Name: Olivera, Angelo Carl S.	**Date Performed:** 08-22-2023
Course/Section: CPE232 CPE31S4	**Date Submitted:**
Instructor: Jonathan V. Taylar	**Semester and SY:**

Activity 2: SSH Key-Based Authentication and Setting up Git

1. **Objectives:**

1.1 Configure remote and local machine to connect via SSH using a KEY instead of using a password

1.2 Create a public key and private key

1.3 Verify connectivity

1.4 Setup Git Repository using local and remote repositories

1.5 Configure and Run ad hoc commands from local machine to remote servers

Part 1: Discussion

It is assumed that you are already done with the last Activity (**Activity 1: Configure Network using Virtual Machines).** *Provide screenshots for each task*.

It is also assumed that you have VMs running that you can SSH but requires a password. Our goal is to remotely login through SSH using a key without using a password. In this activity, we create a public and a private key. The private key resides in the local machine while the public key will be pushed to remote machines. Thus, instead of using a password, the local machine can connect automatically using SSH through an authorized key.

What Is ssh-keygen?

Ssh-keygen is a tool for creating new authentication key pairs for SSH. Such key pairs are used for automating logins, single sign-on, and for authenticating hosts.

SSH Keys and Public Key Authentication

The SSH protocol uses public key cryptography for authenticating hosts and users. The authentication keys, called SSH keys, are created using the keygen program.

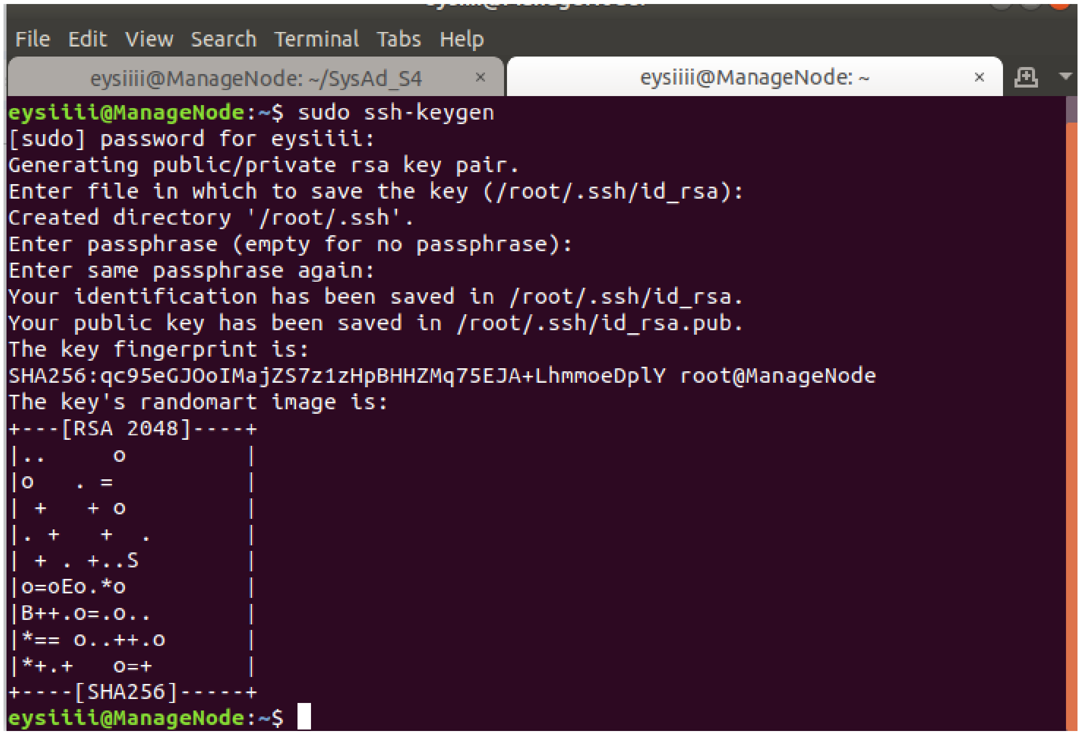
SSH introduced public key authentication as a more secure alternative to the older .rhosts authentication. It improved security by avoiding the need to have password stored in files and eliminated the possibility of a compromised server stealing the user's password.

However, SSH keys are authentication credentials just like passwords. Thus, they must be managed somewhat analogously to usernames and passwords. They should have a proper termination process so that keys are removed when no longer needed.

Task 1: Create an SSH Key Pair for User Authentication

1. The simplest way to generate a key pair is to run *ssh-keygen* without arguments. In this case, it will prompt for the file in which to store keys. First,

