.target hibernate.target hybrid-sleep.target
```

To prevent the system from going into suspend state upon closing the lid, edit the `/etc/systemd/logind.conf` file.

```
[Login]
```

```
HandleLidSwitch=ignore
```

```
HandleLidSwitchDocked=ignore
```

????

```
# Approach #1
```

```
lsblk
```

```
nvme0n1 259:0 0 465.8G 0 disk
```

```
└─nvme0n1p1 259:1 0 512M 0 part /boot/efi
```

```
└─nvme0n1p2 259:2 0 465.3G 0 part /
```

```
nvme1n1 259:3 0 953.9G 0 disk /media/alang/AlangsData
```

```
# List UUID of disk
```

```
lsblk -l -o NAME,FSTYPE,MOUNTPOINT,UUID
```

```
NAME FSTYPE MOUNTPOINT UUID
```

```
sda
```

```
sda1 ext4 /boot f830a3fa-1f94-42f4-9dca-5b5c077eab66
```

```
sda2 ext4 / dcbdf18c-2fb4-426c-9dac-d13a45b7ebba
```

```
sda3 swap [SWAP] 6f40f01b-e9ed-4092-9c65-1445d92ec9da
```

```
sda4 ext4 6df9a3a6-052e-41f3-b15a-cb258db0267f
```

```
OVM_SYS_REPO_PART_3600508b1001cbe65c99583659f085b36 (dm-0)
```

```
ext4 6df9a3a6-052e-41f3-b15a-cb258db0267f
```

```
sr0
```

```
# Approach #2, requires to run as super-user.
```

```
sudo lshw -short -class disk,volume
```

```
H/W path          Device          Class          Description
```

```
=====
```

```
=
```

```
/0/100/14/0/3/4/0.0.0 /dev/sda      disk          Mass-Storage
```

```
/0/100/14/0/3/4/0.0.0/0 /dev/sda      disk
```

last

```
# To check the last ten login attempts, you can pipe it with "head"
```

```
last | head -n 10
```

```
# using complete usernames and hostnames
```

```
last -w
```

```
# find the device used by the user
```

```
tty
```

```
# To find the last login by date,
```

```
last --since <date>
```

```
last --until <date>
```

```
last --since -2days
```

```
# find the last bad login attempts
```

```
sudo lastb
```

```
tail -f -n 100 /var/log/auth.log | grep -i failed
```

```
# find the last SSH logins
tail -f -n 100 /var/log/auth.log | grep -i sshd
sudo journalctl -r -u ssh | grep -i failed

# find last login times for all users
lastlog
lastlog -u <user>
```

????????

```
dmidecode -s system-manufacturer
systemd-detec-virt
virt-what
```

????

```
sudo lshw -short

H/W path          Device          Class          Description
=====
=
                system          NUC8i7HVK
/0                bus            NUC8i7HVB
/0/0             memory        64KiB BIOS
/0/2f            memory        16GiB System Memory
/0/2f/0          memory        8GiB SODIMM DDR4 Synchronous Unbuffered (Unregistered)
/0/2f/1          memory        8GiB SODIMM DDR4 Synchronous Unbuffered (Unregistered)
/0/34            memory        256KiB L1 cache
/0/35            memory        1MiB L2 cache
/0/36            memory        8MiB L3 cache
/0/37            processor     Intel(R) Core(TM) i7-8809G CPU @ 3.10GHz
/0/100           bridge        Xeon E3-1200 v6/7th Gen Core Processor Host Bridge/DRA
/0/100/1         bridge        Xeon E3-1200 v5/E3-1500 v5/6th Gen Core Processor PCIe
/0/100/1/0       /dev/fb0      display        Polaris 22 [Radeon RX Vega M GH]
/0/100/1/0.1     multimedia    Advanced Micro Devices, Inc. [AMD/ATI]
/0/100/1.1       bridge        Xeon E3-1200 v5/E3-1500 v5/6th Gen Core Processor PCIe
/0/100/1.1/0     bus           ASMedia Technology Inc.
/0/100/1.1/0/0   usb3          bus            xHCI Host Controller
/0/100/1.1/0/1   usb4          bus            xHCI Host Controller
```

...

#

```
sudo lshw -html > HardwareSummary.html
```

Finding Number of Ram Slots

```
sudo dmidecode -t memory
```

```
sudo lshw -class memory
```

More options

```
sudo lshw -C <option>
```

Option	Description
network	Gets the details of the network hardware devices.
memory	Displays the details of RAM in your system.
storage	Prints details of the storage drives.
system	Gets the details of the motherboard and plug-and-play slots
multimedia	Details of the sound card of your system.
display	Know more about what is powering the display output.
bridge	Displays info about the PCIe bridges.
bus	It will list down buses and their details.
CPU	List the processor details

Inxi

Install

