*What is Linux?
Ans. Linux is an operating system based on UNIX and was first introduced by Linus Torvalds. It is based on the Linux Kernel and can run on different hardware platforms manufactured by Intel, MIPS, HP, IBM, SPARC, and Motorola. Another popular element in Linux is its mascot, a penguin figure named Tux.

*What is the difference between UNIX and LINUX?
Ans.

Sr. No.	Key	Linux	Unix
1	Development	Linux is open source and is developed by Linux community of developers.	Unix was developed by AT&T Bell labs and is not open source.
2	Cost	Linux is free to use.	Unix is licensed OS.
3	Supportd File systems	Ext2, Ext3, Ext4, Jfs, ReiserFS, Xfs, Btrfs, FAT, FAT32, NTFS.	fs, gpfs, hfs, hfs+, ufs, xfs, zfs.
4	GUI	Linux uses KDE and Gnome. Other GUI supported are LXDE, Xfce, Unity, Mate.	Unix was initially a command based OS. Most of the unix distributions now have Gnome.
5	Usage	Linux is used in wide varieties from desktop, servers, smartphones to mainframes.	Unix is mostly used on servers, workstations or PCs.
6	Default Shell	Bash (Bourne Again SHell) is default shell for Linux.	Bourne Shell is default shell for Unix.
7	Target processor	Linux was initially developed for Intel's x86 hardware processors. Now it supports 20+ processor families.	CUnix supports PA-RISC and Itanium family.
8	Example	Ubuntu, Debian GNU, Arch Linux, etc.	SunOS, Solaris, SCO UNIX, AIX, HP/UX, ULTRIX etc.

*What is BASH?
Ans. BASH is short for Bourne Again SHell. It was written by Steve Bourne as a replacement to the original Bourne Shell (represented by /bin/sh). It combines all the features from the original version of Bourne Shell, plus additional functions to make it easier and more convenient to use. It has since been adapted as the default shell for most systems running Linux.

*What is Linux Kernel?
Ans. The Linux Kernel is a low-level systems software whose main role is to manage hardware resources for the user. It is also used to provide an interface for user-level interaction.

*What is LILO?
Ans. LILO is a boot loader for Linux. It is used mainly to load the Linux operating system into main memory so that it can begin its operations.

*What is a swap space?
Ans. Swap space is a certain amount of space used by Linux to temporarily hold some programs that are running concurrently. This happens when RAM does not have enough memory to hold all programs that are executing.

*What is the advantage of open source?
Ans. Open source allows you to distribute your software, including source codes freely to anyone who is interested. People would then be able to add features and even debug and correct errors that are in the source code. They can even make it run better and then redistribute these enhanced source code freely again. This eventually benefits everyone in the community.

*What are the basic components of Linux?
Ans. Just like any other typical operating system, Linux has all of these components: kernel, shells and GUIs, system utilities, and an application program. What makes Linux advantageous over other operating system is that every aspect comes with additional features and all codes for these are downloadable for free.

*Does it help for a Linux system to have multiple desktop environments installed?
Ans. In general, one desktop environment, like KDE or Gnome, is good enough to operate without issues. It's all a matter of preference for the user, although the system allows switching from one environment to another. Some programs will work in one environment and not work on the other, so it could also be considered a factor in selecting which environment to use.

*Which are the Shells used in Linux?
Ans. The most common Shells used in Linux are
bash: Bourne Again Shell is the default for most of the Linux distributions
ksh: Korn Shell is a high-level programming language shell
csh: C Shell follows C like syntax and provides spelling correction and Job Control
zsh: Z Shell provides some unique features such as filename generation, startup files, login/logout watching, closing comments etc.
fish: Friendly Interactive Shell provides some special features like web-based configuration, auto-suggestions, fully scriptable with clean scripts

*What is the importance of the GNU project?
Ans. This so-called Free software movement allows several advantages, such as the freedom to run programs for any purpose and freedom to study and modify a program to your needs. It also allows you to redistribute copies of software to other people, as well as the freedom to improve software and have it released for the public.

*Describe the root account.
Ans. The root account is like a systems administrator account and allows you full control of the system. Here you can create and maintain user accounts, assigning different permissions for each account. It is the default account every time you install Linux.
*What is CLI?
Ans. CLI is short for Command Line Interface. This interface allows the user to type declarative commands to instruct the computer to perform operations. CLI offers greater flexibility. However, other users who are already accustomed to using GUI find it difficult to remember commands including attributes that come with it.

*What is GUI?
Ans. GUI, or Graphical User Interface, make use of images and icons that users click and manipulate as a way of communicating with the computer. Instead of having to remember and type commands, the use of graphical elements makes it easier to interact with the system, as well as adding more attraction through images, icons, and colors.

*How can you find out how much memory Linux is using?
Ans. From a command shell, use the "concatenate" command: cat /proc/meminfo for memory usage information. You should see a line starting something like Mem: 64655360, etc. This is the total memory Linux thinks it has available to use.

You can also use commands
free - m
vmstat
top
htop
to find current memory usage

*What is a typical size for a swap partition under a Linux system?
Ans. The preferred size for a swap partition is twice the amount of physical memory available on the system. If this is not possible, then the minimum size should be the same as the amount of memory installed.

*What is an inode?
The inode is a database that describes the file/directory attributes such as metadata and the physical location on the hard drive.

*What are symbolic links?
Ans. Symbolic links are essentially shortcuts that reference to a file instead of its inode value.This method can be applied to directories and can reference across different hard disks/volumes.

*What are hard links?
Ans. hard link is a direct reference to a file via its inode. You can also only hardlink files and not directories.

*How do you change permissions under Linux?
Ans. Assuming you are the system administrator or the owner of a file or directory, you can grant permission using the chmod command. Use + symbol to add permission or – symbol to deny permission, along with any of the following letters: u (user), g (group), o (others), a (all), r (read), w (write) and x (execute). For example, the command chmod go+rw FILE1.TXT grants read and write access to the file FILE1.TXT, which is assigned to groups and others.

*In Linux, what names are assigned to the different serial ports?
Ans. Serial ports are identified as /dev/ttyS0 to /dev/ttyS7. These are the equivalent names of COM1 to COM8 in Windows.

*How do you access partitions under Linux?
Ans. Linux assigns numbers at the end of the drive identifier. For example, if the first IDE hard drive had three primary partitions, they would be named/numbered, /dev/hda1, /dev/hda2 and /dev/hda3.

*What is the maximum length for a filename under Linux?
Any filename can have a maximum of 255 characters. This limit does not include the path name, so therefore the entire pathname and filename could well exceed 255 characters.

*What are filenames that are preceded by a dot
Ans. In general, filenames that are preceded by a dot are hidden files. These files can be configuration files that hold important data or setup info. Setting these files as hidden makes it less likely to be accidentally deleted.

*Explain virtual desktop.
Ans. This serves as an alternative to minimizing and maximizing different windows on the current desktop. Using virtual desktops can clear the desktop when you can open one or more programs. Rather than minimizing/restoring all those programs as needed, you can simply shuffle between virtual desktops with programs intact in each one.

*How do you share a program across different virtual desktops under Linux?
Ans. To share a program across different virtual desktops, in the upper left-hand corner of a program window look for an icon that looks like a pushpin. Pressing this button will "pin" that application in place, making it appear in all virtual desktops, in the same position onscreen.

*What is the pwd command?
Ans. The pwd command is short for print working directory command.
Example:

```
pwd
```

Output:

```
/home/guru99/myDir
```

*What are daemons?
Ans. Daemons are services that provide several functions that may not be available under the base operating system. Its main task is to listen for service request and at the same time to act on these requests. After the service is done, it is then disconnected and waits for further requests.
OR
A daemon is a computer program that runs as a background process to provide functions that might not be available in the base Operating System. Daemons are usually used to run services in the background without directly being in control of interactive users. The purpose of Daemons are to handle periodic requests and then forward the requests to appropriate programs for execution.
*What are the kinds of permissions under Linux?
Ans. There are 3 kinds of permissions under Linux:- Read: users may read the files or list the directory- Write: users may write to the file of new files to the directory- Execute: users may run the file or lookup a specific file within a directory

*How does case sensitivity affect the way you use commands?
Ans. When we talk about case sensitivity, commands are considered identical only if every character is encoded as is, including lowercase and uppercase letters. This means that CD, cd, and Cd are three different commands. Entering a command using uppercase letters, where it should be in lowercase, will produce different outputs.

*What are environmental variables?
Ans. Environmental variables are global settings that control the shell's function as well as that of other Linux programs. Another common term for environmental variables is global shell variables.

*What are the different modes when using vi editor?
Ans.Command Mode/Regular Mode: It is the default mode for the vi editors. It is generally used to type commands that usually perform particular or specific vi functions. To enter this mode from another mode (Insert mode), one must press [esc]. In simple words, it lets you view the content.

Insertion Mode/Edit Mode: This mode allows you to do text editing, or type text into a file. To enter this mode from another mode (command mode), one must press [esc]. In simple words, it lets you delete or insert text or content.

Ex Mode/Replacement Mode: This mode is generally used to save the files and execution of the commands. It basically executes files with different parameters. To enter this mode, one must press [:]. In simple words, it lets you overwrite content or text.

*Is it possible to use shortcuts for a long pathname?
Ans. Yes, there is. A feature known as filename expansion allows you do this using the TAB key. For example, if you have a path named /home/iceman/assignments directory, you would type as follows: /ho[tab]/ice[tab]/assi[tab] . This, however, assumes that the path is unique and that the shell you're using supports this feature.

*What is redirection?
Ans. Redirection is the process of directing data from one output to another. It can also be used to direct an output as an input to another process.

*What is grep command?
Ans. grep a search command that makes use of pattern-based searching. It makes use of options and parameters that are specified along with the command line and applies this pattern in searching the required file output.
Grep stands for Global Regular Expression Print. The grep command is used to search for a text in a file by pattern matching based on regular expression.

*What are the contents of /usr/local?
Ans. It contains locally installed files. This directory matters in environments where files are stored on the network. Specifically, locally-installed files go to /usr/local/bin, /usr/local/lib, etc.). Another application of this directory is that it is used for software packages installed from source, or software not officially shipped with the distribution.

*How do you terminate an ongoing process?
Ans. Every process in the system is identified by a unique process id or pid. Use the kill command followed by the pid to terminate that process. To terminate all process at once, use kill 0.

*How do you insert comments in the command line prompt?
Ans. Comments are created by typing the # symbol before the actual comment text. This tells the shell to completely ignore what follows. For example "# This is just a comment that the shell will ignore."

*What is command grouping and how does it work?
Ans. You can use parentheses to group commands. For example, if you want to send the current date and time along with the contents of a file named OUTPUT to a second file named MYDATES, you can apply command grouping as follows: (date cat OUTPUT) > MYDATES

*Write a command that will look for files with an extension "c", and has the occurrence of the string "apple" in it.
 Ans. Find ./ -name "*.c" | xargs grep –i "apple"

* Write a command that will display all .txt files, including its individual permission.
Ans. ls -al *.txt

*Write a command that will do the following:
-look for all files in the current and subsequent directories with an extension c,v
-strip the,v from the result (you can use sed command)
-use the result and use a grep command to search for all occurrences of the word ORANGE in the files.
Ans. Find ./ -name "*.c,v" | sed 's/,v//g' | xargs grep "ORANGE"

*What is the command to calculate the size of a folder?
Ans. To calculate the size of a folder uses the command du –sh folder1.

*How can you find the status of a process?
Ans. Use the command "ps ux"

*How can you check the memory status?
Ans. You can use the command
free -m to display output in MB
free -g to display output in GB

*How can you append one file to another in Linux?
Ans. To append one file to another in Linux you can use command cat file2 >> file 1. The operator >> appends the output of the named file or creates the file if it is not created. While another command cat file 1 file 2 > file 3 appends two or more files to one.
*Explain how you can find a file using Terminal?
Ans. To find a file you have to use a command, find . –name "process.txt" . It will look for the current directory for a file called process.txt.

*Explain how you can create a folder using Terminal?
Ans. To create a folder, you have to use command mkdir. It will be something like these: ~$ mkdir Guru99

*Explain how you can view the text file using Terminal?
Ans. To view the text file, go to the specific folder where the text files are located by using the command cd and then type less filename.txt.

*Explain how to enable curl on Ubuntu LAMP stack?
Ans. To enable curl on Ubuntu, first, install libcurl, once done use following command
sudo/etc/init .d /apache2 restart or sudo service apache2 restart.

*Explain how to enable root logging in Ubuntu?
Ans. The command which enables root logging is
#sudo sh-c 'echo "greater-show-manual-login=true" >>/etc/lightdm/lightdm.conf'

*How can you run a Linux program in the background simultaneously when you start your Linux Server?
Ans. By using nohup. It will stop the process receiving the NOHUP signal and thus terminating it you log out of the program which was invoked with. & runs the process in the background.

*What are the process states in Linux?
Ans. The process states are as follows:
Ready: The process is created and is ready to run
Running: The process is being executed
Blocked or wait: Process is waiting for input from the user
Terminated or Completed: Process completed execution, or was terminated by the Operating System
Zombie: Process terminated, but the information still exists in the process table.

Zombie processes usually occur for child processes, as the parent process still needs to read its child's exit status. This is known as reaping the zombie process.

*Explain Process Management System Calls in Linux
Ans. The System Calls to manage the process are:
fork () : Used to create a new process
exec() : Execute a new program
wait() : Wait until the process finishes execution
exit() : Exit from the process
And the System Calls used to get Process ID are:
getpid():- get the unique process id of the process
getppid():- get the parent process unique id

*Explain Regular Expressions and Grep
Ans. Regular Expressions are used to search for data having a particular pattern. Some of the commands used with Regular Patterns are: tr, sed, vi and grep.

Some of the common symbols used in Regular Expressions are:

∧	Match the beginning of the String
$	Match the end of the String
*	Match zero or more characters
?	Match exactly one character

*What is the minimum number of disk partitions required to install Linux?
Ans. The minimum number of partitions required is 2.
One partition is used as the local file system where all the files are stored. This includes files of the OS, files of applications and services, and files of the user. And the other partition is used as Swap Space which acts as an extended memory for RAM.

*What is the export command used for?
Ans. The export command is used to set and reload the environment variables. For example, if you want to set the Java path, then the command would be:

```
$ export JAVA_HOME = /home/user/Java/bin
```

*What is netstat command in Linux?
Ans. netstat command gives various information about the network and routing tables, interface statics and more about the system.

*What is lsof command in Linux?
Ans. lsof means List of file, we can know which file is opened by which process.
lsof

*What are the features of the Linux operating system?
Ans. Following are the features of the Linux Operating System
Portable: Software can work on different types of hardware in the same way. It can carry easily in pen drives and memory cards.
Open Source: Source code available for free, and its community-based development project.
Multi-User: Multiple users can use ram, applications and run programs at the same time.
Multiprogramming: Multiple program or applications can run at the same time.
Shell: It has a special interpreter program where you can execute programs and commands of the system.
Security: It provides authentication, authorization, and encryption to provide security to the data.

*Describe how a parent and child process communicates each other?
Ans. Parent process communicates with the child process by using pipes, sockets, messages queues and more.

*How to copy text to the clipboard?
Ans: Use this command: cat file.txt | xclip -selection clipboard
*How do you check resources usage?
Ans: Use this command to check resource usage: /usr/bin/time -v ls

*How do you run a command for a limited time?
Ans: Use this command: timeout 10s ./script.sh

*Restart every 30 minutes
Ans. while true; do timeout 30m ./script.sh; done

*How to put never expiry to a user?
Ans. # passwd -x -1 <user login name> How to put never expiry to a user?

*How can you make a service run automatically after boot?
Ans. # chkconfig <service name> on

*How to check whether the ssh is running or not on the remote host?
Ans. # nmap -p 22 <IP address of the remote host> (to see the ssh is running or not on remote system)

*How to check the remote server services are running or not?
Ans. Nmap servername portname

*Step out if you are facing too many file system while login via ssh?
Ans. Lsof |wc –l (list of open files)

*How to disable direct root login?
Ans. Using /etc/ssh/sshd_config
*Kernel path
Ans. /boot/grub/grub.cfg

*What is linux library file extension,
Ans. .so

*Which is the best command that can be used for checking selinux activation status
Ans. getenforce

*My command ‘setenforce 0’ is not working, what to do?
Ans. Edit /etc/selinux/config and change the enforcement to disabled and reboot the server.