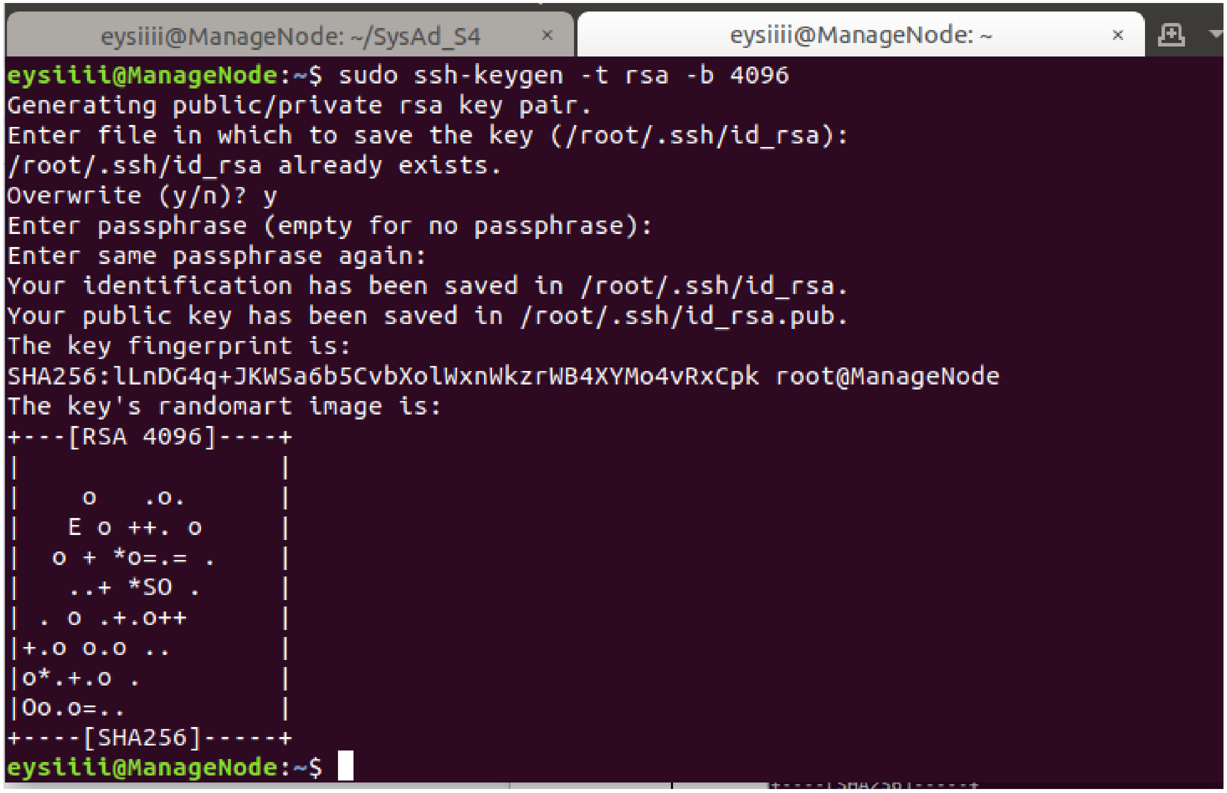
the tool asked where to save the file. SSH keys for user authentication are usually stored in the users .ssh directory under the home directory. However, in enterprise environments, the location is often different. The default key file name depends on the algorithm, in this case *id_rsa* when using the default RSA algorithm. It could also be, for example, *id_dsa* or *id_ecdsa*.



File Edit View Search Terminal Tabs Help
eysiiii@ManageNode: ~/SysAd_S4
eysiiii@ManageNode: ~

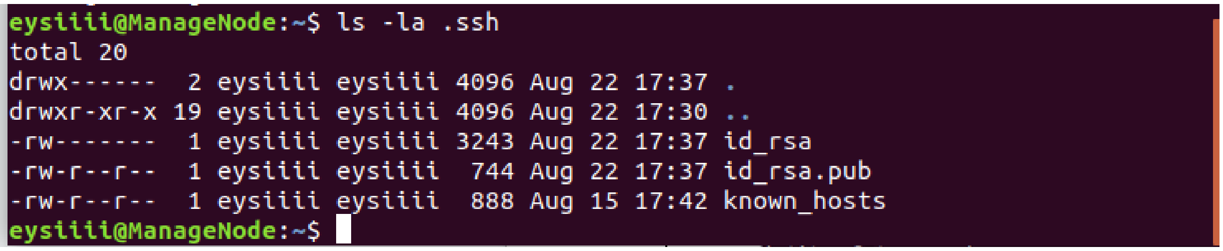
```
eysiiii@ManageNode:~$ sudo ssh-keygen
[sudo] password for eysiiii:
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:qc95eGJOoIMajZS7z1zHpBHHZMq75EJA+LhmmoeDplY root@ManageNode
The key's randomart image is:
+---[RSA 2048]----+
|..     o         |
|o   . =          |
| +   + o         |
|. +   +  .       |
| + . +..S        |
|o=oEo.*o         |
|B++.o=.o..       |
|*== o..++.o      |
|*+.+   o=+       |
+----[SHA256]-----+
eysiiii@ManageNode:~$
```

2. Issue the command *ssh-keygen -t rsa -b 4096.* The algorithm is selected using the -t option and key size using the -b option.



```
eysiiii@ManageNode:~$ sudo ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:lLnDG4q+JKWSa6b5CvbXolWxnWkzrWB4XYMo4vRxCpk root@ManageNode
The key's randomart image is:
+---[RSA 4096]----+
|                 |
|    o   .o.      |
|   E o ++. o     |
|  o + *o=.= .    |
|   ..+ *SO .     |
| . o .+.o++      |
|+.o o.o ..       |
|o*.+.o .         |
|Oo.o=..          |
+----[SHA256]-----+
eysiiii@ManageNode:~$
```

