Contents

1

Linux

1.1 Resources

Books

1. Unix and Linux System Administration Handbook (Ordered)
2. The Practice of System and Network Administration

Communities

1. Superuser → https://superuser.com/
2. Server fault → https://serverfault.com/
3. Digital Ocean → https://www.digitalocean.com/community/tutorials

Sites

1. Ubuntu → https://help.ubuntu.com/
2. Tutorial Linux → https://tutorialinux.com/

Links

1. https://www.slideshare.net/kavyasri790693/linux-admin-interview-questions
2. http://simplylinuxfaq.blogspot.in/p/linux-system-admin-interview-questions.html
3. https://github.com/kylejohnson/linux-sysadmin-interview-questions/blob/master/test.md
4. https://github.com/chassing/linux-sysadmin-interview-questions#hard

1.2 Users, Passwords & Permissions

Users

1	Root	UID : 0, GUID : 0 (root)
2	Root Permissions	RW permissions for all files, but execute privilages can be removed
3	pseudo-users	Have a group w/ special privilages, use su <Group> to login as that group, w/ root this sets the group to the group defined
4	Adding a user	useradd <uname> (single) → newusers <batch file> (batch mode useradd). With no args a user is created with the system defaults, usually with a home dir etc.
5	Lock an Account	usermod -l <user>
6	New password	passwd <username>
7	Default file permissions	Set UMASK in /etc/login.defs (debians). Takes away the permissions
8	Change Owner & Group	chown
9	Password & login info	/etc/passwd → the hashed password itself is held in /etc/shadow
10	Change Permissions	chmod Bit mask OGA rwx
11	Delete User	userdel, removing recusively home folder and files → userdel -r

Groups

1	Wheel	Group allowing access to the sudo/su command to become another user or the superuser, for sudo this is enabled with visudo.
2	Add user to a group	usermod -a -G <group> <user> (-a only used with -G, without -a, -G makes the given groups the only additional groups he is a member of)
3	Change users primary group	usermod -g <group> <user>
4	New Group	groupadd <group>
5	All groups on system	getent group
6	chgrp	change the group ownership of a file

Sudo

1. Add a user as a sudoer by using visudo. You can specify users or groups.

2. Common to have a sudo or wheel group and to give that group root permissions in visudo
3. Syntax → <user> computerAddress=(<Runas_Alias>) <Command_Alias>
4. You can use a Runas_Alias to define a semi-super user that owns a group of files or processes. Then the user can use sudo to run as that user. Same you can limit the commands that a user can run as sudo with the Command_Alias
5. to give sudo root access use: <user> ALL=(ALL) ALL → root privilages to <user> with use of sudo

1.3 Processes

Process Info

1	PID	Process ID → PID 1 is init, spawns all other ids
2	proc	In /proc → State of running processes in a virtual file system
3	Process types	user → started w/out special permissions, daemon → exist in background, kernel → execute only in 'kernel space'
4	Forked	process being started by a parent process
5	Nice	Priority level [-20 (Highest) → 19 (Lowest)] → 0 is default. Call with: nice <val> <process>, reset the priority level with: renice <new val> <PID>
6	Process Monitering	Top, ps aux, htop → good tool

Process states

RHEL Doc: https://access.redhat.com/sites/default/files/attachments/processstates_20120831.pdf

1	**R** → Runnable/Running	1. Born or forked 2. Ready to run or runnable 3. Running in user space or running in kernel space

2	**S** → Sleeping/Waiting	1. Present in main memory 2. Present in secondary memory storage (swap space on disk)
3	**D** → Blocked/Uninterruptable sleep	Very fast, unobserved, just high priority
4	**T** → Temporarily Stopped	Temporarily stopped but can be restarted
5	**Z** → Zombie	Terminated but parent process has not released it yet

Process Signals

1	Send commands	See kill
2	pgrep	Use user or type to find the PID of processes
3	pkill	same as pgrep but it stops the matching PID
4	kill	Send a signal to a process with: kill -s <val> (default is 15) → see man(7) signals for the signals

1.4 Bash Scripting

Shell Variables

1	Set a shell variable from a program output	$(arg)
2	getconf	List system config variables
3	export	Allows a shell variable to be accessed by called processes
4	&&	call a command only if the proceeding one exited successfully. <command 1> && <command 2>
5	||	call a command only if the proceeding one failed. <command 1> ||<command 2>

Pipes & Redirection

1	Pipes	Sends the output of one file into the input of another → cat <filename> | grep <string>
2	Redirect	Use > to overwrite a file, >> to append. Use 1>> for STDOUT & 2>> for STDERR, use >& to redirect both.<command> < <file> send the file contents to the command

General Tools

1	curl	Tool for talking over several different protocols
2	wget	Downloads files from an address, same as curl but GNU