*What are the known commands for disk partitioning?
Ans. fdisk, parted

###BASIC LINUX COMMANDS###

1. tty - reveals the current terminal
2. whoami - reveals the currently logged-in user
3. which - reveals where in the search path a program is located
4. echo - prints to the screen
4a. echo $PATH - dumps the current path to STDOUT
4b. echo $PWD - dumps ths contents of the $PWD variable
4c. echo $OLDPWD - dumps the most recently visited directory
5. set - prints and optionally sets shell variables
6. clear - clears the screen or terminal
7. reset - resets the screen buffer
8. history - reveals your command history
8a. !690 - executes the 690th command in our history
8b. history command is maintained on a per-user basis via:~/.bash_history
8c   ~ = users's $HOME directory in the BASH shell
9. pwd - prints the working directory
10. cd - changes directory to desired directory
10a. 'cd ' with no options changes to the $HOME directory
10b. 'cd ~' changes to the $HOME directory
10c. 'cd /' changes to the root of the file system
10d. 'cd Desktop/' changes us to the relative directory 'Desktop'
10e. 'cd ..' changes us one-level up in the directory tree
10f. 'cd ../..' changes us two-levels up in the directory tree
11. Arrow keys (up and down) navigates through your command history
12. BASH supports tab completion:type unique characters in the command and press 'Tab' key
13. You can copy and paste in GNOME terminal windows using:
  a. left button to copy or ctrl-C to
  b. right button to paste OR Ctrl-Shift-v to paste
14. ls - lists files and directories
 a. ls / - lists the contents of the '/' mount point
 b. ls -l - lists the contents of a directory in long format:Includes: permissions, links, ownership, size, date, name
 c. ls -ld /etc - lists properties of the directory '/etc', NOT the contents of '/etc'
 d. ls -ltr - sorts chronologically from older to newer (bottom)
 e. ls --help - returns possible usage information
 f. ls -a - reveals hidden files. e.g. '.bash_history'
 g. ls ?a*
 h. ls ???
 i. ls a* starting with a OR anywhere a *a OR in betw*a*

Note: files/directories prefixed with '.' are hidden. e.g. '.bash_history'

15. cat - catenates files
 a. cat 123.txt - dumps the contents of '123.txt' to STDOUT
 b. cat 123.txt 456.txt dumps both files to STDOUT
 c. cat 123.txt 456.txt > 123456.txt - creates new catenated file
d. cat 123.txt 456.txt >> appends a file

16. mkdir - creates a new directory
 a. mkdir test5 - creates a single directory with the name specified
c. mkdir -p test1/test2/test3/ will create nested directories

17. cp - copies files
 a. cp 123.txt test/ By default, 'cp' does NOT preserve the original modification time
 b. cp -v 456.txt test
18. mv - moves files and renames files
 a. mv 123456.txt test - moves the file, preserving time

19. rm - removes files/directories
 a. rm 123.txt
 b. rm -rf 456.txt - removes recursively and enforces

20. touch - creates blank file/updates timestamp
 a. touch test.txt - will create a zero-byte file, if it doesn't exist
 b. touch 123456.txt - if exists update the timestamp
 c. touch -t 200801091530 123456.txt - changes timestamp

21. stat - reveals statistics of files
 a. stat 123456.txt - reveals full attributes of the file

22. find - finds files using search patterns
 a. find / -name 'fstab'
Note: 'find' can search for fields returned by the 'stat' command

23. alias - returns/sets aliases for commands
 a. alias - dumps current aliases
 b. alias copy='cp -v'

###Linux Redirection & Pipes###
Ability to control input and output

Input redirection '<':
 1. cat < 123.txt
Note: Use input redirection when program does NOT default to file as input

Output redirection '>':
 1. cat 123.txt > onetwothree.txt
Note: Default nature is to:
 1. Clobber the target file
 2. Populate with information from input stream

Append redirection '>>':

1. cat 123.txt >> numbers.txt - creates 'numbers.txt' if it doesn't exist, or appends if it does

2. cat 456.txt >> numbers.txt

Pipes '|':
Connects the output stream of one command to the input stream of a subsequent command

1. cat 123.txt | sort
2. cat 456.txt 123.txt | sort
3. cat 456.txt 123.txt | sort | grep 3

###Command Chaining###

1. Permits the execution of multiple commands in sequence
2. Also permits execution based on the success or failure of a previous command

1. cat 123.txt ; ls -l - this runs first command, then second command without regards for exit status of the first command

2. cat 123.txt && ls -l - this runs second command, if first command is successful
3. cat 123.txt || ls -l - this runs second command, if first command fails

24. more|less - paginators, which display text one-page @ a time
 1. more /etc/fstab
 2. less 1thousand.txt

25. seq - echoes a sequence of numbers
 a. seq 1000 > 1thousand.txt - creates a file with numbers 1-1000

26. su - switches users
 a. su - with no options attempts to log in as 'root'

27. head - displays opening lines of text files
 a. head /var/log/messages

28. tail - displays the closing lines of text files
 a. tail /var/log/messages

29. wc - counts words and optionally lines of text files
 a. wc -l /var/log/messages7
 b. wc -l 123.txt

30. file - determines file type
 a. file /var/log/messages

---

*Boot process of Linux
Ans. 1.The computer's BIOS performs POST.
2.BIOS reads the MBR for the bootloader.
3.GRUB 2 bootloader loads the vmlinuz kernel image.
4.GRUB 2 extracts the contents of the initramfs image.
5.The kernel loads driver modules from initramfs.
6.Kernel starts the system's first process, systemd.
7.The systemd process takes over. It:
Reads configuration files from the /etc/systemd directory
Reads file linked by /etc/systemd/system/default.target
Brings the system to the state defined by the system target
Executes /etc/rc.local

*File system of Linux
Ans. Ext, Ext2, Ext3 and Ext4 file system
JFS File System
ReiserFS File System
XFS File System
Btrfs File System
Swap File System

*What is sticky bit
A Sticky bit is a permission bit that is set on a file or a directory that lets only the owner of the file/directory or the root user to delete or rename the file. No other user is given privileges to delete the file created by some other user.

*What is SUID in Linux?
SUID(Set-user Identification) and SGID(Set-group identification) are two special permissions that can be set on executable files, and These permissions allow the file being executed to be executed with the privileges of the owner or the group. SUID: It is special file permission for executable files.

*Port no of protocols
Ans. ftp 20/21
ssh 22
telnet 23
smtp 25
dns 53
dhcp 67/68
tftp 69
http 80
https 443
pop 110
ntp 123
imap 143
snmp 161/162
bgp 179
ldap 389
tls/ssl 989/990
irc 194
netbios 135-139

*What is tcpdump ? Why it is used?

Ans. tcpdump is a data-network packet analyzer computer program that runs under a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

*What is OS Hardening? Tell me different OS Hardening points ?

Ans. Hardening of the OS is the act of configuring an OS securely, updating it, creating rules and policies to help govern the system in a secure manner, and removing unnecessary applications and services. This is done to minimize a computer OS's exposure to threats and to mitigate possible risk.

1. Install security updates and patches
2. Use strong passwords
3. Implement a firewall
4. Keep things clean
5. Limit access
6. Create backups (and test!)
7. Perform system auditing
8. Disable all unnecessary services.
9. Remove all unnecessary executables and registry entries

*Difference between Centos 6 and Centos 7

Features	RHEL 7	RHEL 6
Default File System	XFS	EXT4
Kernel Version	3.10.x-x kernel	2.6.x-x Kernel
Kernel Code Name	Maipo	Santiago
General Availability Date of First Major Release	2014-06-09 (Kernel Version 3.10.0-123)	2010-11-09 (Kernel Version 2.6.32-71)
First Process	systemd (process ID 1)	init (process ID 1)
Runlevel	runlevels are called as "targets" as shown below: runlevel0.target -> poweroff.target runlevel1.target -> rescue.target runlevel2.target -> multi-user.target runlevel3.target -> multi-user.target runlevel4.target -> multi-user.target runlevel5.target -> graphical.target runlevel6.target -> reboot.target /etc/systemd/system/default.target (this by default is linked to the multi-user.target OR graphical.target)	Traditional runlevels defined : runlevel 0 runlevel 1 runlevel 2 runlevel 3 runlevel 4 runlevel 5 runlevel 6 and the default runlevel would be defined in "/etc/inittab" file.
Host Name Change	In Red Hat Enterprise Linux 7, as part of the move to the new init system (systemd), the hostname variable is defined in "/etc/hostname" file.	In Red Hat Enterprise Linux 6, the hostname variable was defined in the "/etc/sysconfig/network" configuration file.
Change In UID Allocation	By default a new user created would get UIDs assigned starting from 1000. This could be changed in "/etc/login.defs" file if required.	Default UID assigned to users would start from 500. This could be changed in "/etc/login.defs" file if required.

Max Supported File Size	Maximum (individual) file size = 500TB Maximum filesystem size = 500TB (This maximum file size is only on 64-bit machines. Red Hat Enterprise Linux does not support XFS on 32-bit machines.)	Maximum (individual) file size = 16TB Maximum filesystem size = 16TB (This maximum file size is based on a 64-bit machine. On a 32-bit machine, the maximum files size is 8TB.)
File System Check	"xfs_repair" XFS does not run a file system check at boot time.	"e2fsck" File system check would gets executed at boot time.
Differences Between xfs_repair & e2fsck	"xfs_repair" - Inode and inode blockmap (addressing) checks. - Inode allocation map checks. - Inode size checks. - Directory checks. - Pathname checks. - Link count checks. - Freemap checks. - Super block checks.	"e2fsck" - Inode, block, and size checks. - Directory structure checks. - Directory connectivity checks. - Reference count checks. - Group summary info checks.
Difference Between xfs_growfs & resize2fs	"xfs_growfs" xfs_growfs takes mount point as arguments.	"resize2fs" resize2fs takes logical volume name as arguments.
Change In File System Structure	/bin, /sbin, /lib, and /lib64 are now nested under /usr.	/bin, /sbin, /lib, and /lib64 are usually under /
Boot Loader	GRUB 2 Supports GPT, additional firmware types, including BIOS, EFI and OpenFirmware. Ability to boot on various file systems (xfs, ext4, ntfs, hfs+, raid, etc)	GRUB 0.97
KDUMP	RHEL7 supports kdump on large memory based systems up to 3 TB	Kdump doesn’t work properly with large RAM based systems.
System & Service Manager	"Systemd" systemd is a system and service manager for Linux, and replaces SysV and Upstart used in previous releases of Red Hat Enterprise Linux. systemd is compatible with SysV and Linux Standard Base init scripts.	Upstart
Enable/Start Service	For RHEL 7, the systemctl command replaces service and chkconfig. - Start Service : "systemctl start nfs-server.service". - Enable Service : To enable the service (example: nfs service) to start	Using "service" command and "chkconfig" commands. - Start Service : "service nfs start" OR "/etc/init.d/nfs start" - Enable Service : To start with specific runlevel : "chkconfig --level 3

	automatically on boot : "systemctl enable nfs-server.service". Although one can still use the service and chkconfig commands to start/stop and enable/disable services, respectively, they are not 100% compatible with the RHEL 7 systemctl command	5 nfs on"
Default Firewall	"Firewalld (Dynamic Firewall)" The built-in configuration is located under the "/usr/lib/firewalld" directory. The configuration that you can customize is under the "/etc/firewalld" directory. It is not possible to use Firewalld and Iptables at the same time. But it is still possible to disable Firewalld and use Iptables as before.	Iptables
Network Bonding	"Team Driver" -/etc/sysconfig/network-scripts/ifcfg-team0 - DEVICE=”team0” - DEVICETYPE=”Team”	"Bonding" -/etc/sysconfig/network-scripts/ifcfg-bond0 - DEVICE=”bond0”
Network Time Synchronization	Using Chrony suite (faster time sync compared with ntpd)	Using ntpd
NFS	NFS4.1 NFSv2 is no longer supported. Red Hat Enterprise Linux 7 supports NFSv3, NFSv4.0, and NVSv4.1 clients.	NFS4
Cluster Resource Manager	Pacemaker	Rgmanager
Load Balancer Technology	Keepalived and HAProxy	Piranha
Desktop/GUI Interface	GNOME3 and KDE 4.10	GNOME2
Default Database	MariaDB is the default implementation of MySQL in Red Hat Enterprise Linux 7	MySQL
Managing Temporary Files	RHEL 7 uses systemd-tmpfiles (more structured, and configurable, method to manage tmp files and directories).	Using "tmpwatch"

*Difference between centos 7 and centos 8

Feature	CentOS 7	CentOS 8
Kernel	Based on Fedora 19 and upstream kernel 3.10	Based on Fedora 28 and upstream kernel 4.18
Git	Git version 1.8	Git version 2.18
Security	Comes with support for OpenSSL 1.0.1 and TLS 1.0	Comes with support for OpenSSL 1.1.1 and TLS 1.3, TLS 1.0 and TLS 1
Software Management	Used YUM v3, distributed with RPM 4.11	YUM package manager is now based on the DNF technology and it provides support for modular content. Uses YUM v4, distributed with RPM 4.14

httpd/Apache	HTTP Server 2.4	HTTP Server 2.4
Python	Python 2.7.5 and limited support for Python 2.7	Python 3.6 and limited support for Python 2.7
php, ruby, perl	PHP 5.4.16, Ruby 2.0.0, Perl 5.16.3	PHP 7.2, Ruby 2.5, Perl 5.26. PHP uses FastCGI Process Manager (FPM) by default
Desktop Environment	Default GNOME Display Manager is X.Org server	Default GNOME Display Manager is Wayland, GNOME Shell version 3.28
Databases	MySQL 5.5, MariaDB 5.5, PostgreSQL 9.2	MariaDB 10.3, MySQL 8.0, PostgreSQL 10, PostgreSQL 9.6, and Redis 5
Virtualization	Uses qemu-kvm and virt-manager	Distributed with qemu-kvm 2.12, virt-manager deprecated and Cockpit taking over
Firewall	Uses iptables packet filtering framework	Uses nftables packet filtering framework
Nginx	Nginx not available by default.	CentOS 8 introduces Nginx web server. Version 1.14
Networking Framework	iptables	nftables which is used by firewalld as its default backend.
Java	OpenJDK 8	Both OpenJDK 11 and OpenJDK 8
NTP	Both ntp daemon and chronyd available	Only chrony NTP protocol
Storage Management	LVM default	LVM and Stratis
Containers	Docker for CentOS 7 available	Docker is not included. For working with containers, use the **podman**, **buildah**, **skopeo**, and **runc** tools.

*What are the use of /etc/fdisk
fdisk is a menu-driven program for creation and manipulation of partition tables. It understands DOS-type partition tables and BSD-type or SUN-type disklabels.
fdisk does not understand GPTs (GUID partition tables) and it is not designed for large partitions. In these cases, use the more advanced GNU parted.
fdisk does not use DOS-compatible mode and cylinders as display units by default. The old deprecated DOS behavior can be enabled with the '-c=dos -u=cylinders' command-line options.
Hard disks can be divided into one or more logical disks called partitions. This division is recorded in the partition table, found in sector 0 of the disk. In the BSD world, one talks about 'disk slices' and a 'disklabel'.

*What do you see in top command
Uptime : The first value is the system time. The second value represents how long the system has been up and running, while the third value indicates the current number of users on the system.

Average: The load average is broken down into three time increments. The first shows the load for the last one minute, the second for the last five minutes, and the final value for the last 15 minutes. The results are a percentage of CPU load between 0 and 1.0. The processor is likely overworked if 1.0 (or higher) is displayed.

```
top - 23:03:09 up 4 min, 1 user, load average: 0.75, 0.59, 0.25
```

Tasks: The second line is the Tasks output, and it's broken down into five states. These five states display the status of processes on the system:

total shows the sum of the processes from any state.

running shows how many processes are handling requests, executing normally, and have CPU access.

sleeping indicates processes awaiting resources, which is a normal state.

stopped reports processes exiting and releasing resources; these send a termination message to the parent process.

zombie refers to a process waiting for its parent process to release it; it may become orphaned if the parent exits first.
Zombie processes usually mean an application or service didn't exit gracefully. A few zombie processes on a long-running system are not usually a problem.