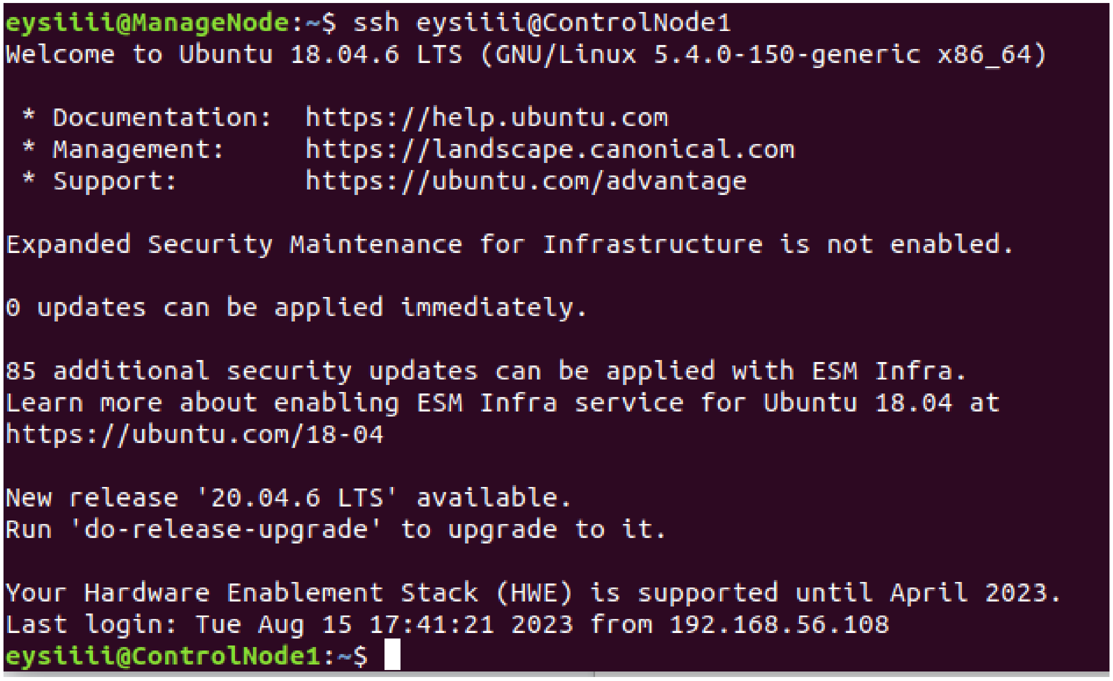
3. When asked for a passphrase, just press enter. The passphrase is used for encrypting the key, so that it cannot be used even if someone obtains the private key file. The passphrase should be cryptographically strong.
4. Verify that you have created the key by issuing the command *ls -la .ssh.* The command should show the .ssh directory containing a pair of keys. For example, id_rsa.pub and id_rsa.



```
eysiiii@ManageNode:~$ ls -la .ssh
total 20
drwx------  2 eysiiii eysiiii 4096 Aug 22 17:37 .
drwxr-xr-x 19 eysiiii eysiiii 4096 Aug 22 17:30 ..
-rw-------  1 eysiiii eysiiii 3243 Aug 22 17:37 id_rsa
-rw-r--r--  1 eysiiii eysiiii  744 Aug 22 17:37 id_rsa.pub
-rw-r--r--  1 eysiiii eysiiii  888 Aug 15 17:42 known_hosts
eysiiii@ManageNode:~$
```

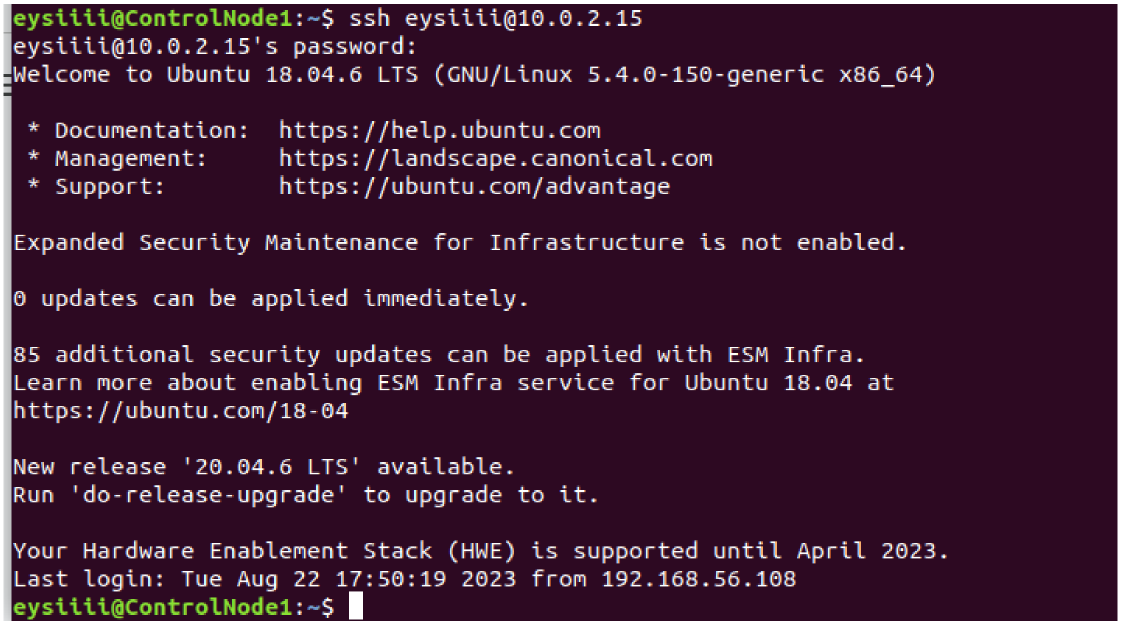
Task 2: Copying the Public Key to the remote servers

1. To use public key authentication, the public key must be copied to a server and installed in an *authorized_keys* file. This can be conveniently done using the *ssh-copy-id* tool.