1.5 Maintenance

Running Jobs

1	Schedule Jobs (user)	crontab, edit using crontab -e, kept in /var/spool/cron/crontabs, also package specific cron jobs are in /etc/cron.d
2	Schedule Jobs (system)	/etc/crontab
3	at	Run a process at a specified time, accepts HH:MM
4	batch	Run a process when the load drops to a specified level

Backups

Backup Tools: http://www.admin-magazine.com/Articles/Using-rsync-for-Backups
Rsync Snapshots: http://www.mikerubel.org/computers/rsync_snapshots/

- rsync → Remote/Local, Local/Remote, & Local/Local file copying. Sends only the differences between the source & existing files in the destination
  - Use: rsync <options> <source> <destination>
    - Source → Can be files → *.c, or everything in a directory <path name>/, remove the trailing slash to copy the directory.

        * To specify a remote host <computer name> use → <computer name>:<path> as the <source> or <destination>. No : means local only.
    - Options:
        * -a → Archieve mode, saves symbolic links, devices, attributes, permissions, ownership, groups, and is recursive (i.e. -a == -rlptgoD).
        * -t → Transfer files, if file exists, remote-update protocol is used to update the file by sending only the differences
        * -z → Compress before sending
        * –delete → Delete files from the recieving side if not in backup (CAUTION: run –dry-run to see what will be removed first)
        * –progress & -v tells you whats going on

- Backup Types → All can be done using rsync
    - Incrimental → Only record changes from last incrimental backup
    - Differential → Records changes since the last total backup
    - Replica → Just replicate the whole shebang

- Rsync for incrimental backups
    - Have a full backup <Full Backup> → rsync to a fresh loc
    - Have <Backup.0> which has all the incrimental changes
    - Make each backup look like a full backup using hard links (cp -al)

1.6 Strings & Searching

Grep

1	Description	Search for a character pattern in a string
2	Use	grep <string> <filename> → returns the lines with the character pattern <string> in file filename
3	<option> -r	Follow directories
4	<option> -n	Get the line number
5	<option> -l	Get files with the string
6	<option> -i	Ignore case

Strings

1	cut -d <delim> -f <field1>-<field2>	Break a line on a delim, then take the fields in range, c of chars, b bytes
2	sed	**{FIXME: research needed}**
3	awk	**{FIXME: research needed}**

1.7 Files

Files

1	Types	7 types block special, char spectial, directory, normal file, symbolic link, named pipe, socket
2	diff	Get difference between 2 files or dirs
3	comm	select or reject common lines between files
4	ln	Create a symbolic link → sym links dont have to exist unlike hardlinks
5	link	Create a hard link → file must exist, links and binds the same disk space, if original file is removed, the disk space is still bound to the hard link
6	Find the file's character set	file -i → gives the mime type, search for

File Tools

1	cat	Read a file
2	tac	Read a file backwards
3	Head	Read first few file lines
4	Tail	Read last few file lines
5	read	read from user input → read var → will set the var variable

Find

1. Find a specific file by name find {Starting directory} -name <filename>
2. Finding by type → find <Starting directory> -type <d/f...>
3. Searching depth → find <conditions> -maxdepth <depth>

4. Running a command on all found files → find <conditons> -exec <command> + (the + ends the command)
5. Files by last accessed time → -atime <days_ago or -amin min_ago>
   a) a → accessed, m → modified, c → changed
   b) use -daystart to count from the start of the current day instead of right now
   c) use + for greater than the time, - for less and none for exactly

Finding Stuff

1	Locate (mlocate in suse)	Use updatedb to prepare a database with file locations, then that can be used instead of the slower find
2	which	Shows the full path of (shell) commands (or aliases)
3	whereis	Searches for commands installed and where it is → only for programs no aliases

TAR & ZIP

1	Make a tarball	tar -cpf fileout.tar filename1 filename2..., add p to mantain permissions
2	Extract a tarball	tar -xpf filename.tar (be cautious of 'tarbombs' extract in a directory)
3	tar & gzip	tar -czpf fileout.tar.gz filename1 filename2...
4	Uncompress .tar.gz	tar -xzpf filename.tar.gz
5	Compress to .gz	gzip filename
6	Uncompress .gz	gzip -c filename.gz
7	Compress to .Z	compress filename
8	Uncompress .Z	uncompress filename.Z

1.8 File System

Hierarchy (FHS-V2.3)

