CONFIGURE AND SECURE SSH

DESCRIPTION	COMMANDS / OPTIONS
To displays a list of users that are currently logged in to the system	**w [options] user** -h Suppresses the header row from being displayed in the output. -u Ignores the username when calculating the current process and CPU times. -s Uses the short format, omitting the login time, JCPU (total CPU time used by all processes), and PCPU (CPU time used by the current process) times. -f Toggles the printing of the ‘from’ field (remote hostname). By default, it is not printed, but this option can change that. -i Displays the IP address instead of the hostname in the ‘from’ field. -V Displays version information about the ‘w’ command. -o Prints a blank space for idle times that are less than one minute. user Shows information about the specified user only
Login to remote host using ssh	**ssh [options][username]@[hostname/IP address]** -1 Forces ssh to use protocol SSH-1 only. -2 Forces ssh to use protocol SSH-2 only. -4 Allows IPv4 addresses only. -6 Allows IPv6 addresses only. -A Authentication agent connection forwarding is enabled. -a Authentication agent connection forwarding is disabled. -C Compresses all data -c Selects the cipher specification for encrypting the session -g Allows remote hosts to connect to local forwarded ports. -p Port to connect to on the remote host.
To configure SSH	**To install ssh packege Openssh** sudo yum install openssh **To start ssh services** systemctl start sshd.service **check firewall allowed** Firewall-cmd –list-all **ssh configuration files** /etc/ssh/

DESCRIPTION	**COMMANDS / OPTIONS**
Secure copy	**scp [option] <source ><RemoteHost>: <RmoteLocation>** -P port: Specifies the port to connect on the remote host -p Preserves modification times, access times, and modes from the original file -q Disables the progress meter -r Recursively copy entire directories -s Name of program to use for the encrypted connection
Generating key pairs using sshkeygen To create a key pair. By default, the ssh-keygen saves your private and public keys in the ~/.ssh/id_rsa and ~/.ssh/id_rsa.pub files.	**ssh-keygen** -f specifies the files in which to save the keys **Share the Public Key** ssh-copy-id [options] <filepath><remoteHost> -i Intractive
Disable Root Login Via SSH in RHEL 8 ｜ Forbid SSH Root Login in Linux	**Vim / etc / ssh/sshd_config** PermitRootLogin **yes/no** systemctl restart sshd.service
Allow Or Deny Selected Users / Groups To Login Via SSH in Linux	Vim / etc / ssh/sshd_config **insert entery to allowed user login ssh** AllowUsers <userNames> DenyUsers<userNames>
Setup SSH Idle Timeout in Linux	**Vim / etc / ssh/sshd_config** ClientAliveInterval ClientAliveCountMax
Add port & allowed rule	**Vim / etc / ssh/sshd_config** Change SSH Default Port in Linux Port 22 **list port allowed** Firewall-cmd –list-all firewall-cmd --permanent –add-port=22/tcp semanage port -l | grep ssh semanage port -a -t ssh_port_t -p tcp 22 systemctl restart sshd