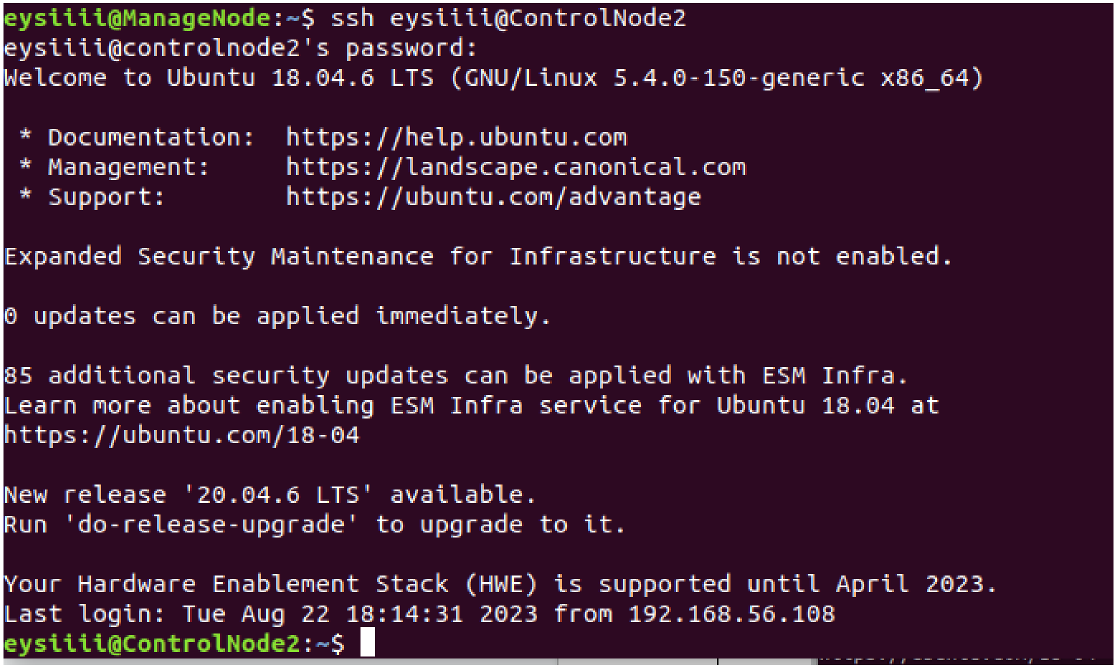


```
eysiiii@ManageNode:~$ ssh eysiiii@ControlNode1
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

85 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 18.04 at
https://ubuntu.com/18-04

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Tue Aug 15 17:41:21 2023 from 192.168.56.108
eysiiii@ControlNode1:~$
```

2. Issue the command similar to this: *ssh-copy-id -i ~/.ssh/id_rsa user@host*

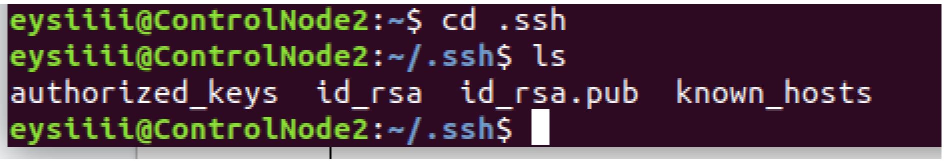


```
eysiiii@ControlNode1:~$ ssh eysiiii@10.0.2.15
eysiiii@10.0.2.15's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

85 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 18.04 at
https://ubuntu.com/18-04

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Tue Aug 22 17:50:19 2023 from 192.168.56.108
eysiiii@ControlNode1:~$
```



```
eysiiii@ManageNode:~$ ssh eysiiii@ControlNode2
eysiiii@controlnode2's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

85 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 18.04 at
https://ubuntu.com/18-04

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Tue Aug 22 18:14:31 2023 from 192.168.56.108
eysiiii@ControlNode2:~$ 
```

3. Once the public key has been configured on the server, the server will allow any connecting user that has the private key to log in. During the login process, the client proves possession of the private key by digitally signing the key exchange.



```
eysiiii@ControlNode2:~$ cd .ssh
eysiiii@ControlNode2:~/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub  known_hosts
eysiiii@ControlNode2:~/.ssh$ 
```

4. On the local machine, verify that you can SSH with Server 1 and Server 2. What did you notice? Did the connection ask for a password? If not, why?

   it connects to server 1 and 2. yes it asks.

Reflections:

Answer the following:

1. How will you describe the ssh-program? What does it do?
   SSH as a secret tunnel that lets you safely control another computer from your own. It's like a private phone line that keeps your conversations (commands and data) secure while you manage the remote computer, even if you're far away.

