Module 16 Linux server - Operate running systems

* ***Assignment Level Basic to Advance***

1. ***What is PID?***

***Ans.*** *In computing, the process identifier (a.k.a. process ID or PID) is a number used by most operating system kernels—such as those of Unix, macOS and Windows—to uniquely identify an active process.*

1. ***What is PPID?***

***Ans.*** *A process that creates a new process is called a parent process; the new process is called a child process. The parent process ID (PPID) becomes associated with the new child process when it is created.*

1. ***What is the use of “PS “command?***

***Ans.*** *The PS command enables you to check the status of active processes on a system, as well as display technical information about the processes.*

1. ***What is the use of “PS aux “command?***

***Ans.*** *The PS aux command is a tool to monitor processes running on your Linux system. A process is associated with any program running on your system, and is used to manage and monitor a program's memory usage, processor time, and I/O resources.*

1. ***What is the use of “tops “command?***

***Ans.*** *The top utility is a commonly used tool for displaying system-performance information.*

1. ***Which command is used to change priority value?***

***Ans.***

1. ***What is the use of “jobs” command?***

***Ans.*** *The jobs command will list all jobs on the system; active, stopped, or otherwise.*

1. ***What is the use of grep command?***

***Ans.*** *The grep command can search for a string in groups of files. When it finds a pattern that matches in more than one file, it prints the name of the file, followed by a colon, then the line matching the pattern.*

1. ***What is system?***

***Ans.*** *A system is an arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not.*

1. ***What are daemons?***

***Ans.*** *n computing, a daemon (pronounced DEE-Muhn) is a program that runs continuously as a background process and wakes up to handle periodic service requests, which often come from remote processes.*

1. ***I want to check the service status for” sshd”, which will help me?***

***Ans.*** *“*systemctl status sshd” command will help.

1. ***How to stop and start services in terminal?***

***Ans.*** *We can stop and start any services with help of “systemctl” command.*

1. ***What is the use of openSSH ?***

***Ans.***[*SSH (Secure Shell)*](https://www.ssh.com/ssh/) *is a tool for secure system administration, file transfers, and other communication across the Internet or other untrusted network. It encrypts identities, passwords, and transmitted data so that they cannot be eavesdropped and stolen.*

[*OpenSSH*](https://en.wikipedia.org/wiki/OpenSSH) *is an open-source implementation of the* [*SSH protocol*](https://www.ssh.com/ssh/protocol/)*. It is based on the free version by* [*Tatu Ylonen*](https://ylonen.org/) *and further developed by the* [*OpenBSD*](http://openbsd.org/) *team and the user community.*

*Tatu Ylonen founded* [*SSH Communications Security*](https://www.ssh.com/) *to provide commercial support for enterprises, and the original version evolved into* [*Tectia SSH*](https://www.ssh.com/products/tectia-ssh/)*. The commercial version also supports Windows and IBM mainframe (z/OS) platforms and includes full support for X.509 certificates and smartcard authentication (for example the CAC and PIV cards used by US government).*

*The open-source version is delivered as source code or precompiled binaries under a BSD-style license. The project team provides no support services for end-users, but community-based support is available (on a voluntary basis) from various security web forums.*

1. ***Which command is used to generate key in Linux?***

***Ans.***ssh-keygen command is used to generating key in Linux.

1. ***Which command is used to copy ssh key?***

***Ans.*** *We can use ssh-copy-id command to copy ssh key.*

1. ***How do we prohibit the root user from logging in using ssh?***

***Ans.*** *1. Open the SSH configuration file sshd\_config with the text editor vi: vi /etc/ssh/sshd\_config.*

*2. In the line PermitRootLogin yes replace the word Yes with the word No.*

*3. Save the file.*

*4. Restart the service. Ubuntu. service ssh restart. CentOS 7. systemctl restart sshd.*

1. ***How do we prohibit password authentication using ssh?***

***Ans.*** *1. # vim /etc/ssh/sshd\_config. Look for the line Password Authentication yes and replace yes with no.*

*2. Password Authentication no. Press ESC key and save the changes to the file and exit the editor by typing: wq! and then hit Enter. ...*

*3. # service sshd restart*.

1. ***Where we find general logs?***

***Ans.*** *Linux has a special directory for storing logs called /var/log. This directory contains logs from the OS itself, services, and various applications running on the system.*

1. ***Where we find secure logs?***

***Ans.*** *We can see secure logs in this location /var/log/secure*

1. ***Where we find mail log?***

***Ans.*** *We can see mail logs in this location /var/log/maillog*

1. ***Where we find scheduling logs?***

***Ans.*** *We can see scheduling logs in this location /var/log/cron*

1. ***Where we find booting logs?***

***Ans.*** *We can see booting logs in this location /var/log/boot.log*

1. ***What is the use of “lastb” command?***

***Ans.*** *The lastb command is used to display information pertaining to failed login attempts.*

1. ***Where we find general logs?***

***Ans.*** *Linux has a special directory for storing logs called /var/log. This directory contains logs from the OS itself, services, and various applications running on the system.*