Docs: http://www.pathname.com/fhs/pub/fhs-2.3.pdf

1	bin	Essential command binaries
2	boot	Static files of the boot loader → unbootable w/out
3	dev	Device files
4	etc	Host-specific system configuration → must be static, cannot be a binary
5	lib	Essential shared libraries and kernel modules →
6	media	Mount point for removeable media → use lsblk to get the names of these
7	mnt	Mount point for mounting a filesystem temporarily
8	opt	Add-on application software packages
9	sbin	Essential system binaries
10	srv	Data for services provided by this system
11	tmp	Temporary files
12	usr	Secondary hierarchy
13	var	Variable data
14	home (optional)	User home dirs
15	lib<qual> (normally lib64 or lib32, optional)	If multiple library versions are needed like 32 & 64 bit
16	root (optional)	Home dir for root user

Mounting

1	Mounting	mount /dev/<device> destination
2	What disk are mounted	mount
3	Connected disks	lsblk prints out all of the connected devices nicely formatted
4	Mounting on boot	edit /etc/fstab

RAID

1	Name	Redundant array of inexpensive/independant disks
2	Description	Combines mutiple storage devices onto one virtualized disk. Used to improve performance and/or reliability

3	Performance	Improves performance by striping data across disks, allowing simultanious read/write operations of multiple disks.
4	Reliability	Mirrors data on multiple disks to deal w/ disk failure.
5	Levels	RAID has has levels 0,1,0+1,1+0,2,3,4,5,&6
6	RAID 0	Performance → stripes data across multiple disks to speed up R/W
7	RAID 1	Reliability → aka Mirroring, duplicates data to multiple disks
8	RAID 0+1	Reliability w/ Performance → Mirrors of striped data
9	RAID 1+0	Performance w/ Reliability → Stripped mirrors of data
10	RAID 5	Performance w/ some relibility → N-1 disks store data can lose 1 disk
11	RAID 6	Performance w/ Reliability → Like RAID 5 but with N-2 disks. Can lose upto 2 disks
12	Others	RAID 2-4 are rarely used.
13	JBOD	Just a bunch of disks (aka linear RAID), combines several disks into a single logical one.

What would you do to recover a lost the root password to a Unix/Linux system? Write a locking function in bash What is a pre-emptive kernel, what does that mean to you? What is the name and location of the system log on a Unix or Linux system? What would you do to recover a lost the root password to a Unix/Linux system?

2

Networking

2.1 Resources

Books

1. Beginning Linux Programming (3rd)
2. Unix Network Programming
3. Networking for System Administrators
4. Unix & Linux System Administration Handbook, 4^{th}

Links

1. **Network Questions:** https://github.com/kylejohnson/linux-sysadmin-interview-questions/blob/master/test.md

2.2 Connections

Sockets

1	Def	A unix file type with duplex communication
2	Use	Communicating between processes
3	List Sockets	TCP/UDP → Socklist, all → netstat & ss
4	Listening TCP Sockets	netstat -tl

- Attributes: Domain, Type, Protocol
  - Domain → Address family (UNIX → AF_UNIX, TCP/IP → AF_INET, etc)

  - Type → Communication characteristics
    * Stream Sockets (SOCK_STREAM) → Sequenced & reliable 2 way byte stream. Large messages fragmented, transmitted, & reassembled. Order of packets is guarenteed
    * Datagram Sockets (SOCK_DGRAM) → Doesn't establish & maintain a connection. Unsequenced & unreliable.
  - Protocol → UNIX and TCP/IP sockets dont require protocols → use 0 for the default

- Communication Protocols
  1. UDP → AF_INET domain with SOCK_DGRAM connection type
  2. TCP/IP → AF_INET domain with SOCK_STREAM connection type
  3. Others exist, but are less common

TCP/IP

The application determines which communication protocol is more appro- priate. On the Web, you normally do not want data to go missing during transmission (a piece of text, image, or downloaded software might get lost, with annoying to catastrophic results), hence TCP is the correct choice. For television or voice chat, it is usually preferrable to live with small breaks in the service (a pixellated picture or a brief burst of static) than for everything to grind to a halt while the system arranges for a missing datagram to be

1	IP Packet	A data packet sent by the TCP or UDP protocol. Contains header info and data. 20 header bytes and variable number of data bytes
2	Local host	Means *this computer*, connects to the loopback address → 127.0.0.1 - 127.255.255.254 (IPv4) & ::1 (IPv6)
3	ARP	Address resolution protocol. Maps an address (like IPv4 address) to a device (like a MAC address). Same for IPv6 this is done by NDP (see below)
4	NDP	Neighbor Discovery Protocol, removes necessity of DHCP for configuring hosts, although DHCPv6 does exist
5	MAC Address	Media access control address. Unique identifier assigned to network interfaces for communications at the data link layer of a network segment. Also known as Ethernet hardware address (EHA), hardware address or physical address. MAC addresses are supposedly unique world wide. Find current mac w/ arp
6	Find an IP or site name	dig <site name>/<ip address>