2. How do you know that you already installed the public key to the remote servers?

   by using this command to the terminal cat ~/.ssh/authorized_keys

Part 2: Discussion

Provide screenshots for each task.

It is assumed that you are done with the last activity (**Activity 2: SSH Key-Based Authentication**).

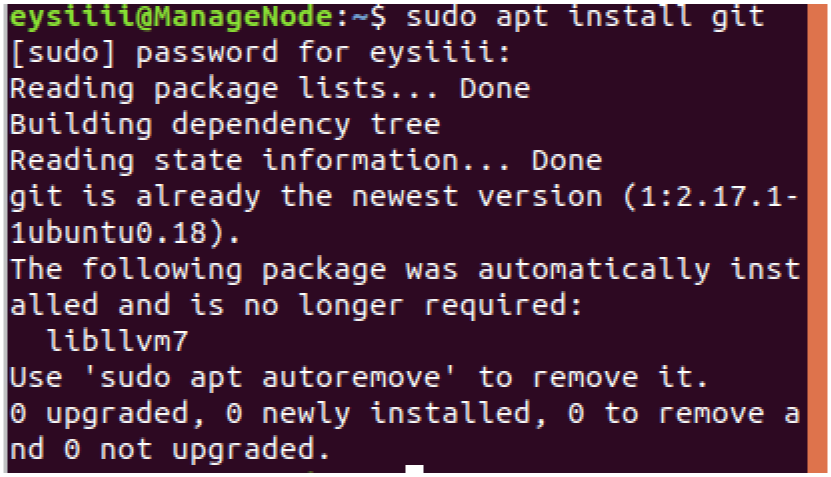
Set up Git

At the heart of GitHub is an open-source version control system (VCS) called Git. Git is responsible for everything GitHub-related that happens locally on your computer. To use Git on the command line, you'll need to download, install, and configure Git on your computer. You can also install GitHub CLI to use GitHub from the command line. If you don't need to work with files locally, GitHub lets you complete many Git-related actions directly in the browser, including:

- Creating a repository
- Forking a repository
- Managing files
- Being social

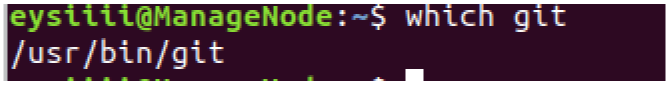
Task 3: Set up the Git Repository

1. On the local machine, verify the version of your git using the command *which git.* If a directory of git is displayed, then you don't need to install git. Otherwise, to install git, use the following command: *sudo apt install git*



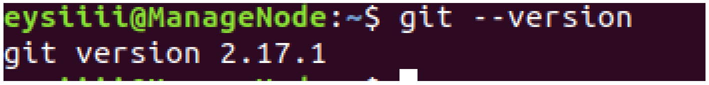
```
eysiiii@ManageNode:~$ sudo apt install git
[sudo] password for eysiiii:
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version (1:2.17.1-
1ubuntu0.18).
The following package was automatically inst
alled and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove a
nd 0 not upgraded.
```

2. After the installation, issue the command *which git* again. The directory of git is usually installed in this location: *user/bin/git.*



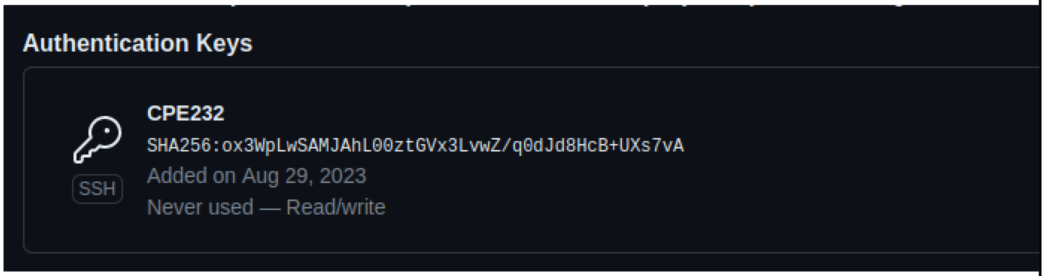
```
eysiiii@ManageNode:~$ which git
/usr/bin/git
```

3. The version of git installed in your device is the latest. Try issuing the command *git --version* to know the version installed.



```
eysiiii@ManageNode:~$ git --version
git version 2.17.1
```