%Cpu(s): They provide insight into exactly what the CPUs are doing.

MiB Memory: The first line—MiB Mem—displays physical memory utilization.

MiB Swap: Linux can take advantage of virtual memory when physical memory space is consumed by borrowing storage space from storage disks. The process of swapping data back and forth between physical RAM and storage drives is time-consuming and uses system resources, so it's best to minimize the use of virtual memory.

*Where is password stored for any user
A shadow password file, also known as /etc/shadow, is a system file in Linux that stores encrypted user passwords and is accessible only to the root user, preventing unauthorized users or malicious actors from breaking into the system.
The common practice of storing passwords in the /etc/passwd file leaves the Linux system vulnerable to break-in attempts. To eliminate this vulnerability, newer Linux systems use the /etc/shadow file to store user passwords instead.
Traditional password files are maintained in /etc/passwd, but the actual hashed passwords are stored in /etc/shadow.

*what can be the reasons if I'm unable to connect to a server remotely?
ANS.There could be many reason that you may not be able to take remote connection to server.
1.It could be that sufficient Permission are not give to have access to the server remotely.
2If the permission are given then it could be connectivity issue,firewall blocking the required.
3.It Could be due to Group policy to deny the remote connection and many more

*User is unable to login to domain- what could be the reasons?
ANS.There could be many reasons as below.
1.Connectivity issue with DC due to dns misconfig.
2.Account lockout or in disable state.
3.DC unreaachable due physical connectivity issue.
4.Domain PC secure channel broken with DC.
5.Cleint PC n/w cable unplugged
6.User account deleted from AD and many more

*What is kernel compilation ?
Ans. Kernel Compilation means converting this C code of the kernel to low level assembly instructions, so that one can use this code and run it on a computer. ... There are programmers who like to - say, change the way the Kernel or Operating System runs on their computer. Compilation is the process of changing a higher level program (that us humans can write, understand) to low level instructions that a machine can understand.

*What is a she bang value ?
Ans. It is called a shebang or a "bang" line. It is nothing but the absolute path to the Bash interpreter. It consists of a number sign and an exclamation point character (#!), followed by the full path to the interpreter such as /bin/bash. All scripts under Linux execute using the interpreter specified on a first line.

*From where and how to check system logs ?
Ans. The most common log files are:
/var/log/boot.log: System Boot log (the boot log stores all information related to booting operations)
/var/log/auth.log: Auth logs (the authentication log stores all authentication logs, including successful and failed attempts)
/var/log/httpd/: Apache access and error logs
/var/log/mysqld.log: MySQL database server log file
/var/log/debug: Debug logs (the debug log stores detailed messages related to debugging and is useful for troubleshooting specific system operations)
/var/log/daemon.log: Daemon logs (the daemon log contains information about events related to running the Linux operation)
/var/log/maillog: Mail server logs (the mail log stores information related to mail servers and archiving emails)
/var/log/kern.log: Kernel logs (the kernel log stores information from the Ubuntu Linux kernel)
/var/log/yum.log: Yum command logs

*What will you use to view a specific users 3 days back activities?
Ans. cat /home/aaronkilik/.bash_history

*What is patching how often it should be done ? Is it done manually or automatically?
Ans. Sometimes patches add new features to a package and this can be when issues occur. Adding new features can cause things to break (usually due to broken configuration files).

Automatic patch advantages
1The tools apply patches to the operating system to fix newly discovered security or performance bugs.
2They also often update applications that are installed on the system, even if they are not part of the operating system itself.
3No matter which operating system you use, automatic updates can help to ensure that your software is protected against security vulnerabilities and other problems.
Automatic patch disadvantage
1They may not keep all of the software on your system up-to-date. Even if they patch most of your applications, some applications may be managed by other update tools. Some may not have any auto-update facility at all. For this reason, automatic updates can create a false sense of security if you rely on them alone.
2Automatic updates usually can’t update firmware or other special types of files. These updates need to be applied manually, or via special tools.
3An up-to-date system is not necessarily immune to every possible security vulnerability. There may be undiscovered vulnerabilities that have not yet been patched. This is another way in which update tools can breed false sense of security.
4Updates often take a long time to download and install. In the meantime, normal workloads are interrupted. It is usually not possible to know exactly how long an update will take until it is already in progress, and some update tools don’t let you configure which times of day updates are applied.

Manual patch advantage

1Patches can be held during busy/quiet periods.

2The admin can ensure that services are always restarted to use the patch.

3The admin can search for dependant applications that maybe using a library that has been patched (e.g. glibc patches)

4The admin is already logged onto the server ready to act in case something does break.

*Difference between snapshot revert and snapshot backup ? Can we recover after deleting vmware with snapshot ?

1. Backup :

Backup generally suggests the duplicate of your data. When a backup is initiated, it generates copies of your files, comprising files pertaining to your website and mailboxes. These copies are conventionally kept in a different location than the original content, thus making them ideal for disaster rehabilitation. Backups are the mechanism that could take minutes, hours, or days to complete, depending on the data. This conveys that the data at the end of the backup may not be compatible with the data at the time when the backup initiated. Backups are planned to be stored for long periods of time and, if they are stored off server, they can be used to restore servers after a server failure.

2. Snapshot :

Snapshot refers to an instantaneous “picture” of your server’s file system at a certain period of time. This picture apprehends the entire file system as it was when the snapshot was taken. When a snapshot is accustomed to restore the server, the server will revert to exactly how it was at the time of the snapshot. Snapshots are designed for short term storage. When space departs, new snapshots eventually overwrite older ones. For this reason, snapshots are usually only good if you want to revert to a recent version of your server.

*Difference between /bin and /sbin files ?

/bin This directory contains executable programs which are needed in single user mode and to bring the system up or repair it.

/sbin Like /bin, this directory holds commands needed to boot the system, but which are usually not executed by normal users.

*What is a umask value ? What umask value does root and a normal used contains

Ans. Umask, or the user file-creation mode, is a Linux command that is used to assign the default file permission sets for newly created folders and files. The term mask references the grouping of the permission bits, each of which defines how its corresponding permission is set for newly created files. The bits in the mask may be changed by invoking the umask command.

0 : read, write and execute
1 : read and write
2 : read and execute
3 : read only
4 : write and execute
5 : write only
6 : execute only
7 : no permissions

The default umask 002 used for normal user. With this mask default directory permissions are 775 and default file permissions are 664. The default umask for the root user is 022 result into default directory permissions are 755 and default file permissions are 644

*Explain about firewalls & IPtables?
Firewall:

Pros
Changes are done and effected immediately without rebooting the system.
It makes adapting firewall settings easy for applications, services and users.
Its interface is user friendly and easy to understand
It is free to download and use on any Linux device
Cons
For a user who has adapted to running the Linux kernel firewall directly through iptables, it would be difficult to make the switch to firewalld.

Iptables
Pros
It is a rather versatile control tool for the command line.
It allows the user to tweak all aspects of the Linux firewall
Its basic concepts are fairly easy to understand
There is an extensive, free and openly available array of documentation about it which allows the user to study iptables straight from the source
Cons
The system needs to restart in order to effect system changes
It is fairly difficult to use

*What is network bonding or teaming?
Ans. When a system administrator wants to increase the bandwidth available and provide redundancy and load balancing for data transfers, a kernel feature known as network bonding allows to get the job done in a cost-effective way.
In simple words, bonding means aggregating two or more physical network interfaces (called slaves) into a single, logical one (called master). If a specific NIC (Network Interface Card) experiences a problem, communications are not affected significantly as long as the other(s) remain active.

*What is KVM or virtualization
Ans. Kernel-based Virtual Machine (KVM) is an open source virtualization technology built into Linux®. Specifically, KVM lets you turn Linux into a hypervisor that allows a host machine to run multiple, isolated virtual environments called guests or virtual machines (VMs).

*What is grub boot configuration? How to use system rescue?
Ans. GRUB stands for GRand Unified Bootloader. Its function is to take over from BIOS at boot time, load itself, load the Linux kernel into memory, and then turn over execution to the kernel. Once the kernel takes over, GRUB has done its job and it is no longer needed. GRUB supports multiple Linux kernels and allows the user to select between them at boot time using a menu

*What is the difference between TCP and UDP ?

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).
TCP has a (20-80) bytes variable length header.	UDP has a 8 bytes fixed length header.
TCP is heavy-weight.	UDP is lightweight.
TCP doesn’t supports Broadcasting.	UDP supports Broadcasting.
TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

*Different types of RAIDS ? Which is the best raid to use ?
Ans. The abbreviation stands for either Redundant Array of Independent Drives. A RAID system consists of two or more drives working in parallel. These can be hard discs, but there is a trend to also use the technology for SSD (Solid State Drives). There are different RAID levels, each optimized for a specific situation.
RAID 0 – striping
RAID 1 – mirroring
RAID 5 – striping with parity
RAID 6 – striping with double parity
RAID 10 – combining mirroring and striping

*Difference between Load Average and CPU Usage ?
Ans. CPU usage: There ratio (usually expressed as a percentage)of time that the CPU is busy doing stuff. This measure only makes sense if you know over which period the percentage is being calculated.
Load: Average queue length for the CPU - including the process currently executing. For this to make sense, you need to know the period over which this is being measured.
They are related, but one does not necessarily correlate to the other.

*If a system has crashed and KDump file has generated how would you up the system ?
Ans. Kdump is a kernel crash dumping mechanism that allows you to save the contents of the system’s memory for later analysis.Kdump uses kexec to boot into a second kernel whenever system crashes. This second kernel, often called the crash kernel, boots with very little memory and captures the dump image.

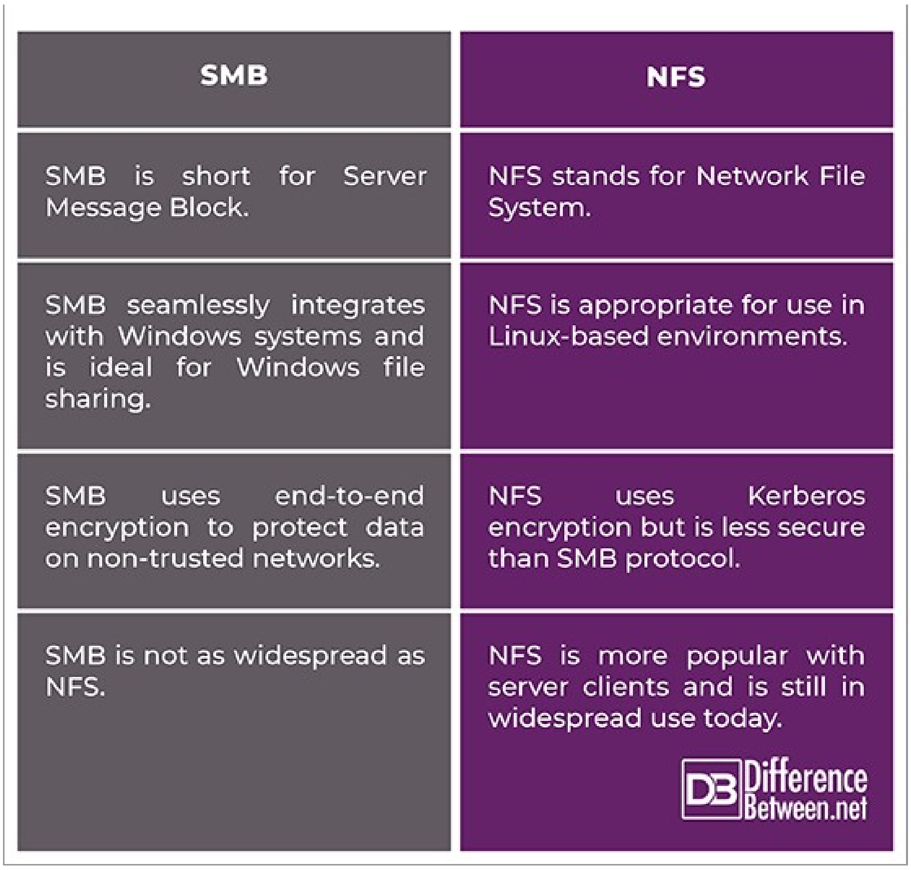
The first kernel reserves a section of memory that the second kernel uses to boot. Kexec enables booting the capture kernel without going through the BIOS, so contents of the first kernel's memory are preserved, which is essentially the kernel crash dump

*What is inode number ? Difference between PID and Inode number ?
Ans. An Inode number is a uniquely existing number for all the files in Linux and all Unix type systems.
When a file is created on a system, a file name and Inode number is assigned to it.
Generally, to access a file, a user uses the file name but internally file name is first mapped with respective Inode number stored in a table.

*What all commands you have used for network management ?
Ans. Ping, netstat, arp, tracert, host, nslookup, traceroute(tracert are computer network diagnostic commands for displaying possible routes and measuring transit delays of packets across an Internet Protocol network)

*If df cmd shows my /var is used 8GB out of 10GB and du command shows 9GB out of 10GB ? What could be the reason?
Ans. Basically, df reads the superblock only and trusts it completely. du reads each object and sums them up.
du == Disk Usage. It walks through directory tree and counts the sum size of all files therein. It may not output exact information due to the possibility of unreadable files, hardlinks in directory tree, etc. It will show information about the specific directory requested. Think, "How much disk space is being used by these files?"
df == Disk Free. Looks at disk used blocks directly in filesystem metadata. Because of this it returns much faster that du but can only show info about the entire disk/partition. Think, "How much free disk space do I have?"

*Diffrence between samba and nfs?



SMB	NFS
SMB is short for Server Message Block.	NFS stands for Network File System.
SMB seamlessly integrates with Windows systems and is ideal for Windows file sharing.	NFS is appropriate for use in Linux-based environments.
SMB uses end-to-end encryption to protect data on non-trusted networks.	NFS uses Kerberos encryption but is less secure than SMB protocol.
SMB is not as widespread as NFS.	NFS is more popular with server clients and is still in widespread use today.

*What is yum?
Ans. yum is the primary tool for getting, installing, deleting, querying, and managing Red Hat Enterprise Linux RPM software packages from official Red Hat software repositories, as well as other third-party repositories. yum is used in Red Hat Enterprise Linux versions 5 and later. Versions of Red Hat Enterprise Linux 4 and earlier used up2date.

* What is grep?
Ans. The grep filter searches a file for a particular pattern of characters, and displays all lines that contain that pattern. The pattern that is searched in the file is referred to as the regular expression (grep stands for globally search for regular expression and print out).

* Types of Backup?
Ans.
Full backups - A full backup is the most basic of all backup types. And as its name suggests, it's also the most comprehensive. In a full data or system backup, all data is copied to another location.
Advantage: A complete copy of all data is available in one location and restoration time is minimal.
Disadvantage: A full backup takes longer to execute than other types of backups.

Incremental backups - This type only backs up the information that has changed since the last backup occurred.
Advantage: Because only the changed data is being backed up, an incremental backup can be carried out as often as needed. Incremental backups are completed quickly and require fewer resources.
Disadvantage: While incremental backups have the fastest backup time, they also boast the slowest data recovery time.

Differential backups - Similar to an incremental backup, a differential backup copies all data changed since the last full backup every time it is run.
Advantage: A differential backup provides a way of backing up changed data to the same convenient location as all new data.
Disadvantage: A differential backup requires more time and space to complete.

*What is LVM
Ans. LVM stands for Large Volume Management. LVM allows for very flexible disk space management. It provides features like the ability to add disk space to a logical volume and its filesystem while that filesystem is mounted and active and it allows for the collection of multiple physical hard drives and partitions into a single volume group which can then be divided into logical volumes.

*What are network topologies
Ans. Bus Topology: nodes are connected using the central link known as the bus.
Star Topology: nodes are connected to one single node known as the central node.
Ring Topology: node is connected to exactly two nodes forming a ring structure
Mesh Topology: node is connected to one or many nodes.
Tree Topology: star and bus topology also know as an extended bus topology.
Hybrid: combination of different topologies to form a new topology

*What are Private and Special IP addresses?