```
sudo apt-get install inxi
```

Check dependencies

```
inxi --recommends
```

Shows Full Linux System Information

```
inxi -F
```

Find Linux Laptop or PC Model Information

```
inxi -M
```

```
# Find Linux CPU and CPU Speed Information
```

```
inxi -C
```

```
# Find Graphic Card Information in Linux
```

```
inxi -G
```

```
# Find Audio/Sound Card Information in Linux
```

```
inxi -A
```

GUI Tools

```
# HardInfo
```

```
sudo apt-get install hardinfo
```

lspci

```
lspci
```

```
lspci -v -s <bus number>:<device number>.<function number>
```

???????

RedHat/CentOS

```
# RedHat/CentOS 6
```

```
yum install make libtool autoconf subversion git cvs wget libogg-devel gcc gcc-c++ pkgconfig
```

```
# RedHat/CentOS 7
```

```
yum group install "Development Tools"
```

Ubuntu/Debian

```
apt-get install build-essential
```

dd

```
#  MBR
```

```
dd if=/dev/hdx of=/path/to/image count=1 bs=512
```

```
# [ ] iso [ ]
dd if=/dev/cdrom of=/root/cd.iso

# [ ] [ ] [ ] [ ] [ ]
dd if=/dev/urandom of=/dev/hda1

# [ ] USB-Flash
dd if=/dev/sdb | gzip > ./my-usb_flash.img.gz

# [ ] USB-Flash
gzip -dc ./my-usb_flash.img.gz | dd of=/dev/sdb

# [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] 10GB
dd if=/dev/zero of=/path/to/image bs=1G count=10
# NOTE: [ ] Linux [ ] [ ] [ ] [ ] [ ]
fallocate -l 1G test.img

# Test network bandwidth between 2 Linux servers
dd if=/nas-mount-point/samplefile of=/dev/null bs=1M count=1024 iflag=direct
dd if=/dev/zero of=/nas-mount-point/samplefile bs=1M count=1024 oflag=direct
# NOTE: the samplefile is greater than 1GB and the RAM is preferably more than 2GB.

# [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] size [ ] [ ]
dd if=/dev/hda of=/dev/hdb conv=noerror,sync status=progress

# Quick benchmark test for writing 1GB file
dd if=/dev/zero of=/tmp/delme.dd bs=1024 count=1000000 status=progress
```

cat: ????

```
cat /dev/sda1 > /dev/sdb1
```

history

- [Bash History Display Date And Time For Each Command](#)
- [How to disable bash shell history in Linux](#)
- [Parsing Bash history in Linux](#)
- [Linux History Command with Advance Examples](#)

See time stamp in bash history

```
echo 'export HISTTIMEFORMAT="%F %T "' >> ~/.bash_profile
```

??????

?? Swap ? processes

```
for file in /proc/*/status ; do awk '/VmSwap|Name/{printf $2 " " $3}END{ print ""}' $file; done | sort -k 2 -n -r | less
```

OOM (Out of Memory) Killer

- [Linux Memory Overcommitment and the OOM Killer | Baeldung on Linux](#)

Swap ??

```
# [ ] [ ] swap [ ]
free
swapon -s

# [ ]/[ ] swap
swapon /dev/sda3
swapoff /dev/sda3

# [ ] [ ] swap [ ]
mkswap /dev/sda3
```

make-swapfile.sh?1GB

```
#!/bin/bash

dd if=/dev/zero of=/swapfile bs=1024 count=1024k
chown root:root /swapfile
chmod 0600 /swapfile
mkswap /swapfile
swapon /swapfile
echo "/swapfile          swap          swap      defaults      0 0" >> /etc/fstab
sysctl vm.swappiness=10
echo vm.swappiness=10 >> /etc/sysctl.conf
```

```
free -h
cat /proc/sys/vm/swappiness
```

Extend the existing SWAP partition:

🗨️ NOTE: ??? Production ?????????????????????? SWAP partition ???

```
[root@tycitpdb05-a ~]# grep -i swap /etc/fstab
/dev/mapper/rootvg-swap swap          swap    defaults    0 0

[root@tycitpdb05-a ~]# ls -al /dev/mapper/rootvg-swap
lrwxrwxrwx 1 root root 7 Aug 15 11:49 /dev/mapper/rootvg-swap -> ../dm-1

[root@tycitpdb05-a ~]# swapon -s
Filename                                Type      Size    Used    Priority
/dev/dm-1                              partition 4194300 0       -2

[root@tycitpdb05-a ~]# swapoff -v /dev/mapper/rootvg-swap
swapoff /dev/mapper/rootvg-swap

[root@tycitpdb05-a ~]# lvextend -L16G /dev/rootvg/swap
Size of logical volume rootvg/swap changed from 4.00 GiB (1024 extents) to 16.00 GiB (4096 extents).
Logical volume rootvg/swap successfully resized.