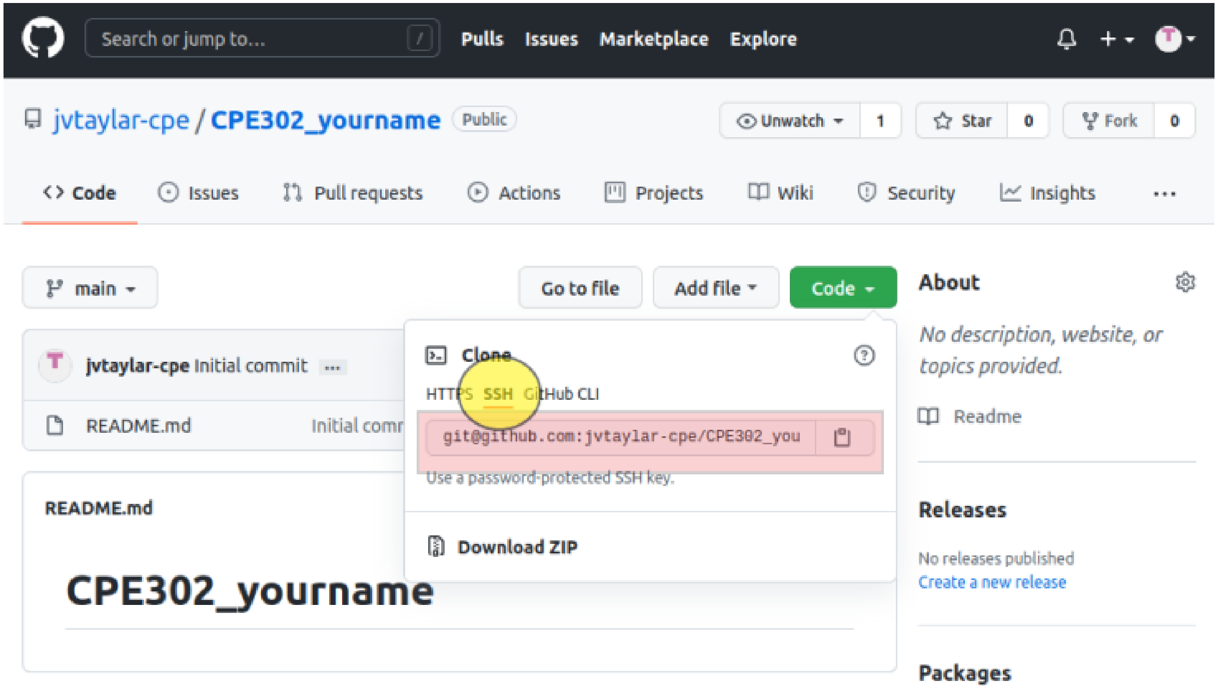
4. Using the browser in the local machine, go to www.github.com.
5. Sign up in case you don't have an account yet. Otherwise, login to your GitHub account.
    a. Create a new repository and name it as CPE232_yourname. Check Add a README file and click Create repository.
    b. Create a new SSH key on GitHub. Go your profile's setting and click SSH and GPG keys. If there is an existing key, make sure to delete it. To create a new SSH keys, click New SSH Key. Write CPE232 key as the title of the key.
    c. On the local machine's terminal, issue the command cat .ssh/id_rsa.pub and copy the public key. Paste it on the GitHub key and press Add SSH key.



Authentication Keys

CPE232
SHA256:ox3WpLwSAMJAhL00ztGVx3LvwZ/q0dJd8HcB+UXs7vA
Added on Aug 29, 2023
Never used — Read/write

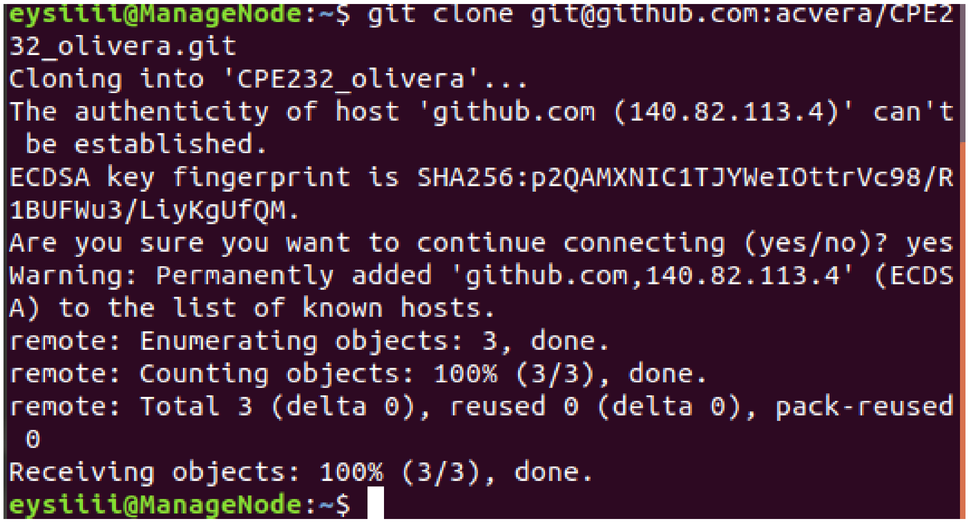
    d. Clone the repository that you created. In doing this, you need to get the link from GitHub. Browse to your repository as shown below. Click on the Code drop down menu. Select SSH and copy the link.



git@github.com:jvtaylar-cpe/CPE302_you

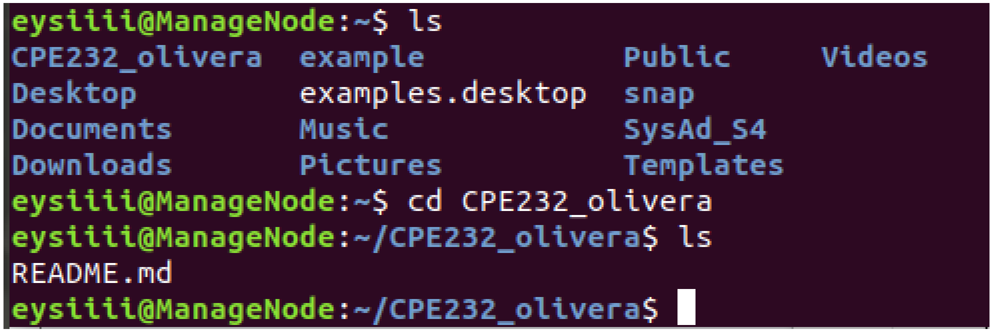
Use a password-protected SSH key.