Private Address: For each class, there are specific IPs that are reserved specifically for private use only. This IP address cannot be used for devices on the Internet as they are non-routable.

IPv4 Class	Private IPv4 Start Address	Private IPv4 End Address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
B	192.168.0.0	192.168.255.255

IPv4 Class	IPv4 Start Address	IPv4 End Address	Usage
A	0.0.0.0	127.255.255.255	Used for Large Network
B	128.0.0.0	191.255.255.255	Used for Medium Size Network
C	192.0.0.0	223.255.255.255	Used for Local Area Network
D	224.0.0.0	239.255.255.255	Reserved for Multicasting
E	240.0.0.0	255.255.255.254	Study and R&D

*What is the difference between LDAP and Active Directory?

Active Directory

Active Directory, AD for short, is a directory server developed by Microsoft that allows storing directory service information such as users and devices in a centralized and hierarchical database. AD comes with many services such as authentication, access policies, and group management.

LDAP

Lightweight Directory Access Protocol (LDAP) is a protocol that applications can use to speak to directory services such as Active Directory. The LDAP protocol queries user information to read, modify or update it.

During user authentication, LDAP can bind to the directory service database, such as Active Directory. While advanced ways of authentication such as Kerberos token and client certificate are possible, the simplest authentication is simply checking the username and password the user entered into the application log-in form against the information stored in a directory server.

*What do forest, trees, domain mean ?

A domain is a logical group of network objects like computers , users, devices that have the same active directory database . A tree is a collection of domains within a Microsoft active directory network in which each domain has exactly one parent, leading to hierarchical tree structure and forest is a group of active directory trees.

*According to you what is the difference between FAT and NTFS ?

FAT :-

- There is no security when the user logs in locally .
- It usually supports file names that have only 8 characters .
- it does not support file compression .
- The partition and file size can be up to 4 GB.
- There is no such security permission for file and folder level .
- It doesn’t support bad cluster mapping so it is not very reliable

NTFS :-

- There is security for both the local and the remote users.
- It usually supports file names that have 255 characters .
- It supports the file compression
- The partition size can be upto 16 exabyte .
- There is security for file and folder level.
- It supports bad cluster mapping and transaction logging so it is highly reliable

*What do you know about proxy servers ?

It acts as the gateway between a local network (for eg:- computers in a company) and a large-scale network (for ex :- internet). By using this server there is an increase in performance and security as it can be used to prevent the employees from browsing the inappropriate and distracting sites .

*What is the difference between a work group and a domain ?
In a workgroup there is a particular system which has the collection of systems having their own rules and local users logins. Whereas in domain the centralized authentication server which is a collection of systems tells what the rules are . Workgroups are like P2P networks whereas on the flip side domains are like standard client /server relationships

*What can you tell us about the light – weight directory access protocol ?
The LDAP (light-weight directory access protocol) is used to name the object in an AD(Active Directory) and makes it widely accessible for management and query applications . it is most commonly used to provide a central place to store the usernames and passwords

*What is IP Spoofing and what can we do to prevent it ?
It is a type of mechanism that is used by the attackers to get the authorized access to the system. In this the intruder is sending the message to the computer with an IP address that it is coming from a trusted source/host. We can prevent it by performing packet filtering using the special routers and firewalls we allow packets with recognized formats to enter the network.

*What do you know about HTTPS and what port does it use ?
The HTTPS uses the SSL certificates so as to confirm that the server you are connecting is the one that it says . the HTTPS traffic goes over the TCP port 443.

*What can you tell us about port forwarding ?
Ans :- when we want to communicate with the inside of a secured network then there is the use of a port forwarding table within the router or other connection management device that will allow the specific traffic to be automatically forwarded on to a particular destination. Most probably it does not allow access to the server from outside directly into your network.

*What is Telnet ?
It is one of the application protocols that allow the connection on any port and is a very small and versatile utility. It allows the admin to connect to the remote devices. in case telnet transfers data in the form of text. on a remote host, telnet provides access to a command-line interface because of some of the security concerns

*What are the first five commands you type on a *nix server after login?

- lsblk to see information on all block devices
- who to see who is logged into the server
- top to get a sense of what is running on the server
- df -khT to view the amount of disk space available on the server
- netstat to see what TCP network connections are active

*How do you make a process run in the background, and what are the advantages of doing so?

You can make a process run in the background by adding the special character & at the end of the command. Generally, applications that take too long to execute, and don't require user interaction are sent to the background so that we can continue our work in the terminal.

*Running these commands as root a good or bad idea?

Running (everything) as root is bad due to two major issues. The first is *risk*. Nothing prevents you from making a careless mistake when you are logged in as root. If you try to change the system in a potentially harmful way, you need to use sudo, which introduces a pause (while you're entering the password) to ensure that you aren't about to make a mistake.

The second reason is *security*. Systems are harder to hack if you don't know the admin user's login information. Having access to root means you already have one half of the working set of admin credentials.

*What is the difference between rm and rm -rf?

The rm command by itself only deletes the named files (and not directories). With -rf you add two additional features: The -r, -R, or --recursive flag recursively deletes the directory's contents, including hidden files and subdirectories, and the -f, or --force, flag makes rm ignore nonexistent files, and never prompt for confirmation.

Compress.tgz has a file size of approximately 15GB. How can you list its contents, and how do you list them only for a specific file?

To list the file's contents:

```
tar tf archive.tgz
```

To extract a specific file:

```
tar xf archive.tgz filename
```

* What is RAID? What is RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10?

A RAID (Redundant Array of Inexpensive Disks) is a technology used to increase the performance and/or reliability of data storage. The RAID levels are:

- RAID 0: Also known as disk striping, which is a technique that breaks up a file, and spreads the data across all of the disk drives in a RAID group. There are no safeguards against failure. (Citation)
- RAID 1: A popular disk subsystem that increases safety by writing the same data on two drives. Called *mirroring*, RAID1 does not increase write

performance, but read performance may increase up to the sum of each disks' performance. Also, if one drive fails, the second drive is used, and the failed drive is manually replaced. After replacement, the RAID controller duplicates the contents of the working drive onto the new one.

- RAID 5: A disk subsystem that increases safety by computing parity data and increasing speed. RAID 5 does this by interleaving data across three or more drives (striping). Upon failure of a single drive, subsequent reads can be calculated from the distributed parity such that no data is lost.
- RAID 6: Which extends RAID 5 by adding another parity block. This level requires a minimum of four disks, and can continue to execute read/write with any two concurrent disk failures. RAID 6 does not have a performance penalty for reading operations, but it does have a performance penalty on write operations because of the overhead associated with parity calculations.
- RAID 10: Also known as RAID 1+0, RAID 10 combines disk mirroring and disk striping to protect data. It requires a minimum of four disks, and stripes data across mirrored pairs. As long as one disk in each mirrored pair is functional, data can be retrieved. If two disks in the same mirrored pair fail, all data will be lost because there is no parity in the striped sets. (Citation)

*Which port is used for the ping command?
The ping command uses ICMP. Specifically, it uses ICMP echo requests and ICMP echo reply packets.

ICMP does not use either UDP or TCP communication services: Instead, it uses raw IP communication services. This means that the ICMP message is carried directly in an IP datagram data field.

*What is the difference between a router and a gateway? What is the default gateway?
Router describes the general technical function (layer 3 forwarding), or a hardware device intended for that purpose, while *gateway* describes the function for the local segment (providing connectivity to elsewhere). You could also state that you "set up a router as a gateway." Another term is *hop*, which describes forwarding between subnets.

The term *default gateway* is used to mean the router on your LAN, which has the responsibility of being the first point of contact for traffic to computers outside the LAN.

* Explain the boot process for Linux.

BIOS -> Master Boot Record (MBR) -> GRUB -> the kernel -> init -> runlevel

* How do you check the error messages while the server is booting up?
Kernel messages are always stored in the kmsg buffer, visible via the dmesg command.

Boot issues and errors call for a system administrator to look into certain important files, in conjunction with particular commands, which are each handled differently by different versions of Linux:

- /var/log/boot.log is the system boot log, which contains all that unfolded during the system boot.

- /var/log/messages stores global system messages, including the messages logged during system boot.
- /var/log/dmesg contains kernel ring buffer information.

* Explain the boot process for Linux.

BIOS -> Master Boot Record (MBR) -> GRUB -> the kernel -> init -> runlevel*

*How do you check the error messages while the server is booting up?
Kernel messages are always stored in the kmsg buffer, visible via the dmesg command.
Boot issues and errors call for a system administrator to look into certain important files, in conjunction with particular commands, which are each handled differently by different versions of Linux:

- /var/log/boot.log is the system boot log, which contains all that unfolded during the system boot.
- /var/log/messages stores global system messages, including the messages logged during system boot.
- /var/log/dmesg contains kernel ring buffer information.

* How do you change kernel parameters? What kernel options might you need to tune?
To set the kernel parameters in Unix-like systems, first edit the file /etc/sysctl.conf. After making the changes, save the file and run the sysctl -p command. This command makes the changes permanent without rebooting the machine

* Explain the /proc filesystem.
The /proc filesystem is virtual, and provides detailed information about the kernel, hardware, and running processes. Since /proc contains virtual files, it is called the *virtual file system*. These virtual files have unique qualities. Most of them are listed as zero bytes in size.

Virtual files such as /proc/interrupts, /proc/meminfo, /proc/mounts and /proc/partitions provide an up-to-the-moment glimpse of the system's hardware. Others, such as /proc/filesystems and the /proc/sys directory provide system configuration information and interfaces.

* How do you run a script as another user without their password?
For example, if you were editing the sudoers file (such as /private/etc/sudoers), you might use visudo to add the following:

```
user1 ALL=(user2) NOPASSWD: /opt/scripts/bin/generate.sh
```

* What is the UID 0 toor account? Have you been compromised?
The toor user is an alternative superuser account, where toor is root spelled backward. It is intended to be used with a non-standard shell, so the default shell for root does not need to change.

This purpose is important. Shells which are not part of the base distribution, but are instead installed from ports or packages, are installed in /usr/local/bin; which, by default, resides on a different file system. If root's shell is located in /usr/local/bin and the file system containing /usr/local/bin is not mounted, root could not log in to fix a problem, and the sysadmin would have to reboot into single-user mode to enter the shell's path.

* How does tracert work and what protocol does it use?
The command tracert—or traceroute depending on the operating system—allows you to see exactly what routers you touch as you move through the chain of connections to your final destination. If you end up with a problem where you can't connect to or ping your final destination, a tracert can help in that you can tell exactly where the chain of connections stops. (Citation)

With this information, you can contact the correct people; whether it be your own firewall, your ISP, your destination's ISP, or somewhere in the middle. The tracert command—like ping—uses the ICMP protocol, but also can use the first step of the TCP three-way handshake to send SYN requests for a response.

* What is the main advantage of using chroot? When and why do we use it? What is the purpose of the mount /dev, mount /proc, and mount /sys commands in a chroot environment?
An advantage of having a chroot environment is that the filesystem is isolated from the physical host, since chroot has a separate filesystem inside your filesystem. The difference is that chroot uses a newly created root (/) as its root directory.
A chroot jail lets you isolate a process and its children from the rest of the system. It should only be used for processes that don't run as root, as root users can break out of the jail easily.
The idea is that you create a directory tree where you copy or link in all of the system files needed for the process to run. You then use the chroot() system call to tell it the root directory now exists at the base of this new tree, and then start the process running in that chroot'd environment. Since the command then can't reference paths outside the modified root directory, it can't perform operations (read, write, etc.) maliciously on those locations. (Citation)

* How do you protect your system from getting hacked?
By following the principle of least privileges and these practices:

- Encrypt with public keys, which provides excellent security.
- Enforce password complexity.
- Understand why you are making exceptions to the rules above.
- Review your exceptions regularly.
- Hold someone to account for failure. (It keeps you on your toes.) (Citation)

* What is LVM, and what are the advantages of using it?
LVM, or Logical Volume Management, uses a storage device management technology that gives users the power to pool and abstract the physical layout of component storage devices for easier and flexible administration. Using the device mapper Linux kernel framework, the current iteration (LVM2) can be used to gather existing storage devices into groups and allocate logical units from the combined space as needed.

* What are sticky ports?
Sticky ports are one of the network administrator's best friends and worst headaches. They allow you to set up your network so that each port on a switch only permits one (or a number that you specify) computer to connect on that port, by locking it to a particular MAC address.

* Explain port forwarding?
When trying to communicate with systems on the inside of a secured network, it can be very difficult to do so from the outside—and with good reason. Therefore, the use of a port forwarding table within the router itself, or other connection management device, can allow specific traffic to automatically forward to a particular destination. For example, if you had a web server running on your network and you wanted to grant access to it from the outside, you would set up port forwarding to port 80 on the server in question. This would mean that anyone entering your IP address in a web browser would connect to the server's website immediately.

Please note, it is usually not recommended to allow access to a server from the outside directly into your network.

* What is a false positive and false negative in the case of IDS?
When the Intrusion Detection System (IDS) device generates an alert for an intrusion which has actually not happened, this is false positive. If the device has not generated any alert and the intrusion has actually happened, this is the case of a false negative.

* What is OOM killer and how does it decide which process to kill first?
If memory is exhaustively used up by processes to the extent that possibly threatens the system's stability, then the out of memory (OOM) killer comes into the picture.
An OOM killer first has to select the best process(es) to kill. *Best* here refers to the process which will free up the maximum memory upon being killed, and is also the least important to the system. The primary goal is to kill the least number of processes to minimize the damage done, and at the same time maximize the amount of memory freed.
To facilitate this goal, the kernel maintains an oom_score for each of the processes. You can see the oom_score of each of the processes in the /proc filesystem under the pid directory:

```
$ cat /proc/10292/oom_score
```

The higher the value of oom_score for any process, the higher its likelihood is of being killed by the OOM Killer in an out-of-memory situation.

Jenkins

1. What is Jenkins?

Jenkins is a self-contained, open-source automation server that can be used to automate all sorts of tasks related to building, testing, and delivering or deploying software. Jenkins can be installed through native system packages, Docker, or even run standalone by any machine with a Java Runtime Environment (JRE) installed.

2. Tell me something about Continuous Integration, Continuous Delivery, and Continuous Deployment?

Continuous Integration: A software development process where the changes made to software are integrated into the main code as and when a patch is ready so that the software will be always ready to be - built, tested, deployed, monitored - continuously.

Continuous Delivery: This is a Software Development Process where the continuously integrated (CI) changes will be tested & deployed continuously into a specific environment, generally through a manual release process, after all the quality checks are successful

Continuous Deployment: A Software Development practice where the continuously integrated (CI) changes are deployed automatically into the target environment after all the quality checks are successful

3. What is a Jenkins job?

A Job/Project is the fundamental unit of a logical work (like a software build, an automation task, test execution, etc) using the Jenkins automation server and other required plugins, configurations & infrastructures.

Jobs can be of different types like - a freestyle project, a multi-configuration project, a pipeline project, a multi-branch project, etc.

4. Define the process of Jenkins.

- First, a developer commits the code to the source code repository. Meanwhile, the Jenkins server checks the repository at regular intervals for changes.
- Soon after a commit occurs, the Jenkins server detects the changes that have occurred in the source code repository. Jenkins will pull those changes and will start preparing a new build.
- If the build fails, then the concerned team will be notified.
- If the build is successful, then Jenkins deploys the build in the test server.
- After testing, Jenkins generates feedback and then notifies the developers about the build and test results.
- It will continue to check the source code repository for changes made in the source code and the whole process keeps on repeating.

5. What are the pre-requisites for using Jenkins?

The answer to this is pretty straightforward. To use Jenkins you require:

- A source code repository which is accessible, for instance, a Git repository.

6. What is the relation between Hudson and Jenkins?

You can just say Hudson was the earlier name and version of current Jenkins. After some issues, they renamed the project from Hudson to Jenkins.

7. Mention some of the useful plugins in Jenkins

Below I have mentioned some important Plugins:

- Maven 2 project
- Git
- Amazon EC2
- HTML publisher
- Copy artifact
- Join
- Green Balls

8. What are the two components that you can integrate Jenkins with?

According to me, the integration of Jenkins is possible with the following:

- Version Control system like GIT, SVN.
- Build tools like Apache Maven.

