SSH Objectives
Tasks in PDF file

SSH Objectives

1. Configure SSH on **server.example.com** to meet the following requirements.
   a) SSH should listen on ports 22 and 2222.
   b) Firewall should allow access to port 2222 from **client.example.com**.
   c) Enable password and key authentication. The changes should persist after reboot.

Commands: (On server.example.com)

yum install openssh-server (To install sshd Service, it will be pre-installed but in case you need to install this)

systemctl start sshd (To start Service)

systemctl enable sshd (To enable service)

systemctl status sshd (To check the status of sshd Service)

vim /etc/ssh/sshd_config (To make changes in ssh server config file as per task requirements)

Port 22 (This is default but you must uncomment this)

Port 2222 (To define non-default port for sshd service to listen on)

PubkeyAuthenication yes (To enable key authentication, This is default)

PasswordAuthenication yes (To enable password authentication, This is Default)

:wq

systemctl restart sshd (Restart sshd service to make the changes effective)

semanage port -a -t ssh_port_t -p tcp 2222 (To apply correct SELINUX Context type on non-default port)

firewall-cmd --add-port=2222/tcp --permanent (To configure firewall to accept inbound ssh traffic on non-default port)

firewall-cmd --reload (To reload the firewall to make the changes effective)

Commands: (On client.example.com)

ssh server.example.com (Establish SSH connection with server.example.com on Default port and it should be successful)

ssh -p 2222 server.example.com (Establish SSH connection with server.example.com on Non-Default port 2222 and it should also be successful)

It will prompt for password in both cases which means PasswordAuthenication is enabled.

For PubKey Authenication, we will discuss/Verify in upcoming tasks.

2. Configure client for password less root authentication against the server using passphrase access.

a) Make sure passphrase is not needed to enter again during active session.

Commands: (On client.example.com)

ssh-keygen -t -rsa (To generate Private/Public key pair on client machine)

Enter passphrase : access

Enter same passphrase again : access

cd /root/.ssh (Move to directory)

ls -l (List the files and verify ,Private and Public Keys are present,id_rsa –Private key, id_rsa.pub-Public key)

ssh-copy-id server.example.com (To copy the Public key to server machine)

Password : ********

ssh server.example.com (Establish ssh connection to server.example.com)

Enter passphrase for key - access (This time it will ask for passphrase not the password and connection will be established)

ssh-agent /bin/bash (To cache the passphrase during the active session)

ssh-add

Enter passphrase :access

ssh server.example.com (Establish ssh connection to server.example.com and this time no need to provide passphrase and you will be logged in)

Note : You don't need to enter the Passphrase during this active session. After logout/login, you will again need to provide passphrase.

3. Configure SSH on **server.example.com** to keep the inactive session open for 30 minutes.

Commands: (On server.example.com)

yum install openssh-server (To install sshd Service, it will be pre-installed but in case you need to install this)

systemctl start sshd (To start Service)

systemctl enable sshd (To enable service)

systemctl status sshd (To check the status of sshd Service)

vim /etc/ssh/sshd_config (To make changes in ssh server config file as per task requirements)

TCPKeepAlive yes (This is default and enables the server to monitor the client)

ClientAliveInterval 300 (This parameter is set to 300 seconds and this means server will check every 5 minutes (300 sec) by sending packets to client to check if client is inactive.

ClientActiveCountMax 6 (We will set this parameter to 6 ,which means server will send packets 6 times every 5 minutes to check if client is still inactive and after 6 attempts it will be timed-out.

:wq

systemctl restart sshd (Restart sshd service to make changes effective)

Note : 5 mintues * 6 = 30 mintues ,Session will be open for 30 min even in case of inactivity.

4. Configure SSH on **client2.example.com** to disable root login.

a) Only user **'riya'** should be allowed to establish ssh connection to **client2.example.com**

Commands: (On client2.example.com)

yum install openssh-server (To install sshd Service, it will be pre-installed but in case you need to install this)

systemctl start sshd (To start Service)

systemctl enable sshd (To enable service)

systemctl status sshd (To check the status of sshd Service)

vim /etc/ssh/sshd_config (To make changes in ssh server config file as per task requirements)

PermitRootLogin no (Set this parameter to no to disable root login)

AllowUsers riya (To allow only user to establish ssh session with client2 machine , rest all will be denied access)

:wq

systemctl restart sshd (Restart sshd service to make changes effective)

Test form client.example.com (or some other host), only user riya will be allowed to make ssh connection with client2.example.com.

Also test with root user, it will be denied.