[root@tycitpdb05-a ~]# mkswap /dev/rootvg/swap
mkswap: /dev/rootvg/swap: warning: wiping old swap signature.
Setting up swapspace version 1, size = 16777212 KiB
no label, UUID=06aac9ae-9e8c-48bd-9f16-5f3d0c32b31f

[root@tycitpdb05-a ~]# swapon -v /dev/rootvg/swap
swapon /dev/rootvg/swap
swapon: /dev/mapper/rootvg-swap: found swap signature: version 1, page-size 4, same byte order
swapon: /dev/mapper/rootvg-swap: pagesize=4096, swaptsize=17179869184, devsize=17179869184
```

xfs ????

- [How to Check and Repair XFS Filesystem in RHEL](#)

?? xfs ????

```
sudo mount -a
mount: /data: mount(2) system call failed: Structure needs cleaning.

sudo umount /data

# with '-n' option to perform a dry run
sudo xfs_repair -n /dev/sdb1
# repair the filesystem
sudo xfs_repair /dev/sdb1
```

xfs ?????

```
# Install the xfsdump
dnf install xfsdump

# Create a full-backup
# -L: for dump session
# -M: for media in drive
# -f: the backup destination
xfsdump -L session_0 -M datapart -f /data/boot.xfsdump /boot

# Create a incremental backup with the level 1
# -l: the backup level (0-9)
xfsdump -l 1 -L session_1 -M datapart -f /data/boot.xfsdump1 /boot

# Restore a full-backup
xfsrestore -f /data/boot.xfsdump /test

# Restore an incremental backup
xfsrestore -r -f /data/boot.xfsdump /test
xfsrestore -r -f /data/boot.xfsdump1 /test
```

Linux Module

- [Linux: How to load a kernel module automatically at boot time](#)

?????????? (Monito File & Directory)

- [Watchman – A File and Directory Watching Tool for Changes](#)
- [Watchman - A file watching service | Watchman \(facebook.github.io\)](#)

- [inotify-tools](#)Linux 2.6.13
rsync ??? script?
- [fswatch - Monitor File and Directory Changes in Linux \(tecmint.com\)](#)
- [AIDE - How to Check Integrity of File and Directory Using “AIDE” in Linux](#)
- [Pyinotify](#)

??????

?? A.txt ????? B.txt ????

```
diff A.txt B.txt | grep "^<" | cut -c3-
```

??????

```
# tree
tree dir1
tree dir2

# diff
diff -q /path/to/dir1 /path/to/dir2
diff -q dir1 dir2
diff -qr dir1 dir2
diff -qrs dir1 dir2
```

????????????

```
# tree
tree -dfr --noreport dir1
tree -dfr --noreport dir1 | xargs -I{} mkdir -p "$HOME/Downloads/{}"
tree -a $HOME/Downloads/dir1

# find + xargs
find dir1 -type d
find dir1 -type d | xargs -I{} mkdir -p "$HOME/Documents/{}"
tree -a $HOME/Documents/dir1

# find + exec
find dir1 -type d -exec mkdir -p "$HOME/Desktop/{}" \;
```

?????

- [How to check memory utilization and usage in Linux](#)

```
# Using meminfo
cat /proc/meminfo
grep -E --color 'Mem|Cache|Swap' /proc/meminfo
```

- **MemTotal**, Total usable RAM (i.e., physical RAM minus a few reserved bits and the kernel binary code).
- **MemFree**, The sum of LowFree+HighFree.
- **MemAvailable**, (since Linux 3.14) An estimate of how much memory is available for starting new applications, without swapping.
- **Buffers**, Relatively temporary storage for raw disk blocks that shouldn't get tremendously large (20MB or so).
- **Cached**, In-memory cache for files read from the disk (the page cache). Doesn't include SwapCached.
- **SwapCached**, Memory that once was swapped out, is swapped back in but still also is in the swap file.

```
# Using free
free -h
# Repeat printing free command output every N seconds.
free -s 5 -c 10
```

- **total**, Total installed memory
- **used**, Used memory (calculated as total – free – buffers – cache)
- **free**, Unused memory (MemFree and SwapFree in /proc/meminfo)
- **shared**, Memory used mostly by tmpfs (Shmem in /proc/meminfo)
- **buffers**, Memory used by kernel buffers (Buffers in /proc/meminfo)
- **cache**, Memory used by the page cache and slabs (Cached and SReclaimable in /proc/meminfo)
- **buff/cache**, Sum of buffers and cache
- **available**, Estimation of how much memory is available for starting new applications, without swapping.