9. How will you define Post in Jenkins?

Post is a section that contains several additional steps that might execute after the completion of the pipeline. The execution of all the steps within the condition block depends upon the completion status of the pipeline. The condition block includes the following conditions – changed success,

10. What are Parameters in Jenkins?

Parameters are supported by Agent section and they are used to support various use-cases pipelines. Parameters are defined at the top-level of the pipeline or inside an individual stage directive.

11. How Can You Clone A Git Repository Via Jenkins?

If you want to clone a Git repository via Jenkins, you have to enter the e-mail and user name for your Jenkins system. Switch into your job directory and execute the "git config" command for that.

12. How to create a backup and copy files in Jenkins?

To create a backup all you need to do is to periodically back up your JENKINS_HOME directory. This contains all of your build jobs configurations, your slave node configurations, and your build history. To create a back-up of your Jenkins setup, just copy this directory. You can also copy a job directory to clone or replicate a job or rename the directory.

13. What you do when you see a broken build for your project in Jenkins?

I will open the console output for the broken build and try to see if any file changes were missed. If I am unable to find the issue that way, then I will clean and update my local workspace to replicate the problem on my local and try to solve it.

14. What are the various ways in which build can be scheduled in Jenkins?

You can schedule a build in Jenkins in the following ways:

- By source code management commits
- After completion of other builds
- Can be scheduled to run at a specified time (crons)
- Manual Build Requests

15. What is the use of Pipelines in Jenkins?

It models a series of related tasks. Pipelines help the teams to review, edit and iterate upon the tasks. Pipelines are durable and it can optionally stop and wait for human approval as well to start the next task. A pipeline is extensible and can perform work in parallel. It supports complex CD requirements.

16. Explain the terms Agent, post-section, Jenkinsfile

Agent: It is directive to tell Jenkins to execute the pipeline in a particular manner and order.

Post-section: If we have to add some notification and to perform other tasks at the end of a pipeline, post-section will definitely run at the end of every pipeline's execution.

Jenkinsfile: The text file where all the definitions of pipelines are defined is called Jenkinsfile. It is being checked in the source control repository.

17. What is the use of JENKINS HOME directory?

All the settings, logs and configurations are stored in the JENKINS_HOME directory.

18. What is a backup plugin? Why is it used?

This is a helpful plugin that backs up all the critical settings and configurations to be used in the future. This is useful in cases when there is a failure so that we don't lose the settings.

19. What is a trigger? Give an example of how the repository is polled when a new commit is detected.

Triggers are used to define when and how pipelines should be executed.

When Jenkins is integrated with an SCM tool, for example, Git, the repository can be polled every time there is a commit.

- The Git plugin should be first installed and set up.

- After this, you can build a trigger that specifies when a new build should be started. For example, you can create a job that polls the repository and triggers a build when a change is committed.

20. How do you achieve continuous integration using Jenkins?

Here are the steps –

- All the developers commit their source code changes to the shared Git repository.
- Jenkins server checks the shared Git repository at specified intervals and detected changes are then taken into the build.
- The build results and test results are shared to the respective developers
- The built application is displayed on a test server like Selenium and automated tests are run.
- The clean and tested build is deployed to the production server.

21. How do you create Multibranch Pipeline in Jenkins?

The Multibranch Pipeline project type enables you to implement different Jenkinsfiles for different branches of the same project. In a Multibranch Pipeline project, Jenkins automatically discovers, manages and executes Pipelines for branches that contain a Jenkinsfile in source control.

22. What is Groovy in Jenkins?

- Apache Groovy is a dynamic object-oriented programming language used as a scripting language for Java platforms.

23. What are the differences between Continuous Integration, Continuous Delivery, and Continuous Deployment?

Continuous Integration	Continuous Delivery	Continuous Deployment
Continuous Integration (CI) is a DevOps software development practice that permits developers to combine/merge the changes to their code in the central repository to run automated builds and tests.	Continuous Delivery (CD) refers to the building, testing, and delivering improvements to the software code. The most critical part of the CD is that the code is always in a deployable state.	Continuous Deployment (CD) is the ultimate stage in the DevOps pipeline. It refers to automatic release of any developer changes from the repository to the production stage.

24. What is a CI/CD pipeline?

CI/CD Pipeline or Continuous Integration/ Continuous Delivery is considered the DevOps approach's backbone. The pipeline is responsible for building codes, running tests, and deploying new software versions.

GIT

1. What is Git and why is it used?

- Git is the most popular, open-source, widely used, and an example of distributed version control system (DVCS) used for handling the development of small and large projects in a more efficient and neat manner.
- It is most suitable when there are multiple people working on projects as a team and is used for tracking the project changes and efficiently supports the collaboration of the development process.

2. What is a version control system (VCS)?

A VCS keeps track of the contributions of the developers working as a team on the projects. They maintain the history of code changes done and with project evolution, it gives an upper hand to the developers to introduce new code, fixes bugs, and run tests with confidence that their previously working copy could be restored at any moment in case things go wrong.

3. How is Git different from Subversion (SVN)?

GIT	SVN
Git is a distributed decentralized version control system	SVN is a centralized version control system.
Git stores content in the form of metadata.	SVN stored data in the form of files.
The master contains the latest stable release.	In SVN, the trunk directory has the latest stable release
The contents of Git are hashed using the SHA-1 hash algorithm.	SVN doesn’t support hashed contents.

4. What language is used in Git?

Git is a fast and reliable version control system, and the language that makes this possible is ‘C.’

5. What is a git repository?

A repository is a file structure where git stores all the project-based files. Git can either stores the files on the local or the remote repository.

6. What does git clone do?

The command creates a copy (or clone) of an existing git repository. Generally, it is used to get a copy of the remote repository to the local repository.

7. What does the command git config do?

The git config command is a convenient way to set configuration options for defining the behavior of the repository, user information and preferences, git installation-based configurations, and many such things.

For example:
To set up your name and email address before using git commands, we can run the below commands:

- git config --global
  user.name
  “<<your_name>>”

- git config --global user.email “<<your_email>>”

8. Can you explain head in terms of git

A head is nothing but a reference to the last commit object of a branch.

9. What does git pull origin master do?

The git pull origin master fetches all the changes from the master branch onto the origin and integrates them into the local branch.

git pull = git fetch + git merge origin/ master

10. Difference between git fetch and git pull.

Git Fetch	Git Pull
The Git fetch command only downloads new data from a remote repository.	Git pull updates the current HEAD branch with the latest changes from the remote server.
It does not integrate any of these new data into your working files.	Downloads new data and integrate it with the current working files.
Command - git fetch origin	Tries to merge remote changes with your local ones.
git fetch --all	Command - git pull origin master

11. How do you find a list of files that has been changed in a particular commit?

The command to get a list of files that has been changed in a particular commit is:

git diff-tree –r {commit hash}

- -r flag allows the command to list individual files
- commit hash lists all the files that were changed or added in the commit.

12. What is the use of the git config command?

The git config command is used to set git configuration values on a global or local level. It alters the configuration options in your git installation. It is generally used to set your Git email, editor, and any aliases you want to use with the git command.

13. What is the functionality of git clean command?

The git clean command removes the untracked files from the working directory.

14. What is SubGit and why is it used?

SubGit is a tool that is used to migrate SVN to Git. It transforms the SVN repositories to Git and allows you to work on both systems concurrently. It auto-syncs the SVN with Git.

15. If you recover a deleted branch, what work is restored?

The files that were stashed and saved in the stashed index can be recovered. The files that were untracked will be lost. Hence, it's always a good idea to stage and commit your work or stash them.

16. What is a conflict?

- Git usually handles feature merges automatically but sometimes while working in a team environment, there might be cases of conflicts such as:

  1. When two separate branches have changes to the same line in a file
  2. A file is deleted in one branch but has been modified in the other.

- These conflicts have to be solved manually after discussion with the team as git will not be able to predict what and whose changes have to be given precedence.

17. What does git status command do?

git status command is used for showing the difference between the working directory and the index which is helpful for understanding git in-depth and also keep track of the tracked and non-tracked changes.

18. What does git add command do?

- This command adds files and changes to the index of the existing directory.
- You can add all changes at once using git add . command.
- You can add files one by one specifically using git add <file_name> command.
- You can add contents of a particular folder by using git add /<folder_name>/ command

19. Why is it considered to be easy to work on Git?

With the help of git, developers have gained many advantages in terms of performing the development process faster and in a more efficient manner. Some of the main features of git which has made it easier to work are:

- Branching Capabilities:
  - Due to its sophisticated branching capabilities, developers can easily work on multiple branches for the different features of the project.
  - It also has an easier merge option along with an efficient work-flow feature diagram for tracking it.

- Distributed manner of development:
  - Git is a distributed system and due to this nature, it became easier to trace and locate data if it's lost from the main server.
  - In this system, the developer gets a repository file that is present on the server. Along with this file, a copy of this is also stored in the developer's system which is called a local repository.
  - Due to this, the scalability of the project gets drastically improved.

- Pull requests feature:
  - This feature helps in easier interaction amongst the developers of a team to coordinate merge-operations.
  - It keeps a proper track of the changes done by developers to the code.

- Effective release cycle:
  - Due to the presence of a wide variety of features, git helps to increase the speed of the release cycle and helps to improve the project workflow in an efficient manner.

20. How will you create a git repository?

- Have git installed in your system.
- Then in order to create a git repository, create a folder for the project and then run git init.
- Doing this will create a .git file in the project folder which indicates that the repository has been created.

21. Tell me something about git stash?

Git stash can be used in cases where we need to switch in between branches and at the same time not wanting to lose edits in the current branch. Running the git stash command basically pushes the current working directory state and index to the stack for future use and thereby providing a clean working directory for other tasks.

22. What is the command used to delete a branch?

- To delete a branch we can simply use the command git branch –d [head].
- To delete a branch locally, we can simply run the command: git branch -d <local_branch_name>
- To delete a branch remotely, run the command: git push origin --delete <remote_branch_name>
- Deleting a branching scenario occurs for multiple reasons. One such reason is to get rid of the feature branches once it has been merged into the development branch.

23. What differentiates between the commands git remote and git clone?

git remote command creates an entry in git config that specifies a name for a particular URL. Whereas git clone creates a new git repository by copying an existing one located at the URL.

24. What does git stash apply command do?

- git stash apply command is used for bringing the works back to the working directory from the stack where the changes were stashed using git stash command.
- This helps the developers to resume their work where they had last left their work before switching to other branches.

25. Differentiate between git pull and git fetch.

git pull	git fetch
This command pulls new changes from the currently working branch located in the remote central repository.	This command is also used for a similar purpose but it follows a two step process: 1. Pulls all commits and changes from desired branch and stores them in a new branch of the local repository. current 2. For changes to be reflected in the current / target branch, git fetch should be followed by git merge command.

git pull = git fetch + git merge

26. Can you give differences between "pull request" and "branch"?

pull request	branch
This process is done when there is a need to put a developer's change into another person's code branch.	A branch is nothing but a separate version of the code.

27. Why do we not call git "pull request" as "push request"?

- "Push request" is termed so because it is done when the target repository requests us to push our changes to it.
- "Pull request" is named as such due to the fact that the repo requests the target repository to grab (or pull) the changes from it.

28. Can you tell the difference between Git and GitHub?

Git	GitHub
This is a distributed version control system installed on local machines which allow developers to keep track of commit histories and supports collaborative work.	This is a cloud-based source code repository developed by using git.
This is maintained by "The Linux Foundation".	This was acquired by "Microsoft"
SVN, Mercurial, etc are the competitors	GitLab, Atlassian BitBucket, etc are the competitors.

- GitHub provides a variety of services like forking, user management, etc along with providing a central repository for collaborative work.

29. What do the git diff and git status commands do?

git diff	git status
This shows the changes between commits, working trees, etc.	This shows the difference between the working directory and index that is essential in understanding git in depth.

- git diff works in a similar fashion to git status with the only difference of showing the differences between commits and also between the working directory and index.

30. What has to be run to squash multiple commits (last N) into a single commit?

Squashing multiple commits to a single one overwrites the history which is why it is recommended to be done using full caution. This step can be done by running the command: git rebase -i HEAD~{{N}} where {{N}} represents the number of commits needed to be squashed.

31. How would you recover a branch that has already pushed changes in the central repository but has been accidentally deleted from every team member's local machines?

We can recover this by checking out the latest commit of this branch in the reflog and then checking it out as a new branch.

32. What is a detached HEAD and what causes this and how to avoid this?

Detached HEAD indicates that the currently checked-out repository is not a local branch. This can be caused by the following scenarios:

- When a branch is a read-only branch and we try to create a commit to that branch, then the commits can be termed as "free-floating" commits not connected to any branch. They would be in a detached state.
- When we checkout a tag or a specific commit and then we try to perform a new commit, then again the commits would not be connected to any branch. When we now try to checkout a branch, these new commits would be automatically placed at the top.

33. What does git annotate command do?

- This command annotates each line within the given file with information from the commit which introduced that change. This command can also optionally annotate from a given revision.
- Syntax: git annotate [<options>] <file> [<revision>]
- You can get to learn more about this command from the official git documentation here.

34. What is the difference between git stash apply vs git stash pop command?

- git stash pop command throws away the specified stash (topmost stash by default) after applying it.
- git stash apply command leaves the stash in the stash list for future reuse. In case we wanted to remove it from the list, we can use the git stash drop command.

git stash pop = git stash apply + git stash drop

35. What command helps us know the list of branches merged to master?

- git branch --merged helps to get the list of the branches that have been merged into the current branch.
- Note: git branch --no-merged lists the branches that have not been merged to the current branch.

36. How will you resolve conflict in Git?

- Conflicts occur whenever there are multiple people working on the same file across multiple branches. In such cases, git won't be able to resolve it automatically as it is not capable of deciding what changes has to get the precedence.
- Following are the steps are done in order to resolve git conflicts:
  1. Identify the files that have conflicts.
  2. Discuss with members who have worked on the file and ensure that the required changes are done in the file.
  3. Add these files to the staged section by using the git add command.
  4. Commit these changes using the git commit command.
  5. Finally, push the changes to the branch using the git.

37. Can you tell the differences between git revert and git reset?

git revert	git reset
This command is used for creating a new commit that undoes the changes of the previous commit.	This command is used for undoing the local changes done in the git repository
Using this command adds a new history to the project without modifying the existing history	This command operates on the commit history, git index, and the working directory.

AWS

Basic AWS Interview Questions

1. Define and explain the three basic types of cloud services and the AWS products that are built based on them?

The three basic types of cloud services are:

- Computing
- Storage
- Networking

Here are some of the AWS products that are built based on the three cloud service types:

Computing - These include EC2, Elastic Beanstalk, Lambda, Auto-Scaling, and Lightsat.

Storage - These include S3, Glacier, Elastic Block Storage, Elastic File System.

Networking - These include VPC, Amazon CloudFront, Route53

2. What is the relation between the Availability Zone and Region?

AWS regions are separate geographical areas, like the US-West 1 (North California) and Asia South (Mumbai). On the other hand, availability zones are the areas that are present inside the regions. These are generally isolated zones that can replicate themselves whenever required.

❑ **AWS Region** is a separate geographic area
❑ E.g. US-West 1 (N. California), Asia South (Mumbai)

❑ Each AWS Region has multiple isolated locations known as **Availability Zones**
❑ All availability zones inside one region are isolated from one another in terms of failure

AWS Region
Availability Zones
simplilearn

©Simplilearn. All rights reserved.

