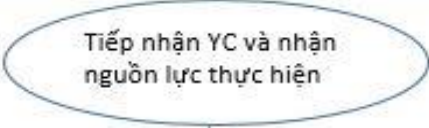
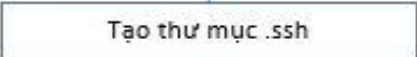
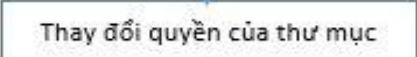
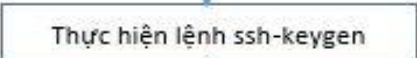
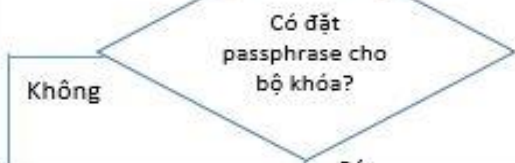
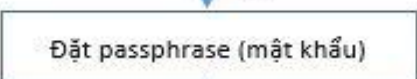
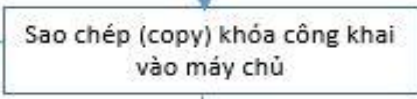


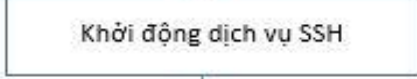
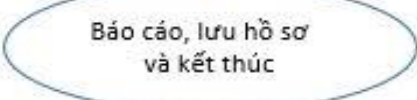


QUY TRÌNH TẠO BỘ KHÓA SSH CHO MÁY TÍNH CHẠY LINUX (Ubuntu)

A. LƯU ĐỒ QUY TRÌNH

Bước	Trách nhiệm	Lưu đồ	Biểu mẫu - Tài liệu
1	Trưởng bộ phận hệ thống, và Nhân viên hệ thống		1. Phiếu yêu cầu, 2. Tài liệu hướng dẫn tạo bộ khóa SSH có Ủy quyền quản trị (username, password)
2	Nhân viên hệ thống		Tài liệu hướng dẫn tạo bộ khóa SSH có Ủy quyền quản trị (username, password)
3	Nhân viên hệ thống		Tài liệu hướng dẫn tạo bộ khóa SSH có Ủy quyền quản trị (username, password)
4	Nhân viên hệ thống		Tài liệu hướng dẫn tạo bộ khóa SSH có Ủy quyền quản trị (username, password)
5	Nhân viên hệ thống		Tài liệu hướng dẫn tạo bộ khóa SSH có Ủy quyền quản trị (username, password)
6	Nhân viên hệ thống		Tài liệu hướng dẫn tạo bộ khóa SSH có Ủy quyền quản trị (username, password)
7	Nhân viên hệ thống		Tài liệu hướng dẫn tạo bộ khóa SSH có Ủy quyền quản trị (username, password)
8	Nhân viên hệ thống		Tài liệu hướng dẫn tạo bộ khóa SSH có Ủy quyền quản trị (username, password)
9	Nhân viên hệ thống		Tài liệu hướng dẫn tạo bộ khóa SSH có Ủy quyền quản trị (username, password)
10	Nhân viên hệ thống		Tài liệu hướng dẫn tạo bộ khóa SSH có Ủy quyền quản trị (username, password)
11	Trưởng bộ phận hệ thống, và Nhân viên hệ thống		1. Phiếu yêu cầu, 2. Biên bản nghiệm thu kết quả tạo bộ khóa SSH 3. Tài liệu hướng dẫn... được cập nhật mới

B. DIỄN GIẢI

Bước 1: Tiếp nhận yêu cầu (YC) và nhận nguồn lực thực hiện

Trưởng bộ phận hệ thống tiến hành:

- Lập Phiếu yêu cầu công việc theo mẫu chung của Phòng CNTT
- Phân công nhân viên hệ thống tạo bộ khóa SSH qua Phiếu yêu cầu (có quy định nội dung thực hiện, lịch thực hiện, nguồn lực được cấp, báo cáo hoàn thành bằng biên bản nghiệm thu v.v.);
- Bàn giao nguồn lực thực hiện (phần cứng (máy chủ Ubuntu Linux (server) và máy cục bộ (local machine)), tài liệu hướng dẫn tạo bộ khóa SSH, ủy quyền quản trị (users, password) cho nhân viên nhận việc và các nguồn lực cần thiết khác để thực hiện được nhiệm vụ;

Biểu mẫu đầu vào của Bước này là:	- Phiếu Yêu cầu công việc của Phòng CNTT
Biểu mẫu đầu ra của Bước này là:	- Phiếu Yêu cầu của Trưởng bộ phận hệ thống có đủ thông tin và có ký xác nhận - Tài liệu hướng dẫn tạo bộ khóa SSH có kèm thông tin ủy quyền quản trị

Bước 2: Tạo thư mục .ssh

Theo tài liệu hướng dẫn tạo bộ khóa SSH, nhân viên hệ thống tiến hành lệnh sau đây để tạo một cặp khóa SSH trên hệ thống máy khách. Hệ thống máy khách là máy kết nối với máy chủ SSH.

