

Guided Practice: Install, Configure, and Test ssh

Outcome

In this Guided Practice, you will install and configure the ssh protocol on your Ubuntu computer and use the CentOS computer to connect to Ubuntu using the ssh protocol.

Resources Needed

- VCASTLE Pod configured for the class. For this Guided Practice, we use the CentOS 8 and Ubuntu 20.04 LTS machines.
- Your user needs to be able to elevate their privileges with sudo.

Level of Difficulty

Moderate

Deliverables

Deliverables are marked in red font or with a red picture border around the screenshot. Additionally, there are questions at the end. **Your username or studentID should be visible in all screenshots that you submit.**

General Considerations

You should be familiar with configuring Linux networking.

Install ssh on Ubuntu

If you're using VCASTLE, log on to Ubuntu. The password is Password1.

Check for IP Address on both machines. If either machine lacks an IP Address, you should turn on networking. Open a terminal.

1. Allow the CIS321 user to run sudo.

```
su root  
sudo adduser CIS321@ecpiscrpting.local sudo
```

Your screenshot should resemble the one below.

```
cis321@ecpiscrpting.local@cis321-ubuntu:~$ su root  
Password:  
root@cis321-ubuntu:/home/cis321@ecpiscrpting.local# sudo adduser cis321@ecpisc  
rpting.local sudo  
Adding user `cis321@ecpiscrpting.local' to group `sudo' ...  
Adding user cis321@ecpiscrpting.local to group sudo  
Done.
```

2. Now, you're going to create a new user that you'll use for some Ansible labs. Call the user **YourStudentID**. This should be your ecpi student id. Give the user **sudo** privileges.

```
adduser YourStudentID
```

Give the user a password of "Password1."

Your screenshot should resemble the one below.

```
root@cis321-ubuntu:/home/cis321@ecpiscrpting.local# adduser ranbel1234  
Adding user `ranbel1234' ...  
Adding new group `ranbel1234' (1001) ...  
Adding new user `ranbel1234' (1001) with group `ranbel1234' ...  
Creating home directory `/home/ranbel1234' ...  
Copying files from `/etc/skel' ...  
New password:  
BAD PASSWORD: The password fails the dictionary check - it is based on a dictio  
nary word  
Retype new password:  
passwd: password updated successfully  
Changing the user information for ranbel1234  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n] Y
```

3. Add your studentID to sudo.

```
adduser studentID sudo
```

```
root@cis321-ubuntu:/home/ranbel1234# adduser ranbel1234 sudo
Adding user `ranbel1234' to group `sudo' ...
Adding user ranbel1234 to group sudo
Done.
```

4. Change to your student id logon, and then change to your student id's home directory.

```
su studentID
cd
```

Your screenshot should resemble the one below.

```
root@cis321-ubuntu:/home/cis321@ecpiscrpting.local# su ranbel1234
ranbel1234@cis321-ubuntu:/home/cis321@ecpiscrpting.local$ cd
ranbel1234@cis321-ubuntu:~$
```

5. By default, when Ubuntu is first installed, remote access via SSH is not allowed. Enabling SSH on Ubuntu is fairly straightforward.

In an Ubuntu terminal windows, type the following. You may be asked for your password.

```
sudo apt install openssh-server
```

```
ranbel1234@cis321-ubuntu:~$ sudo apt install openssh-server
[sudo] password for ranbel1234:
```

If ssh fails to install, do this:

```
sudo apt-get update && sudo apt-get upgrade
```

Then try the download/installation again.

Wait for the package to install.

6. Check the status. The output should tell you that the service is running and enabled to start on system boot.

Type:

```
sudo systemctl status ssh
```

```
ranbel1234@ranbel1234-virtual-machine:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: >
   Active: active (running) since Sat 2020-10-17 13:51:59 EDT; 2min 33s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 3484 (sshd)
     Tasks: 1 (limit: 4623)
    Memory: 1.4M
     CGroup: /system.slice/ssh.service
            └─3484 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
```

Type the following to get back to the command prompt.

```
q:
```

7. Check your Ubuntu machine's IP address by typing

```
ip addr show
```

In the case below, the IP Address is 192.168.1.3. Make a note of it.

```
ranbel1234@cis321-ubuntu:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group d
efault qlen 1000
    link/ether 00:50:56:1a:2b:ee brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global dynamic noprefixroute en
s160
        valid_lft 686354sec preferred_lft 686354sec
    inet6 fe80::3cff:ae6e:6d13:54db/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group d
efault qlen 1000
    link/ether 00:50:56:a7:91:ed brd ff:ff:ff:ff:ff:ff
```

Using the touch command, create a file on Ubuntu. Type

```
touch ThisIsAFileOnTheUbuntuComputer
```

Run the **ls** command to confirm you've created this file.

```
ranbel1234@ranbel1234-virtual-machine:~$ touch ThisIsAFileOnTheUbuntuComputer
ranbel1234@ranbel1234-virtual-machine:~$ ls
Desktop  Documents  Music      Public     ThisIsAFileOnTheUbuntuComputer
Directory Downloads  Pictures   Templates  Videos
ranbel1234@ranbel1234-virtual-machine:~$
```

Take a screenshot like the one above, and paste it into your Lab Report.

Connect from CentOS to Ubuntu

- Now go to the CentOS computer, open a terminal window, and attempt to connect to the Ubuntu computer using the ssh protocol. In the case below, the Ubuntu user is ranbel1234, and the IP address is the IP address of the Ubuntu computer. When prompted, you'll need to enter the password for the Ubuntu user.

Type

```
ssh username@IPOfUbuntuComputer
```

In this example, we've typed **ssh ranbel1234@192.168.1.3**

You should now have an ssh connection from your CentOS computer to the Ubuntu computer, and your CentOS terminal window should look like this:

```
[cis321@ecpiscrpting.local@cis321-centos ~]$ ssh ranbel1234@192.168.1.3
The authenticity of host '192.168.1.3 (192.168.1.3)' can't be established.
ECDSA key fingerprint is SHA256:YmhGvrzVdf6acmLQj4hn15zWS1boYr0Jr9BpmQyhktM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.3' (ECDSA) to the list of known hosts.
ranbel1234@192.168.1.3's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

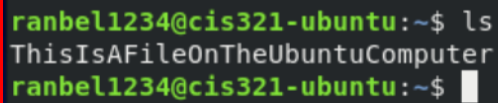
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

You now have an ssh connection to the Ubuntu computer.

9. Since your working directory is the user's home directory on Ubuntu, when you type **ls**, you should see the file you created on Ubuntu.

From the CentOS, type the following. Your output should look similar to this. The important thing is that it displays the file you created on Ubuntu.

```
ls
```

A terminal window with a dark background and a red border. It shows the command 'ls' being executed, resulting in the output 'ThisIsAFileOnTheUbuntuComputer'. The prompt is 'ranbel1234@cis321-ubuntu:~\$' and the cursor is at the end of the line.

```
ranbel1234@cis321-ubuntu:~$ ls  
ThisIsAFileOnTheUbuntuComputer  
ranbel1234@cis321-ubuntu:~$
```

Take a screenshot like the one above, and paste it into your Lab Report.

Type the following to close the ssh connection.

```
exit
```

Guided Practice Questions

In your Guided Practice Lab Report, answer the following questions about this learning activity.

1. What is the purpose of ssh?
2. Why did you install ssh on the Ubuntu computer, and not the CentOS computer?
3. What is the relationship of Ansible to ssh?