3. What is auto-scaling?

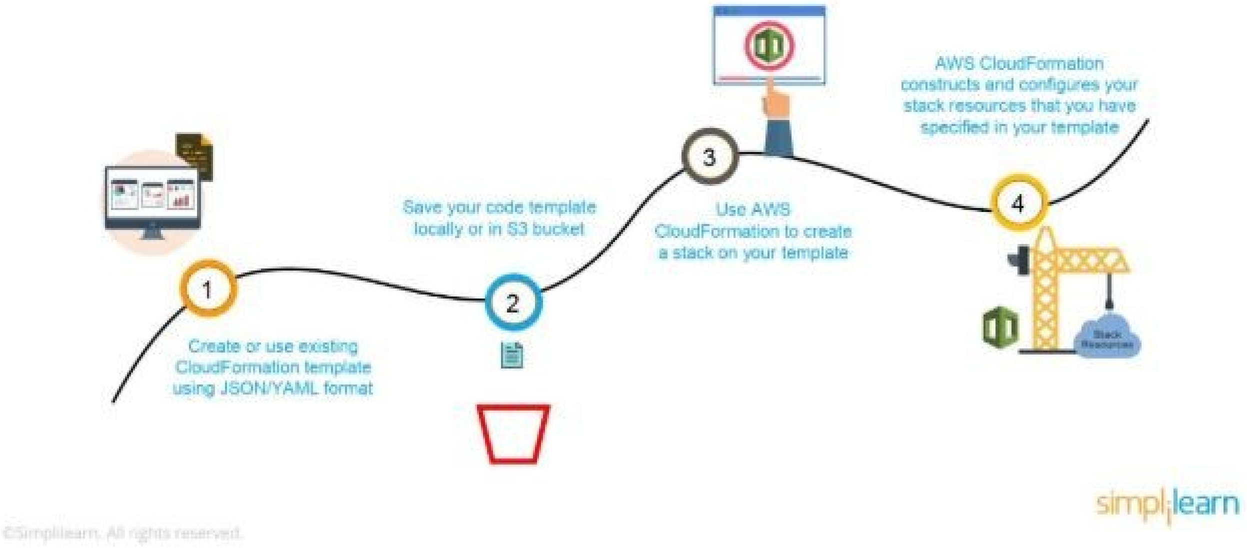
Auto-scaling is a function that allows you to provision and launch new instances whenever there is a demand. It allows you to automatically increase or decrease resource capacity in relation to the demand.

4. What is geo-targeting in CloudFront?

Geo-Targeting is a concept where businesses can show personalized content to their audience based on their geographic location without changing the URL. This helps you create customized content for the audience of a specific geographical area, keeping their needs in the forefront.

5. What are the steps involved in a CloudFormation Solution?

Here are the steps involved in a CloudFormation solution:


1
Create or use existing CloudFormation template using JSON/YAML format
2
Save your code template locally or in S3 bucket
3
Use AWS CloudFormation to create a stack on your template
4
AWS CloudFormation constructs and configures your stack resources that you have specified in your template
Stack Resources
simplilearn
©Simplilearn. All rights reserved.

1. Create or use an existing CloudFormation template using JSON or YAML format.
2. Save the code in an S3 bucket, which serves as a repository for the code.
3. Use [AWS CloudFormation](#) to call the bucket and create a stack on your template.
4. CloudFormation reads the file and understands the services that are called, their order, the relationship between the services, and provisions the services one after the other.

6. How do you upgrade or downgrade a system with near-zero downtime?

You can upgrade or downgrade a system with near-zero downtime using the following steps of migration:

- Open EC2 console
- Choose Operating System AMI
- Launch an instance with the new instance type
- Install all the updates
- Install applications
- Test the instance to see if it’s working
- If working, deploy the new instance and replace the older instance
- Once it’s deployed, you can upgrade or downgrade the system with near-zero downtime.

7. What are the tools and techniques that you can use in AWS to identify if you are paying more than you should be, and how to correct it?

You can know that you are paying the correct amount for the resources that you are using by employing the following resources:

- Check the Top Services Table

It is a dashboard in the cost management console that shows you the top five most used services. This will let you know how much money you are spending on the resources in question.

- Cost Explorer

There are cost explorer services available that will help you to view and analyze your usage costs for the last 13 months. You can also get a cost forecast for the upcoming three months.

- AWS Budgets

This allows you to plan a budget for the services. Also, it will enable you to check if the current plan meets your budget and the details of how you use the services.

- Cost Allocation Tags

This helps in identifying the resource that has cost more in a particular month. It lets you organize your resources and cost allocation tags to keep track of your AWS costs.

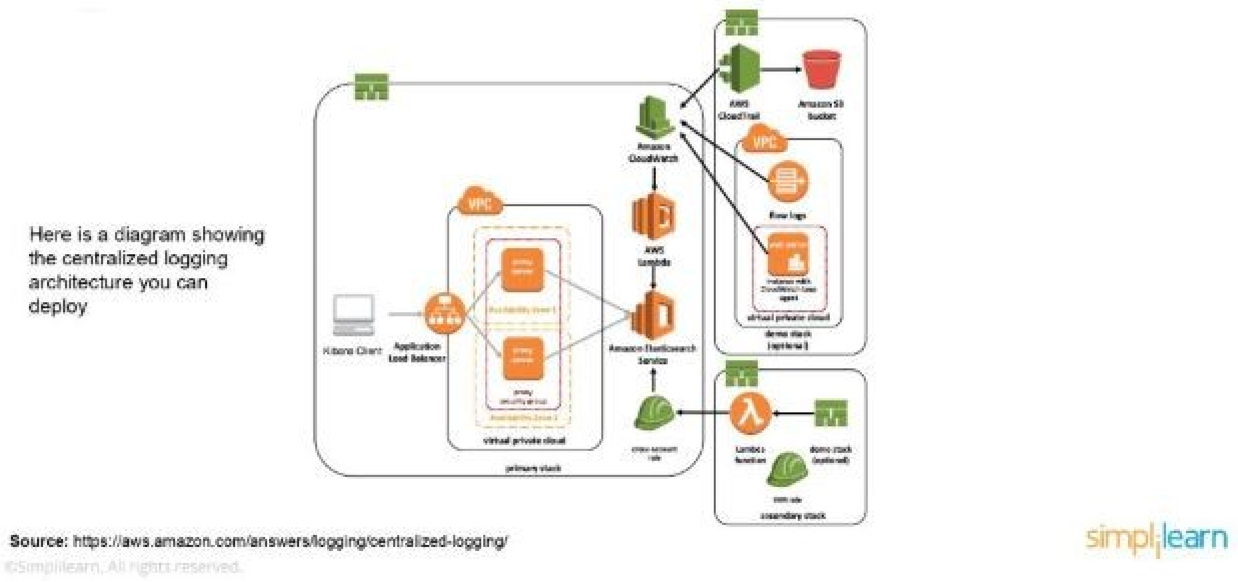
8. Is there any other alternative tool to log into the cloud environment other than console?

The that can help you log into the AWS resources are:

- Putty
- AWS CLI for Linux
- AWS CLI for Windows
- AWS CLI for Windows CMD
- AWS SDK
- Eclipse

9. What services can be used to create a centralized logging solution?

The essential services that you can use are Amazon CloudWatch Logs, store them in Amazon S3, and then use Amazon Elastic Search to visualize them. You can use Amazon Kinesis Firehose to move the data from Amazon S3 to Amazon ElasticSearch.



Here is a diagram showing the centralized logging architecture you can deploy

Source: https://aws.amazon.com/answers/logging/centralized-logging/

©Simplilearn. All rights reserved.

simplilearn

10. What are the native AWS Security logging capabilities?

Most of the AWS services have their logging options. Also, some of them have an account level logging, like in AWS CloudTrail, AWS Config, and others. Let's take a look at two services in specific:

AWS CloudTrail

This is a service that provides a history of the AWS API calls for every account. It lets you perform security analysis, resource change tracking, and compliance auditing of your AWS environment as well. The best part about this service is that it enables you to configure it to send notifications via AWS SNS when new logs are delivered.

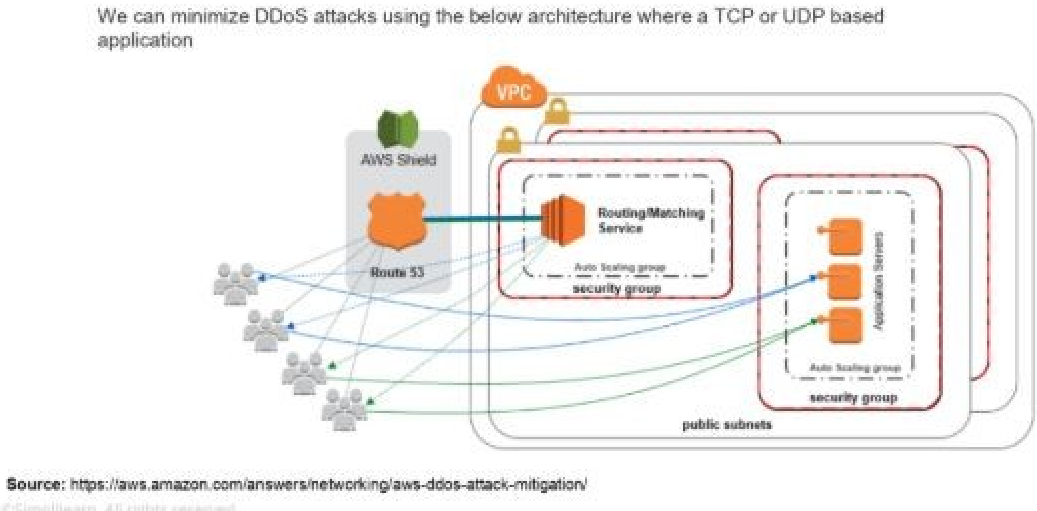
AWS Config

This helps you understand the configuration changes that happen in your environment. This service provides an AWS inventory that includes configuration history, configuration change notification, and relationships between AWS resources. It can also be configured to send information via AWS SNS when new logs are delivered.

11. What is a DDoS attack, and what services can minimize them?

DDoS is a cyber-attack in which the perpetrator accesses a website and creates multiple sessions so that the other legitimate users cannot access the service. The native tools that can help you deny the DDoS attacks on your AWS services are:

- AWS Shield
- AWS WAF
- Amazon Route53
- Amazon CloudFront
- ELB
- VPC



We can minimize DDoS attacks using the below architecture where a TCP or UDP based application

Source: https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/

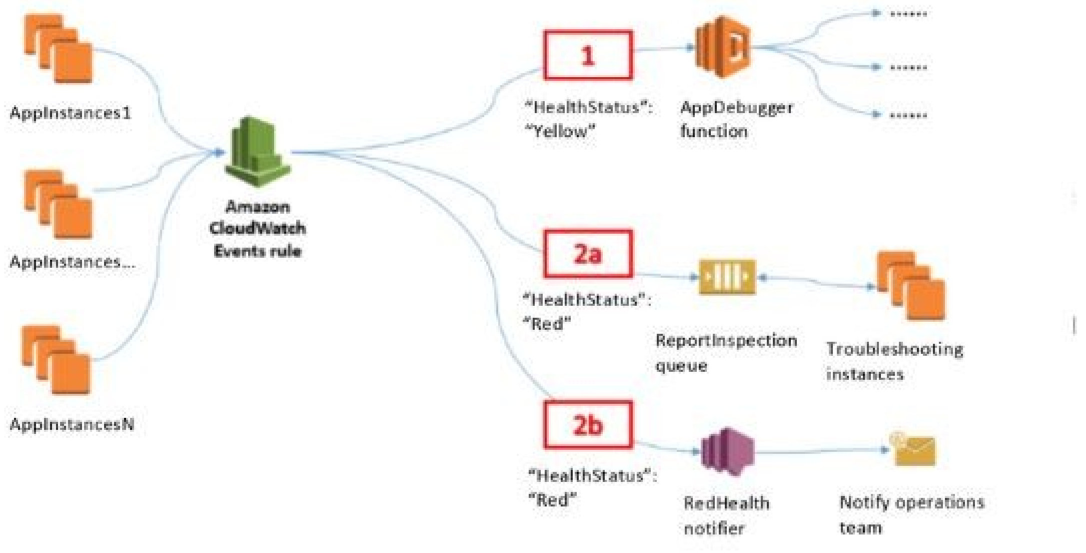
12. You are trying to provide a service in a particular region, but you do not see the service in that region. Why is this happening, and how do you fix it**?**

Not all Amazon AWS services are available in all regions. When Amazon initially launches a new service, it doesn't get immediately published in all the regions. They start small and then slowly expand to other regions. So, if you don't see a specific service in your region, chances are the service hasn't been published in your region yet. However, if you want to get the service that is not available, you can switch to the nearest region that provides the services.

13. How do you set up a system to monitor website metrics in real-time in AWS**?**

Amazon CloudWatch helps you to monitor the application status of various AWS services and custom events. It helps you to monitor:

- State changes in Amazon EC2
- Auto-scaling lifecycle events
- Scheduled events
- AWS API calls
- Console sign-in events



Source: https://aws.amazon.com/blogs/security/how-to-use-amazon-cloudwatch-events-to-monitor-application-health

14. What are the different types of virtualization in AWS, and what are the differences between them?

The three major types of virtualization in AWS are:

- Hardware Virtual Machine (HVM)

It is a fully virtualized hardware, where all the virtual machines act separate from each other. These virtual machines boot by executing a master boot record in the root block device of your image.

- Paravirtualization (PV)

Paravirtualization-GRUB is the bootloader that boots the PV AMIs. The PV-GRUB chain loads the kernel specified in the menu.

- Paravirtualization on HVM

PV on HVM helps operating systems take advantage of storage and network I/O available through the host.

15. Name some of the AWS services that are not region-specific

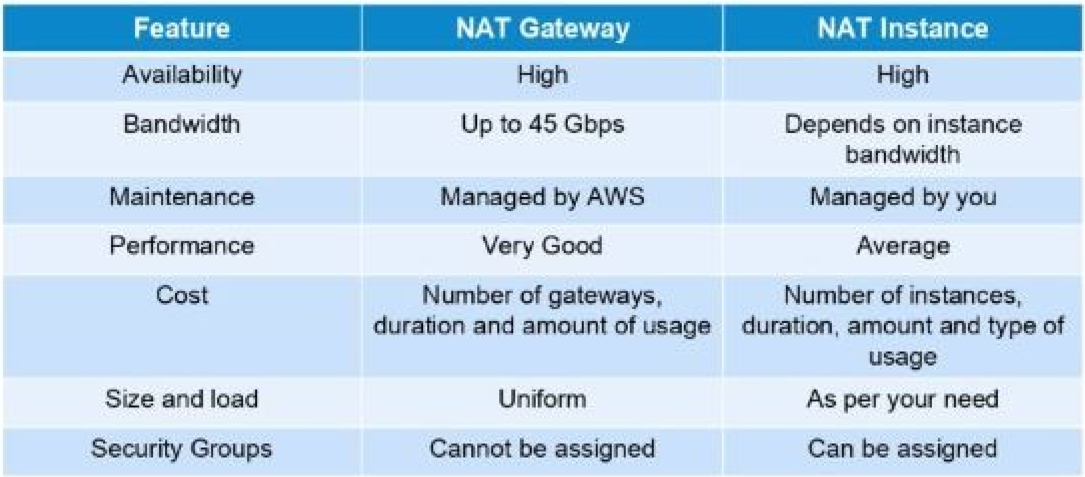
AWS services that are not region-specific are:

- IAM
- Route 53
- Web Application Firewall
- CloudFront

16. What are the differences between NAT Gateways and NAT Instances?

While both NAT Gateways and NAT Instances serve the same function, they still have some key differences.

The following are the key differences between NAT Gateway and NAT Instance:



Feature	NAT Gateway	NAT Instance
Availability	High	High
Bandwidth	Up to 45 Gbps	Depends on instance bandwidth
Maintenance	Managed by AWS	Managed by you
Performance	Very Good	Average
Cost	Number of gateways, duration and amount of usage	Number of instances, duration, amount and type of usage
Size and load	Uniform	As per your need
Security Groups	Cannot be assigned	Can be assigned

17. What is CloudWatch?

The Amazon CloudWatch has the following features:

- Depending on multiple metrics, it participates in triggering alarms.
- Helps in monitoring the AWS environments like CPU utilization, EC2, Amazon RDS instances, Amazon SQS, S3, Load Balancer, SNS, etc.

18. What is an Elastic Transcoder?

To support multiple devices with various resolutions like laptops, tablets, and smartphones, we need to change the resolution and format of the video. This can be done easily by an AWS Service tool called the Elastic Transcoder, which is a media transcoding in the cloud that exactly lets us do the needful. It is easy to use, cost-effective, and highly scalable for businesses and developers.