1. ***Where we find secure logs?***

***Ans.*** *We can see secure logs in this location /var/log/secure*

1. ***Where we find mail log?***

***Ans.*** *We can see mail logs in this location /var/log/maillog*

1. ***Where we find scheduling logs?***

***Ans.*** *We can see scheduling logs in this location /var/log/cron*

1. ***Where we find booting logs?***

***Ans.*** *We can see booting logs in this location /var/log/boot.log*

1. ***What is the use of “lastb” command?***

***Ans.*** *The lastb command is used to display information pertaining to failed login attempts.*

* ***Assignment Level Intermediate***

1. ***Remote host is “NADIAD”, Remote user is “KAMAL, how to access remote user via ssh? [ wright down the command]***

***Ans.*** *Ssh nadlad.*

*--> SSH or Secure Shell is a network communication protocol that enables two computers to communicate (c.f http or hypertext transfer protocol, which is the protocol used to transfer hypertext such as web pages) and share data.*

*--> nadlad is a user that we are accessing by remotely.*

1. ***What is the use of “w -f “command?***

***Ans.*** *w -f: This option will toggle printing the from (remote hostname) field. The default as released is from field which not be printed. Although your system administrator or your distribution maintainer may have compiled a version in which the from field is shown by default.*

1. ***What is “SSH host keys “?***

***Ans.*** *A host key is a cryptographic key used for authenticating computers in the SSH protocol. Host keys are key pairs, typically using the RSA, DSA, or ECDSA algorithms. Public host keys are stored on and/or distributed to SSH clients, and private keys are stored on SSH servers.*

1. ***What is the default location for server’s public key in client side?***

***Ans.*** *There are two kinds of keys: Server or host keys, which identify the server to the user, and user keys, which allow logging in. The private host key of the server is stored in /etc/ssh/. The corresponding public key is automatically added (after a prompt) to known hosts in ~/. ssh on the client.*

1. ***I want to fire “ls -l /etc” command on remote host “desktop” [ wright down the command]***

***Ans.*** *“ls –l /etc” it will show us all file/folder in “/etc” directory.*

1. ***What is the use of this command “# journalctl --since today “***

***Ans.*** *“journalctl--since today”* command use for list all journal entries from today's records

1. ***What is “ chronyd “?***

***Ans.*** *chronyd is used to adjust the system clock that runs in the kernel to synchronize with the NTP clock server. chronyd can determine accurate statistics for the difference between the UTC time and the local system time and adjust the system time accordingly.*

1. ***Full form of NTP***

***Ans.*** *Network Time Protocol*

1. ***Port number for NTP is…***

***Ans.*** *port number 123*

1. ***I want to check Tim zone, which command will help me?***

***Ans.*** *We can see time zone by Using the date command*

1. ***How to set time zone? Give a command….***

***Ans.*** *timedatectl set-timezone command followed by the long name of the time zone you want to set.*

***Task :1***

1. ***Display all processes on display***

***Ans.*** *Done in lab.*

1. ***In terminal, Determine the number of logical CPUs***

***Ans.*** *Done in lab.*

1. ***Start and check any new job***

***Ans.*** *Done in lab.*

1. ***Start any new job in background***

***Ans.*** *Done in lab.*

1. ***Start any background job on foreground***

***Ans.*** *Done in lab.*

1. ***Check running process***

***Ans.*** *Done in lab.*

1. ***Check all running process under user***

***Ans.*** *Done in lab.*

1. ***Kill any process via it’s PID***

***Ans.*** *Done in lab.*

1. ***Change nice values for any new process***

***Ans.***

1. ***Change nice value for any running user***

***Ans.***

1. ***Check the status of sshd.service***

***Ans.*** *Done in lab.*

1. ***Stop the service of sshd.service***

***Ans.*** *Done in lab.*

1. ***Start the service of sshd.service***

***Ans.*** *Done in lab.*

1. ***Login in server vm***

***Ans.*** *Done in lab.*

1. ***Display the status of “chronyd”***

***Ans.*** *Done in lab.*

1. ***Restart “sshd.service”***

***Ans.*** *Done in lab.*

***TASK: 3***

1. ***Start desktop machine***

***Ans.*** *Done in lab.*

1. ***Get remote access of server machine***

***Ans.*** *Done in lab.*

1. ***Create new user in server name “user1”***

***Ans.*** *Done in lab.*

1. ***From desktop machine, login “user1” of server user***

***Ans.*** *Done in lab.*

1. ***Execute single command “hostname”, on remote host (server), and as a remote user “user1”***

***Ans.*** *Done in lab.*

1. ***Display a list of currently logged into the computer***

***Ans.*** *Done in lab.*

1. ***Generate private-public ssh key with password***

***Ans.*** *Done in lab.*

1. ***Import this key on remote host side***

***Ans.*** *Done in lab.*

***Task: 4***

1. ***Open general logs***

***Ans.*** *Done in lab.*

1. ***Open secure message logs***

***Ans.*** *Done in lab.*

1. ***Open only mail logs***

***Ans.*** *Done in lab.*

1. ***Check scheduling logs***

***Ans.*** *Done in lab.*

1. ***Check booting logs***

***Ans.*** *Done in lab.*

1. ***See the info about “bad logging”***

***Ans.*** *Done in lab.*

1. ***Check emperor logs***

***Ans.*** *Done in lab.*

1. ***Check today’s temporary logs***

***Ans.*** *Done in lab.*

1. ***Set new time zone***

***Ans.*** *Done in lab.*