SSH Lab

In this lab you will perform the following tasks:

- Generate a key-pair
- Setup automatic login
- Disable password authentication
- Enable password authentication for selected users

1. Generate key-pair

Login as centos user to your machine.
Generate a key-pair.

```
[centos@centos11 ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/centos/.ssh/id_rsa):(enter)
Enter passphrase (empty for no passphrase): (enter)
Enter same passphrase again: (enter)
Your identification has been saved in /home/centos/.ssh/id_rsa.
Your public key has been saved in /home/centos/.ssh/id_rsa.pub.
The key fingerprint is:
bc:65:40:2d:14:a0:99:3e:71:79:b7:8f:f8:2c:d8:7d centos@centos11
The key's randomart image is:
+--[ RSA 2048]----+
```

Go to the *~/.ssh* directory and list the keys.

```
[centos@centos11 ~]$ cd .ssh
[centos@centos11 .ssh]$ ls id*
id_rsa  id_rsa.pub
```

View the contents of the private key file.

```
[centos@centos11 .ssh]$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA08KVvNYaKEUOnwM9OUDsP4XTSp37wXgJev9nVxex1KMJbEPg
KArIqtmg93nlAkFPwdVguV4pNyWgYYxH+FmzO2vPaZVjhU5hPnLQQ7YCQA3quai2
BsNOetknf7IChZhkgIO/j+AEBp2o8p2umBrksR6SMR9KkJQoXQbJq++eEdutNofH
(snipped)
```

View the contents of the public key file.

```
[centos@centos11 .ssh]$ cat id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDTwpW81hooRQ6fAz05QOw/hdNKnfvBeAl6/2dXF7
HUowlsQ+AoCsiq2aD3eeUCQU/B1WC5Xik3JaBhjEf4WbM7a89plWOFTmE+ctBDtgJADeq5
qLYGw0562Sd/sgKFmGSAg7
(snipped)
```

2. Setup automatic login to the dictu-server

Run ssh-copy-id with the destination username and server.

```
[centos@centos11 ~]$ ssh-copy-id centos-11@centos-server
The authenticity of host 'dictu-server (192.168.4.141)' can't be
established.
ECDSA key fingerprint is
69:85:2b:e5:ef:53:18:55:84:b9:d6:60:3f:5d:28:9f.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s),
to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you
are prompted now it is to install the new keys
centos-11@dictu-server's password:

Number of key(s) added: 1

Now try logging into the machine, with:"ssh centos-11@dictu-server'"
and check to make sure that only the key(s) you wanted were added.

[centos@centos11 ~]$
```

Test the login.

```
[centos@centos11 ~]$ ssh centos-11@centos-server
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Apr 26 09:16:38 2021 from 192.168.4.131
```

Check the contents of the authorized_keys file on the remote server for the dictu-xx user. And see that it is your centos-xx public key.

```
[centos-11@dictu-server1 ~]$ more .ssh/authorized_keys
Ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDPfPwPdxyoFZ8HFul+aiRJ45DKjZ5US
7FaTmJB+lhugCgLAG1cp2dxHwtDc9GT7w5rM4U1L8hRahildoiNsDEr/iiGSv3g2OSvvvH
(snipped)
```

3. **Disable Password Authentication**

On your centos-xx machine, open the /etc/ssh/sshd_config file.

```
[centos@centos11 ~]$ sudo vi /etc/ssh/sshd_config
[sudo] password for centos:
```

Search for the following line:

```
PasswordAuthentication yes
```

Change it to ‘*no*’.

```
PasswordAuthentication no
```

Save the file.
Restart the sshd service:

```
[centos@centos11 ~]$ sudo systemctl restart sshd
```

Test whether you can still connect using a password. You should receive a permission denied message.

```
[centos@centos11 ~]$ ssh centos-11@localhost
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

4. Enable password authentication for selected users

Open the /etc/ssh/sshd_config file and add the following to the very end of the file:

```
Match User centos
  PasswordAuthentication yes
```

In the above lines, only the *centos* user will be able to login using a password.

Restart the sshd service and try to login as *centos*.

```
[centos@centos11 ~]$ sudo systemctl restart sshd
[centos@centos11 ~]$ ssh centos@localhost
centos@localhost's password:
```