AWS Interview Questions for Amazon EC2

19. What is Amazon EC2?

EC2 is short for Elastic Compute Cloud, and it provides scalable computing capacity. Using Amazon EC2 eliminates the need to invest in hardware, leading to faster development and deployment of applications. You can use Amazon EC2 to launch as many or as few virtual servers as needed, configure security and networking, and manage storage. It can scale up or down to handle changes in requirements, reducing the need to forecast traffic. EC2 provides virtual computing environments called “instances.”

20. What Are Some of the Security Best Practices for Amazon EC2?

Security best practices for Amazon EC2 include using Identity and Access Management (IAM) to control access to AWS resources; restricting access by only allowing trusted hosts or networks to access ports on an instance; only opening up those permissions you require, and disabling password-based logins for instances launched from your AMI.

21. Can S3 Be Used with EC2 Instances, and If Yes, How?

Amazon S3 can be used for instances with root devices backed by local instance storage. That way, developers have access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of websites. To execute systems in the Amazon EC2 environment, developers load Amazon Machine Images (AMIs) into Amazon S3 and then move them between Amazon S3 and Amazon EC2.

Amazon EC2 and Amazon S3 are two of the best-known web services that make up AWS.

22. What is the difference between stopping and terminating an EC2 instance?

While you may think that both stopping and terminating are the same, there is a difference. When you stop an EC2 instance, it performs a normal shutdown on the instance and moves to a stopped state. However, when you terminate the instance, it is transferred to a stopped state, and the EBS volumes attached to it are deleted and can never be recovered.

23. What are the different types of EC2 instances based on their costs?

The three types of EC2 instances are:

- On-demand Instance

It is cheap for a short time but not when taken for the long term

- Spot Instance

It is less expensive than the on-demand instance and can be bought through bidding.

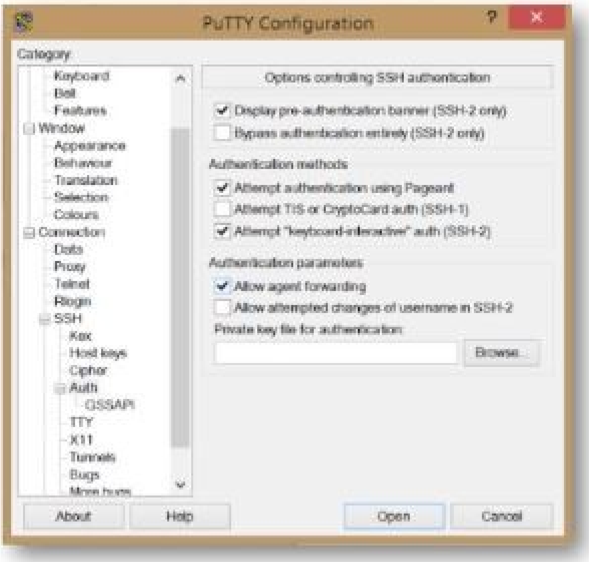
- Reserved Instance

If you are planning to use an instance for a year or more, then this is the right one for you.

24. How do you set up SSH agent forwarding so that you do not have to copy the key every time you log in?

Here's how you accomplish this:

1. Go to your PuTTY Configuration
2. Go to the category SSH -> Auth
3. Enable SSH agent forwarding to your instance



PuTTY Configuration

Category

Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
□ Bypass authentication entirely (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant
□ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☑ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

Private key file for authentication:

25. What are Solaris and AIX operating systems? Are they available with AWS?

Solaris is an operating system that uses SPARC processor architecture, which is not supported by the public cloud currently.

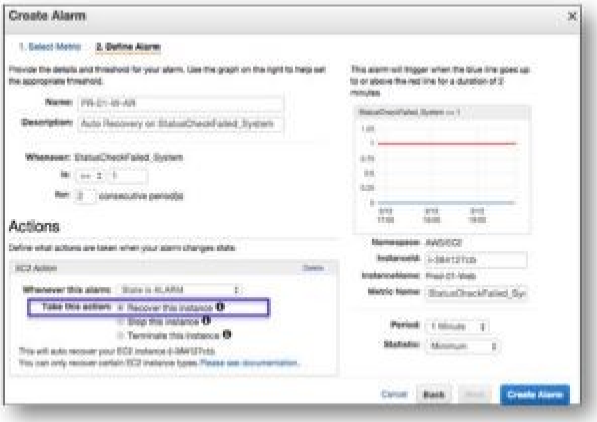
AIX is an operating system that runs only on Power CPU and not on Intel, which means that you cannot create AIX instances in EC2.

Since both the operating systems have their limitations, they are not currently available with AWS.

26. How do you configure CloudWatch to recover an EC2 instance?

Here's how you can configure them:

- Create an Alarm using Amazon CloudWatch
- In the Alarm, go to Define Alarm -> Actions tab
- Choose Recover this instance option



Create Alarm

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

Name: PR-01-W-AR

Description: Auto Recovery on StatusCheckFailed_System

Whenever: StatusCheckFailed_System

is: >= 1

for: 2 consecutive period(s)

Actions

Define what actions are taken when your alarm changes state.

EC2 Action

Whenever this alarm: State is ALARM

Take this action: ● Recover this instance
○ Stop this instance
○ Terminate this instance

This will auto recover your EC2 instance i-384f27cb.
You can only recover certain EC2 instance types. Please see documentation.

This alarm will trigger when the blue line goes up to or above the red line for a duration of 2 minutes

Namespace: AWS/EC2

InstanceId: i-384f27cb

InstanceName: Prod-01-Web

Metric Name: StatusCheckFailed_Sy

Period: 1 Minute

Statistic: Minimum

27. What are the common types of AMI designs?

There are many types of AMIs, but some of the common AMIs are:

- Fully Baked AMI
- Just Enough Baked AMI (JeOS AMI)
- Hybrid AMI

28. What are Key-Pairs in AWS?

The Key-Pairs are password-protected login credentials for the Virtual Machines that are used to prove our identity while connecting the Amazon EC2 instances. The Key-Pairs are made up of a Private Key and a Public Key which lets us connect to the instances.

AWS Interview Questions for S3

29. What is Amazon S3?

S3 is short for Simple Storage Service, and Amazon S3 is the most supported storage platform available. S3 is object storage that can store and retrieve any amount of data from anywhere. Despite that versatility, it is practically unlimited as well as cost-effective because it is storage available on demand. In addition to these benefits, it offers unprecedented levels of durability and availability. Amazon S3 helps to manage data for cost optimization, access control, and compliance.

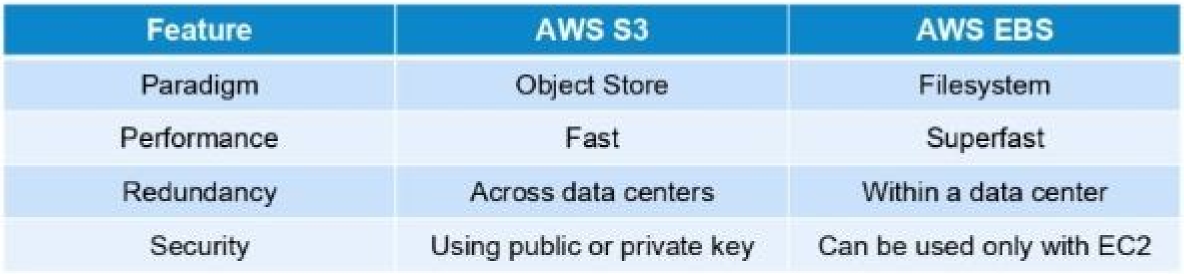
30. How can you recover/login to an EC2 instance for which you have lost the key?

Follow the steps provided below to recover an EC2 instance if you have lost the key:

1. Verify that the EC2Config service is running
2. Detach the root volume for the instance
3. Attach the volume to a temporary instance
4. Modify the configuration file
5. Restart the original instance

31. What are some critical differences between AWS S3 and EBS?

Here are some differences between AWS S3 and EBS



Feature	AWS S3	AWS EBS
Paradigm	Object Store	Filesystem
Performance	Fast	Superfast
Redundancy	Across data centers	Within a data center
Security	Using public or private key	Can be used only with EC2

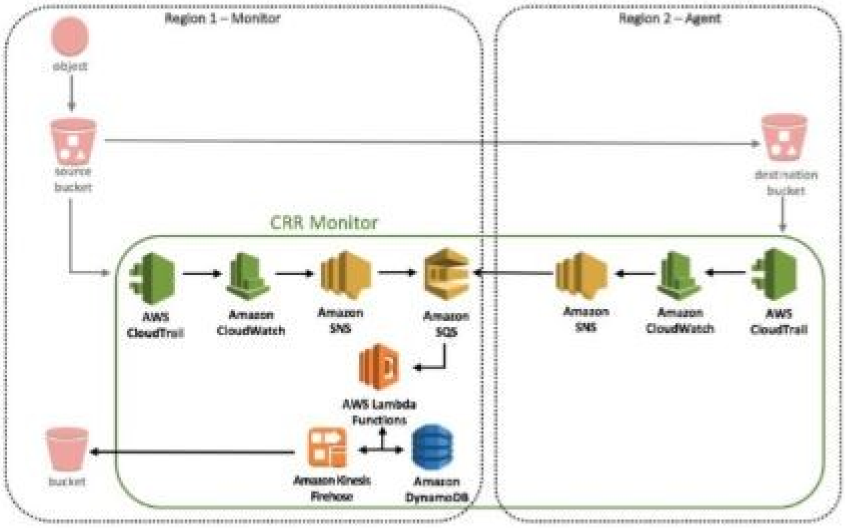
32. How do you allow a user to gain access to a specific bucket?

You need to follow the four steps provided below to allow access. They are:

1. Categorize your instances
2. Define how authorized users can manage specific servers.
3. Lockdown your tags
4. Attach your policies to IAM users

33. How can you monitor S3 cross-region replication to ensure consistency without actually checking the bucket?

Follow the flow diagram provided below to monitor S3 cross-region replication:



34. What is SnowBall?

To transfer terabytes of data outside and inside of the AWS environment, a small application called SnowBall is used.

Data transferring using SnowBall is done in the following ways:

1. A job is created.
2. The SnowBall application is connected.
3. The data is copied into the SnowBall application.
4. Data is then moved to the AWS S3.

35. What are the Storage Classes available in Amazon S3?

The Storage Classes that are available in the Amazon S3 are the following:

- Amazon S3 Glacier Instant Retrieval storage class
- Amazon S3 Glacier Flexible Retrieval (Formerly S3 Glacier) storage class
- Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)
- S3 Outposts storage class
- Amazon S3 Standard-Infrequent Access (S3 Standard-IA)
- Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)
- Amazon S3 Standard (S3 Standard)
- Amazon S3 Reduced Redundancy Storage
- Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

AWS Interview Questions for VPC

36. What Is Amazon Virtual Private Cloud (VPC) and Why Is It Used?

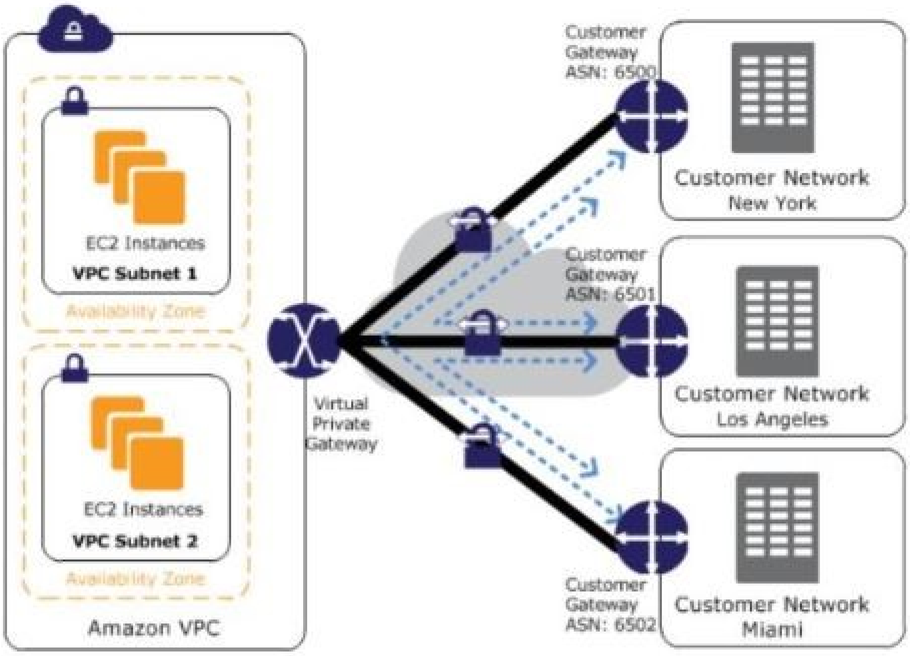
A VPC is the best way of connecting to your cloud resources from your own data center. Once you connect your datacenter to the VPC in which your instances are present, each instance is assigned a private IP address that can be accessed from your data center. That way, you can access your public cloud resources as if they were on your own private network.

37. VPC is not resolving the server through DNS. What might be the issue, and how can you fix it?

To fix this problem, you need to enable the DNS hostname resolution, so that the problem resolves itself.

38. How do you connect multiple sites to a VPC?

If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. Here's a diagram that will show you how to connect various sites to a VPC:



39. Name and explain some security products and features available in VPC?

Here is a selection of security products and features:

- Security groups - This acts as a firewall for the EC2 instances, controlling inbound and outbound traffic at the instance level.
- Network access control lists - It acts as a firewall for the subnets, controlling inbound and outbound traffic at the subnet level.
- Flow logs - These capture the inbound and outbound traffic from the network interfaces in your VPC.

40. How do you monitor Amazon VPC?

You can monitor VPC by using:

- CloudWatch and CloudWatch logs
- VPC Flow Logs

41. How many Subnets can you have per VPC?

We can have up to 200 Subnets per Amazon Virtual Private Cloud (VPC).

General AWS Interview Questions

42. When Would You Prefer Provisioned IOPS over Standard Rds Storage?

You would use Provisioned IOPS when you have batch-oriented workloads. Provisioned IOPS delivers high IO rates, but it is also expensive. However, batch processing workloads do not require manual intervention.

43. How Do Amazon Rds, Dynamodb, and Redshift Differ from Each Other?

Amazon RDS is a database management service for relational databases. It manages patching, upgrading, and data backups automatically. It's a database management service for structured data only. On the other hand, DynamoDB is a NoSQL database service for dealing with unstructured data. Redshift is a data warehouse product used in data analysis.

44. What Are the Benefits of AWS's Disaster Recovery?

Businesses use cloud computing in part to enable faster disaster recovery of critical IT systems without the cost of a second physical site. The AWS cloud supports many popular disaster recovery architectures ranging from small customer workload data center failures to environments that enable rapid failover at scale. With data centers all over the world, AWS provides a set of cloud-based disaster recovery services that enable rapid recovery of your IT infrastructure and data.

45. How can you add an existing instance to a new Auto Scaling group?

Here's how you can add an existing instance to a new Auto Scaling group:

- Open EC2 console
- Select your instance under Instances
- Choose Actions -> Instance Settings -> Attach to Auto Scaling Group
- Select a new Auto Scaling group
- Attach this group to the Instance
- Edit the Instance if needed
- Once done, you can successfully add the instance to a new Auto Scaling group

46. What are the factors to consider while migrating to Amazon Web Services?

Here are the factors to consider during AWS migration:

- Operational Costs - These include the cost of infrastructure, ability to match demand and supply, transparency, and others.
- Workforce Productivity
- Cost avoidance
- Operational resilience

- Business agility

47. What is RTO and RPO in AWS?

RTO or Recovery Time Objective is the maximum time your business or organization is willing to wait for a recovery to complete in the wake of an outage. On the other hand, RPO or Recovery Point Objective is the maximum amount of data loss your company is willing to accept as measured in time.

48. If you would like to transfer vast amounts of data, which is the best option among Snowball, Snowball Edge, and Snowmobile?

AWS Snowball is basically a data transport solution for moving high volumes of data into and out of a specified AWS region. On the other hand, AWS Snowball Edge adds additional computing functions apart from providing a data transport solution. The snowmobile is an exabyte-scale migration service that allows you to transfer data up to 100 PB.