```
# Using vmstat
vmstat -w
```

- **swapd**, the amount of virtual memory used.
- **free**, the amount of idle memory.
- **buff**, the amount of memory used as buffers.
- **cache**, the amount of memory used as cache.
- **inact**, the amount of inactive memory. (-a option)
- **active**, the amount of active memory. (-a option)

- `si`, Amount of memory swapped in from disk (/s).
- `so`, Amount of memory swapped to disk (/s).

???????

Dash

```
# The filename with -- or -
rm -i -v -- -foo
rm -i -v -- --foo
rm -i -v ./-foo

# The filename with -- and whitespaces
rm -i -v -- '-- My Resume . txt'
rm -i -v -- '/path/to/dir/-- My Resume . txt'
rm -i -v -- '/path/to/dir/-- My Resume . txt'

# Using find
find . -name '--my-FileNameGoes-Here' -delete
find /path/to/directory/ -name '---filename with a white spaces' --delete
```

cp: ????????

```
# alias=cp -i -f
yes | cp -r /source /target
```

System Locale

```
# view information about the current installed locale
locale
localectl status

# view more information about an environmental variable
locale -k LC_TIME

# display a list of all available locales
locale -a

# Set System Locale
## Using the commands
```

```
## The following command sets LANG to en_IN.UTF-8 and removes definitions for LANGUAGE.
```

```
sudo update-locale LANG=LANG=en_IN.UTF-8 LANGUAGE
```

```
## Or
```

```
sudo localectl set-locale LANG=en_IN.UTF-8
```

```
sudo update-locale LC_TIME=en_IN.UTF-8
```

```
## Or
```

```
sudo localectl set-locale LC_TIME=en_IN.UTF-8
```

```
## Using the profile
```

```
vi ~/.bash_profile
```

```
LANG="en_IN.utf8"
```

```
export LANG
```

????????

1. Preserve File Permissions and Ownership
2. Maintain Symbolic Links
3. Avoid Disruption to Services or Applications
4. File Locking Issues
5. Efficiency in Log Management

```
> access.log
```

```
: > access.log
```

```
true > access.log
```

```
cat /dev/null > access.log
```

```
cp /dev/null access.log
```

```
dd if=/dev/null of=access.log
```

```
echo -n "" > access.log
```

```
truncate -s 0 access.log
```

tar ??

- [18 Tar Command Examples on Linux](#)

??????

```
# 1. Switch to single user mode
```

```
# NOTE: single mode [D], [D] console [D]
```

```
init 1
```

```
# 2. Tar up the whole system
```

```
tar zcpvf /backups/fullbackup.tar.gz --directory=/ --exclude=proc --exclude=dev --exclude=sys --exclude=boot --exclude=run --exclude=etc/fstab --exclude=backups .
```

```
# 3. Once this completes copy the tar file over to the root directory your new machine
```

```
# 4. Take a snapshot of your new machine. This way if things go wrong you can revert to the snapshot and try again.
```

```
# 5.Extract the tarball on your new machine
```

```
cd /
```

```
tar -zxvpf /path/to/fullbackup.tar.gz
```

Stress Test

- [stress-ng](#)
 - [Linux ?? Stress-ng ?? CPU??????? I/O ?????????? - Office ?? \(officeguide.cc\)](#)
 - [How to Test CPU and Memory Load with Stress & Stress-ng - Shouts.dev](#)
 - [How to Stress Test Your Linux CPU for High Load \(tecmint.com\)](#)

stress

```
stress --cpu 2 --io 3 --vm 4 --vm-bytes 512M --timeout 10m
```

sysbench

```
# size [ ] RAM
```

```
# max-time [ ]
```

```
sysbench --test=fileio --file-total-size=10G prepare
```

```
sysbench --test=fileio --file-total-size=10G --file-test-mode=rndrw --init-rng=on --max-time=300 --max-requests=0 run
```

?????

```
# with command
```

```
command -v <cmd-name>
```

```
# with which
```

```
which <cmd-name>
```

getent: ??????

The same as 'cat /etc/passwd' and 'cat /etc/shadow'

getent passwd

getent passwd <user-name>

getent shadow

getent group

getent group <group-name>

/etc/hosts

getent hosts

/etc/services

getent services

getent services <service-name>

/etc/networks

getent networks

Revision #121

Created 15 June 2020 06:56:16 by Admin

Updated 1 December 2024 09:41:41 by Admin