7	Find site info from DNS	whois <site name>
8	DHCP/DHCPv6	Dynamic Host Configuration Protocol. Standard network protocol for IP. Dynamically distributes network configuration parameters, such as IP addresses, for interfaces and services
9	Default Gateway	Path to reach all none local connections. Computer → Def Gateway (usually a router) → ... → destinations router → destination. Use rout to find gw address
10	NAT	Network address translation. Rerouting IP addresses so that there is only 1 internet routable IP for an entire private network. Used synonomously w/ IP masquarading. Used due to IPv4 exhaustion.
11	IPoAC	IP over Avian Carriers. IP packets carried by pigeon. Mike Tyson IT.
12	Subnet mask	Defines locally reachable connections. etc 192.168.178.0/24 means the first 24 bits are masked away and only the last 8 bits are locally reachable. So 192.168.178.0 to 192.168.178.255 can be reached locally
13	CIDR	Classless Inter-Domain Routing. Page 456 Unix & Linux System Administration Handbook, 4^{th}. AKA supernetting**{FIXME: EXPAND}**

Internet

1	HTTP/HTTPS	Hyper text transfer protocol / secure. Request - response protocl for server-client computing.
2	SMTP	Secure messeging transfer protocol
3	DNS	Domain name service, look up IP addresses from human readable names. Use whois or dig as a cmd line tool.

Tools

1	ifconfig	Network configuration & querying the setup of a network interface

2	ip	
3	whois	
4	arp	
5	route	
6	traceroute	
7	Ping	Uses the control protocol, ICMP, see if communication is possible. Use ping6 to test IPv6 connections

2.3 Remote Connections

SSH

1	Encryption	All communiucations are encryted → handshake determines the encryption protocol and proime number, they then share the public keys and keep a secret key
2	Keys	Secret & public key. Put public key on sever, server sends message to client, client uses secret key to send a return message which confirms the connection.
3	Generating keys	ssh-keygen -t dsa
4	X forwarding	-X (unencrypted), -Y (encrypted)
5	File transfer	SFTP/SCP are the ssh tunnel file transfers, sftp being the upgraded version of scp.
6	SSH Hardening	1. Disable SSH protocol 1 2. Reduce the grace time (time to login) 3. Use TCP wrappers (always good to check) 4. Increase key strength (maybe go to 2048-bit keys) 5. Check the defaults and disable a few options

TLS/SSL

1	TLS	Transport Layer Security
2	SSL	Secure Sockets Layer
3	Encryption	By key pairing
4	Digital certificates	relies on a set of trusted third-party certificate authorities to establish the authenticity of certificates. Ensures that the public key holder is who they claim to be (perventing man in the middle attacks)
5	File transfer	FTPS → FTP SSL or HTTPS → HTTP SSL (or secure, etc)

FTP & Telnet

1	FTP	File transfer protocol. Often used with SSL liscences for FTPS
2	Telnet	Provides cmd line access to a remote host like ssh. Security concerns has made ssh the prefered communication method

Mail Servers

1	SMTP	
2	SMTP relay	
3	MX record	
4	SMTP sending a message	
5	SMTP	

OSI

Using the OSI model, which layer has the responsibility of making sure that the packet gets where it is supposed to go?

1	ISO OSI reference model	Open Systems Interconnection model. 7 layers each of which only see 1 up and 1 down.

Unknowns

Which IP ranges/subnets are "private" or "non-routable" (RFC 1918)? What is a packet filter and how does it work? What is a proxy and how does it work? Explain asynchronous routing? A TCP connection on a network can be uniquely defined by 4 things. What are those things? When a client running a web browser connects to a web server, what is the source port of the connection? What is the destination port of the connection? What is an A record? What is an NS record? What is a PTR record? What is a DNS forwarder? What is meant by "Reverse Lookup"? What is LDAP and what is it used for? What is a DN in LDAP? What is IDS? What is IPS? What is the difference between IDS and IPS? What is meant by the term "DOS Attack"? How does a switch get a mac address? What type of packet to discover a router? How does traceroute work?

1		

3

Programming

3.1 GIT

Setup

1	Get a repo	git clone
2	Make a repo	git init
3	Pull an existing repo	Use init or clone the repo then pull
4	Remote repos	git remote → lists the remote repos, git remote add "name" "url"
5	Configuration	git config → complicated, but add email and user with git config –global user.email & user.name

3.2 Terms

Programming

1	Agile	See below 3.2

1. **Agile:** Software development strategy. Values:
   a) **Individuals and Interactions** over processes and tools
      i. Pair programming → 1 station 2 programmers, driver & navigator/observer
      ii. Colocation → Team members in the same area
   b) **Working Software** over comprehensive documentation

c) **Customer Collaboration** over contract negotiation

d) **Responding to Change** over following a plan

3.3 C/C++

3.4 Python

3.5 MySQL

Start mysql server: rcmysql start