49. Explain what T2 instances are?

The T2 Instances are intended to give the ability to burst to a higher performance whenever the workload demands it and also provide a moderate baseline performance to the CPU.

The T2 instances are General Purpose instance types and are low in cost as well. They are usually used wherever workloads do not consistently or often use the CPU.

50. What are the advantages of AWS IAM?

AWS IAM allows an administrator to provide multiple users and groups with granular access. Various user groups and users may require varying levels of access to the various resources that have been developed. We may assign roles to users and create roles with defined access levels using IAM.

It further gives us Federated Access, which allows us to grant applications and users access to resources without having to create IAM Roles.

51. Explain Connection Draining

Connection Draining is an AWS service that allows us to serve current requests on the servers that are either being decommissioned or updated.

By enabling this Connection Draining, we let the Load Balancer make an outgoing instance finish its existing requests for a set length of time before sending it any new requests. A departing instance will immediately go off if Connection Draining is not enabled, and all pending requests will fail.

52. What is Power User Access in AWS?

The AWS Resources owner is identical to an Administrator User. The Administrator User can build, change, delete, and inspect resources, as well as grant permissions to other AWS users.

Administrator Access without the ability to control users and permissions is provided to a Power User. A Power User Access user cannot provide permissions to other users but has the ability to modify, remove, view, and create resources.

AWS Interview Questions for CloudFormation

53. How is AWS CloudFormation different from AWS Elastic Beanstalk?

Here are some differences between AWS CloudFormation and AWS Elastic Beanstalk:

- AWS CloudFormation helps you provision and describe all of the infrastructure resources that are present in your cloud environment. On the other hand, AWS Elastic Beanstalk provides an environment that makes it easy to deploy and run applications in the cloud.
- AWS CloudFormation supports the infrastructure needs of various types of applications, like legacy applications and existing enterprise applications. On the other hand, AWS Elastic Beanstalk is combined with the developer tools to help you manage the lifecycle of your applications.

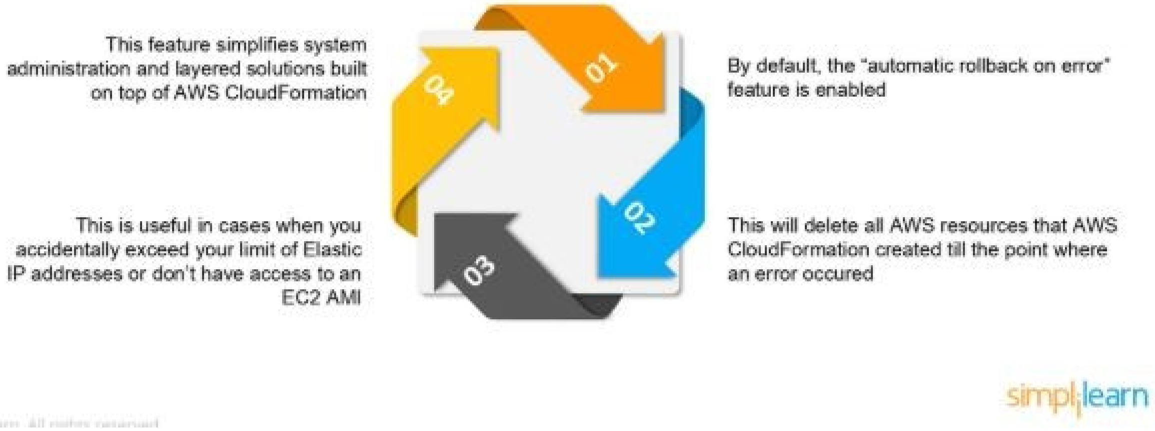
54. What are the elements of an AWS CloudFormation template?

AWS CloudFormation templates are YAML or JSON formatted text files that are comprised of five essential elements, they are:

- Template parameters
- Output values
- Data tables
- Resources
- File format version

55. What happens when one of the resources in a stack cannot be created successfully?

If the resource in the stack cannot be created, then the CloudFormation automatically rolls back and terminates all the resources that were created in the CloudFormation template. This is a handy feature when you accidentally exceed your limit of Elastic IP addresses or don’t have access to an EC2 AMI.



This feature simplifies system administration and layered solutions built on top of AWS CloudFormation

By default, the "automatic rollback on error" feature is enabled

This is useful in cases when you accidentally exceed your limit of Elastic IP addresses or don't have access to an EC2 AMI

This will delete all AWS resources that AWS CloudFormation created till the point where an error occured

AWS Interview Questions for Elastic Block Storage

56. How can you automate EC2 backup using EBS?

Use the following steps in order to automate EC2 backup using EBS:

1. Get the list of instances and connect to AWS through API to list the Amazon EBS volumes that are attached locally to the instance.

2. List the snapshots of each volume, and assign a retention period of the snapshot. Later on, create a snapshot of each volume.
3. Make sure to remove the snapshot if it is older than the retention period.

57. What is the difference between EBS and Instance Store?

EBS is a kind of permanent storage in which the data can be restored at a later point. When you save data in the EBS, it stays even after the lifetime of the EC2 instance. On the other hand, Instance Store is temporary storage that is physically attached to a host machine. With an Instance Store, you cannot detach one instance and attach it to another. Unlike in EBS, data in an Instance Store is lost if any instance is stopped or terminated.

58. Can you take a backup of EFS like EBS, and if yes, how?

Yes, you can use the EFS-to-EFS backup solution to recover from unintended changes or deletion in Amazon EFS. Follow these steps:

1. Sign in to the AWS Management Console
2. Click the launch EFS-to-EFS-restore button
3. Use the region selector in the console navigation bar to select region
4. Verify if you have chosen the right template on the Select Template page
5. Assign a name to your solution stack
6. Review the parameters for the template and modify them if necessary

59. How do you auto-delete old snapshots?

Here's the procedure for auto-deleting old snapshots:

- As per procedure and best practices, take snapshots of the EBS volumes on Amazon S3.
- Use AWS Ops Automator to handle all the snapshots automatically.
- This allows you to create, copy, and delete Amazon EBS snapshots.

AWS Interview Questions for Elastic Load Balancing

60. What are the different types of load balancers in AWS?

There are three types of load balancers that are supported by Elastic Load Balancing:

1. Application Load Balancer
2. Network Load Balancer
3. Classic Load Balancer

61. What are the different uses of the various load balancers in AWS Elastic Load Balancing?

Application Load Balancer

Used if you need flexible application management and TLS termination.

Network Load Balancer

Used if you require extreme performance and static IPs for your applications.

Classic Load Balancer

Used if your application is built within the EC2 Classic network

AWS Interview Questions for Security

62. What Is Identity and Access Management (IAM) and How Is It Used?

Identity and Access Management (IAM) is a web service for securely controlling access to AWS services. IAM lets you manage users, security credentials such as access keys, and permissions that control which AWS resources users and applications can access.

63. How can you use AWS WAF in monitoring your AWS applications?

AWS WAF or AWS Web Application Firewall protects your web applications from web exploitations. It helps you control the traffic flow to your applications. With WAF, you can also create custom rules that block common attack patterns. It can be used for three cases: allow all requests, prevent all requests, and count all requests for a new policy.

64. What are the different AWS IAM categories that you can control?

Using AWS IAM, you can do the following:

- Create and manage IAM users
- Create and manage IAM groups
- Manage the security credentials of the users
- Create and manage policies to grant access to AWS services and resources

65. What are the policies that you can set for your users' passwords?

Here are some of the policies that you can set:

- You can set a minimum length of the password, or you can ask the users to add at least one number or special characters in it.
- You can assign requirements of particular character types, including uppercase letters, lowercase letters, numbers, and non-alphanumeric characters.
- You can enforce automatic password expiration, prevent reuse of old passwords, and request for a password reset upon their next AWS sign in.

- You can have the AWS users contact an account administrator when the user has allowed the password to expire.

66. What is the difference between an IAM role and an IAM user?

The two key differences between the IAM role and IAM user are:

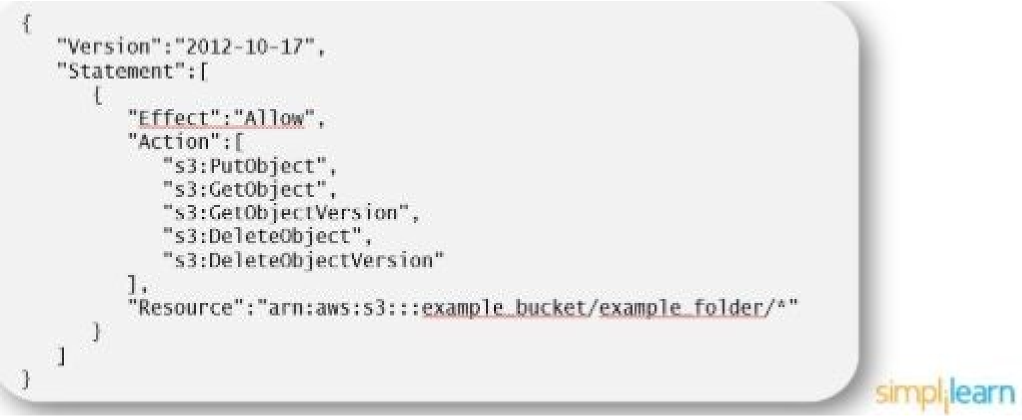
- An IAM role is an IAM entity that defines a set of permissions for making AWS service requests, while an IAM user has permanent long-term credentials and is used to interact with the AWS services directly.
- In the IAM role, trusted entities, like IAM users, applications, or an AWS service, assume roles whereas the IAM user has full access to all the AWS IAM functionalities.

67. What are the managed policies in AWS IAM?

There are two types of managed policies; one that is managed by you and one that is managed by AWS. They are IAM resources that express permissions using IAM policy language. You can create, edit, and manage them separately from the IAM users, groups, and roles to which they are attached.

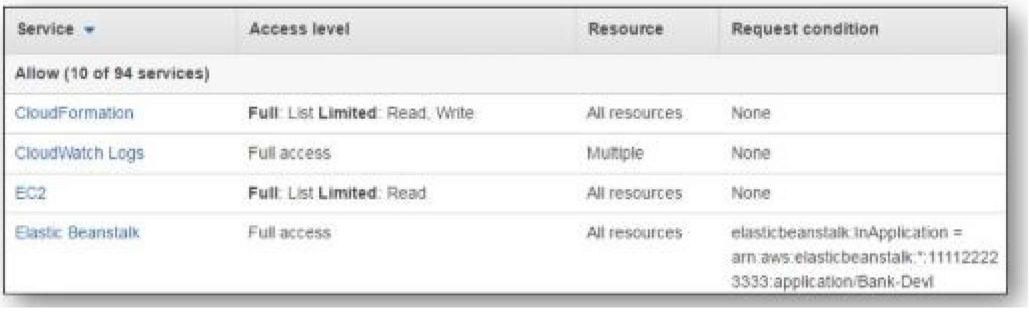
68. Can you give an example of an IAM policy and a policy summary?

Here's an example of an IAM policy to grant access to add, update, and delete objects from a specific folder.



```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::example_bucket/example_folder/*"
      }
   ]
}
```

Here's an example of a policy summary:



Service	Access level	Resource	Request condition
Allow (10 of 94 services)			
CloudFormation	**Full**: List **Limited**: Read, Write	All resources	None
CloudWatch Logs	Full access	Multiple	None
EC2	**Full**: List **Limited**: Read	All resources	None
Elastic Beanstalk	Full access	All resources	elasticbeanstalk:InApplication = arn:aws:elasticbeanstalk:*:111122223333:application/Bank-Devl

69. How does AWS IAM help your business?

IAM enables to:

- Manage IAM users and their access - AWS IAM provides secure resource access to multiple users

- Manage access for federated users – AWS allows you to provide secure access to resources in your AWS account to your employees and applications without creating IAM roles

AWS Interview Questions for Route 53

70. What Is Amazon Route 53?

Amazon Route 53 is a scalable and highly available Domain Name System (DNS). The name refers to TCP or UDP port 53, where DNS server requests are addressed.

71. What Is Cloudtrail and How Do Cloudtrail and Route 53 Work Together?

CloudTrail is a service that captures information about every request sent to the Amazon Route 53 API by an AWS account, including requests that are sent by IAM users. CloudTrail saves log files of these requests to an Amazon S3 bucket. CloudTrail captures information about all requests. You can use information in the CloudTrail log files to determine which requests were sent to Amazon Route 53, the IP address that the request was sent from, who sent the request, when it was sent, and more.

72. What is the difference between Latency Based Routing and Geo DNS?

The Geo Based DNS routing takes decisions based on the geographic location of the request. Whereas, the Latency Based Routing utilizes latency measurements between networks and AWS data centers. Latency Based Routing is used when you want to give your customers the lowest latency possible. On the other hand, Geo Based routing is used when you want to direct the customer to different websites based on the country or region they are browsing from.

73. What is the difference between a Domain and a Hosted Zone?

Domain

A domain is a collection of data describing a self-contained administrative and technical unit. For example, www.simplilearn.com is a domain and a general DNS concept.

Hosted zone

A hosted zone is a container that holds information about how you want to route traffic on the internet for a specific domain. For example, lms.simplilearn.com is a hosted zone.

74. How does Amazon Route 53 provide high availability and low latency?

Here's how Amazon Route 53 provides the resources in question:

Globally Distributed Servers

Amazon is a global service and consequently has DNS services globally. Any customer creating a query from any part of the world gets to reach a DNS server local to them that provides low latency.

Dependency

Route 53 provides a high level of dependability required by critical applications

Optimal Locations

Route 53 uses a global anycast network to answer queries from the optimal position automatically.

AWS Interview Questions for Config

75. How does AWS config work with AWS CloudTrail?

AWS CloudTrail records user API activity on your account and allows you to access information about the activity. Using CloudTrail, you can get full details about API actions such as the identity of the caller, time of the call, request parameters, and response elements. On the other hand, AWS Config records point-in-time configuration details for your AWS resources as Configuration Items (CIs).

You can use a CI to ascertain what your AWS resource looks like at any given point in time. Whereas, by using CloudTrail, you can quickly answer who made an API call to modify the resource. You can also use Cloud Trail to detect if a security group was incorrectly configured.

76. Can AWS Config aggregate data across different AWS accounts?

Yes, you can set up AWS Config to deliver configuration updates from different accounts to one S3 bucket, once the appropriate IAM policies are applied to the S3 bucket.

AWS Interview Questions for Database

77. How are reserved instances different from on-demand DB instances?

Reserved instances and on-demand instances are the same when it comes to function. They only differ in how they are billed.

Reserved instances are purchased as one-year or three-year reservations, and in return, you get very low hourly based pricing when compared to the on-demand cases that are billed on an hourly basis.

78. Which type of scaling would you recommend for RDS and why?

There are two types of scaling - vertical scaling and horizontal scaling. Vertical scaling lets you vertically scale up your master database with the press of a button. A database can only be scaled vertically, and there are 18 different instances in which you can resize the RDS. On the other hand, horizontal scaling is good for replicas. These are read-only replicas that can only be done through Amazon Aurora.

79. What is a maintenance window in Amazon RDS? Will your DB instance be available during maintenance events?

RDS maintenance window lets you decide when DB instance modifications, database engine version upgrades, and software patching have to occur. The automatic scheduling is done only for patches that are related to security and durability. By default, there is a 30-minute value assigned as the maintenance window and the DB instance will still be available during these events though you might observe a minimal effect on performance.

80. What are the consistency models in DynamoDB?

There are two consistency models In DynamoDB. First, there is the Eventual Consistency Model, which maximizes your read throughput. However, it might not reflect the results of a recently completed write. Fortunately, all the copies of data usually reach consistency within a second. The second model is called the Strong Consistency Model. This model has a delay in writing the data, but it guarantees that you will always see the updated data every time you read it.

81. What type of query functionality does DynamoDB support?

DynamoDB supports GET/PUT operations by using a user-defined primary key. It provides flexible querying by letting you query on non-primary vital attributes using global secondary indexes and local secondary indexes.

*What's the most frustrating support issue you've been called to resolve?

*Can you tell us about a time when you initially failed to solve an issue?