e. Issue the command git clone followed by the copied link. For example, *git clone* git@github.com:jvtaylar-cpe/CPE232_yourname.git. When prompted to continue connecting, type yes and press enter.



```
eysiiii@ManageNode:~$ git clone git@github.com:acvera/CPE2
32_olivera.git
Cloning into 'CPE232_olivera'...
The authenticity of host 'github.com (140.82.113.4)' can't
 be established.
ECDSA key fingerprint is SHA256:p2QAMXNIC1TJYWeIOttrVc98/R
1BUFWu3/LiyKgUfQM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'github.com,140.82.113.4' (ECDS
A) to the list of known hosts.
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused
 0
Receiving objects: 100% (3/3), done.
eysiiii@ManageNode:~$
```

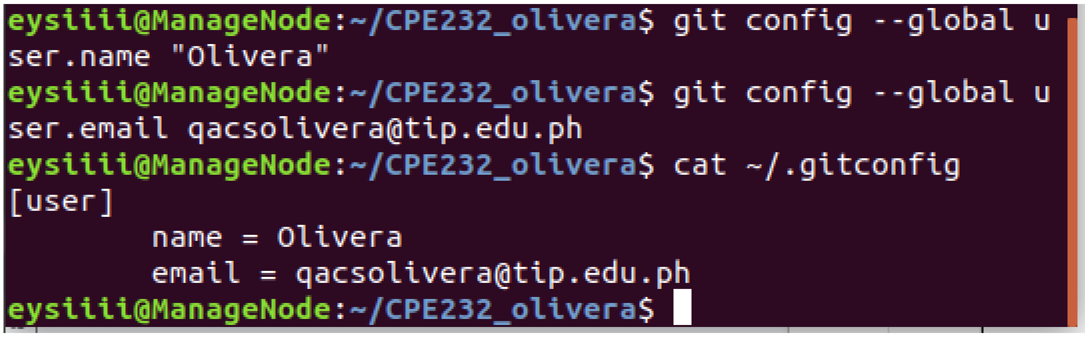
f. To verify that you have cloned the GitHub repository, issue the command *ls*. Observe that you have the CPE232_yourname in the list of your directories. Use CD command to go to that directory and LS command to see the file README.md.



```
eysiiii@ManageNode:~$ ls
CPE232_olivera  example           Public     Videos
Desktop         examples.desktop  snap
Documents       Music             SysAd_S4
Downloads       Pictures          Templates
eysiiii@ManageNode:~$ cd CPE232_olivera
eysiiii@ManageNode:~/CPE232_olivera$ ls
README.md
eysiiii@ManageNode:~/CPE232_olivera$ 
```

g. Use the following commands to personalize your git.

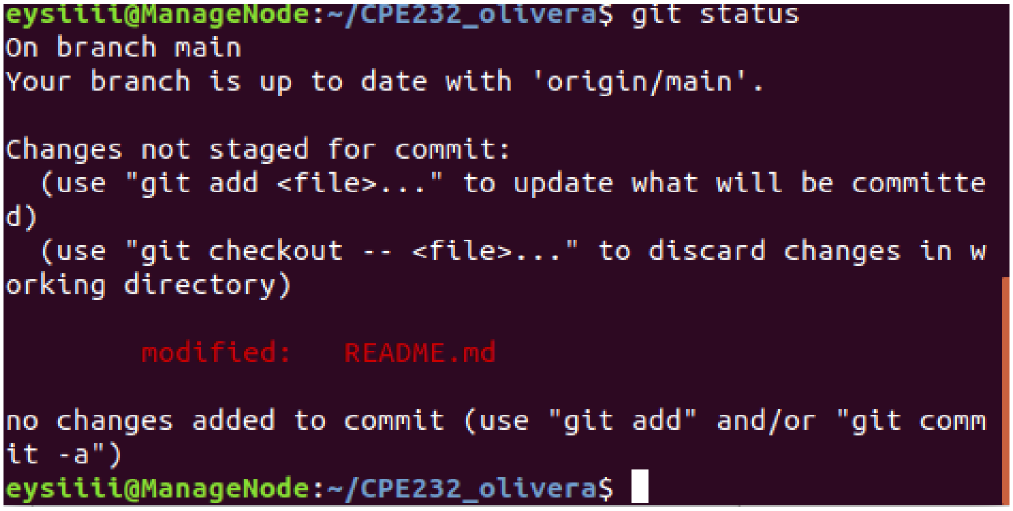
- *git config --global user.name "Your Name"*
- *git config --global user.email yourname@email.com*
- Verify that you have personalized the config file using the command *cat ~/.gitconfig*



```
eysiiii@ManageNode:~/CPE232_olivera$ git config --global u
ser.name "Olivera"
eysiiii@ManageNode:~/CPE232_olivera$ git config --global u
ser.email qacsolivera@tip.edu.ph
eysiiii@ManageNode:~/CPE232_olivera$ cat ~/.gitconfig
[user]
        name = Olivera
        email = qacsolivera@tip.edu.ph
eysiiii@ManageNode:~/CPE232_olivera$ 
```

h. Edit the README.md file using nano command. Provide any information on the markdown file pertaining to the repository you created. Make sure to write out or save the file and exit.

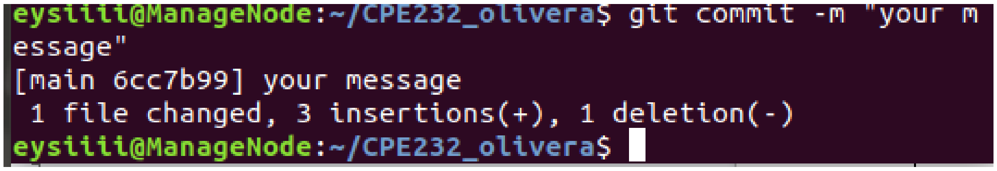
i. Use the *git status* command to display the state of the working directory and the staging area. This command shows which changes have been staged, which haven't, and which files aren't being tracked by Git. Status output does not show any information regarding the committed project history. What is the result of issuing this command?



```
eysiiii@ManageNode:~/CPE232_olivera$ git status
On branch main
Your branch is up to date with 'origin/main'.

Changes not staged for commit:
  (use "git add <file>..." to update what will be committe
d)
  (use "git checkout -- <file>..." to discard changes in w
orking directory)

        modified:   README.md

no changes added to commit (use "git add" and/or "git comm
it -a")
eysiiii@ManageNode:~/CPE232_olivera$ 
```

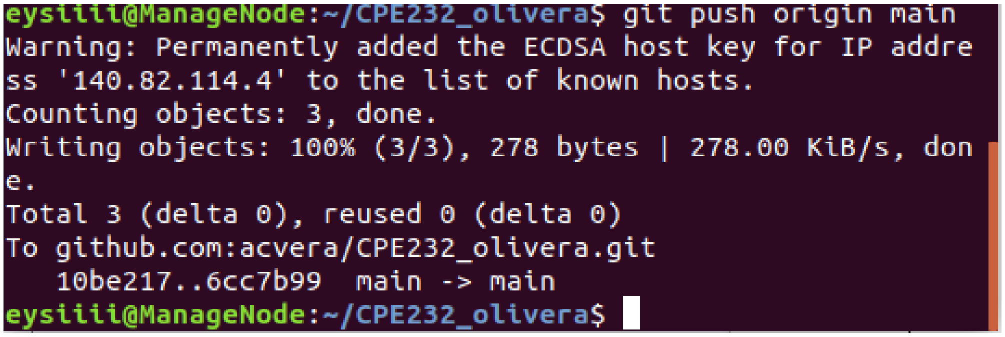
j. Use the command *git add README.md* to add the file into the staging area.

k. Use the *git commit -m "your message"* to create a snapshot of the staged changes along the timeline of the Git projects history. The use of this command is required to select the changes that will be staged for the next commit.



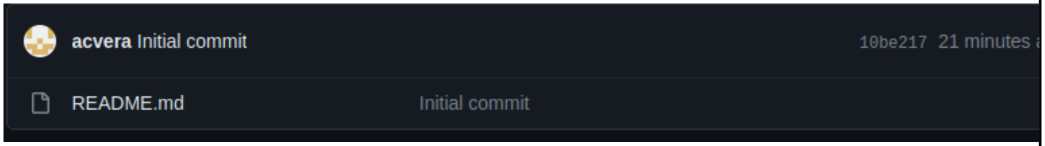
```
eysiiii@ManageNode:~/CPE232_olivera$ git commit -m "your m
essage"
[main 6cc7b99] your message
 1 file changed, 3 insertions(+), 1 deletion(-)
eysiiii@ManageNode:~/CPE232_olivera$ 
```

l. Use the command *git push <remote><branch>* to upload the local repository content to GitHub repository. Pushing means to transfer commits from the local repository to the remote repository. As an example, you may issue *git push origin main.*



```
eysiiii@ManageNode:~/CPE232_olivera$ git push origin main
Warning: Permanently added the ECDSA host key for IP addre
ss '140.82.114.4' to the list of known hosts.
Counting objects: 3, done.
Writing objects: 100% (3/3), 278 bytes | 278.00 KiB/s, don
e.
Total 3 (delta 0), reused 0 (delta 0)
To github.com:acvera/CPE232_olivera.git
   10be217..6cc7b99  main -> main
eysiiii@ManageNode:~/CPE232_olivera$ 
```

m. On the GitHub repository, verify that the changes have been made to README.md by refreshing the page. Describe the README.md file. You can notice the how long was the last commit. It should be some minutes ago and the message you typed on the git commit command should be there. Also, the README.md file should have been edited according to the text you wrote.



acvera Initial commit 10be217 21 minutes a

README.md Initial commit

Reflections:

Answer the following:

3. What sort of things have we so far done to the remote servers using ansible commands?

   We explore and learn the basic of remote hosting and accessing other stations.

4. How important is the inventory file?

It is important because it allows the user to hava a list that allows the admin to manage and host the other stations.

Conclusions/Learnings:

We've learned how to connect to far-away computers using special keys instead of passwords for safety, create these keys as a pair to unlock secure communication, verify that your connection works well, set up safe places for your computer code to collaborate with others, and send quick instructions to far-away computers using those same special keys, all of which empower you to work securely and efficiently in remote and collaborative environments.