Vào cửa sổ dòng lệnh (command line), gõ tổ hợp phím CTRL+ALT+T, tạo một thư mục có tên .ssh trong thư mục chính với tùy chọn -p đảm bảo hệ thống không trả về lỗi nếu thư mục tồn tại:

```
mkdir -p $HOME/.ssh
```

Bước 3: Thay đổi quyền của thư mục

Sau khi thực hiện xong Bước 2, nhân sự hệ thống tiếp tục tiến hành thay đổi quyền của thư mục để cấp cho người dùng các đặc quyền đọc, viết và thực thi:

```
chmod 0700 $HOME/.ssh
```

Bước 4: Thực hiện lệnh ssh-keygen

Sau khi thực hiện xong Bước 3, nhân sự hệ thống tiếp tục tiến hành thực thi lệnh ssh-keygen để tạo cặp khóa RSA:

```
ssh-keygen
```

Bước 5: Có đặt passphrase cho bộ khóa?

Sau khi thực hiện xong Bước 4, hệ thống yêu cầu bạn tạo cụm mật khẩu (“passphrase”) như một lớp bảo mật bổ sung. Nếu đồng ý thì thực hiện bước 6; nếu không thực hiện bước 7.

Bước 6: Đặt passphrase (mật khẩu)

Nhập cụm mật khẩu dễ nhớ và nhấn Enter.

Kết quả đầu ra cho thấy các khóa đã được tạo thành công – xem hình

```
marko@pnap:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/marko/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/marko/.ssh/id_rsa
Your public key has been saved in /home/marko/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Crkc+tF9/pbHPz72LUzCGpsqpavCXv+B0IhnTLLU4CA marko@pnap
The key's randomart image is:
+---[RSA 3072]-----+
|E . oo                |
| . + .                |
|   o                  |
|   o +                |
|  o X . S .           |
|   O * +. . O .       |
| .. * +OO . = *       |
|  oo oo ++ o =+.      |
| ...o.o+o..o..o+B     |
+---[SHA256]-----+
marko@pnap:~$
```

Bước 7: Sao chép (copy) khóa công khai vào máy chủ

Sau khi thực hiện xong Bước 6, nhân sự hệ thống tiếp tục tiến hành sau khi có được cặp khóa, sử dụng khóa chung để xác thực ứng dụng khách trên máy chủ:

1. Lấy địa chỉ IP của máy chủ Ubuntu mà bạn muốn kết nối. Trong cửa sổ terminal của máy chủ, nhập lệnh sau:

```
ip a
```

Tìm địa chỉ IP của hệ thống trong phần thiết bị mạng liên quan:

```
marko@pnap:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f4:54:24 brd ff:ff:ff:ff:ff:ff
    inet 10.240.12.56/24 metric 100 brd 10.240.12.255 scope global dynamic enp0s3
        valid_lft 691186sec preferred_lft 691186sec
    inet6 fe80::a00:27ff:fe4:5424/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:ed:26:4b:c8 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
marko@pnap:~$
```

2. Trên hệ thống máy khách, sử dụng lệnh `ssh-copy-id` để sao chép thông tin nhận dạng vào máy chủ Ubuntu. Sử dụng tùy chọn `-i` để chỉ định khóa muốn chia sẻ:

```
ssh-copy-id -i [ssh-key-location] [username]@[server-ip-address]
```

Hệ thống sao chép nội dung của `~/.ssh/id_rsa.pub` từ hệ thống máy khách vào tệp `~/.ssh/authorized_keys` trên máy chủ.

Nếu đây là lần đầu tiên bạn kết nối với máy chủ, bạn có thể thấy thông báo cho biết không thể thiết lập tính xác thực của máy chủ. Nhập `Yes` và nhấn `Enter` để tiếp tục.

3. Nhập mật khẩu cho tài khoản người dùng máy chủ.

```
marko@pnap:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub marko@10.240.12.56
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/marko/.ssh/id_rsa.pub"
The authenticity of host '10.240.12.56 (10.240.12.56)' can't be established.
ED25519 key fingerprint is SHA256:oBcISkp3bH/rVJ0LccQHGroknSk01fGRGDz1/XtShYw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? 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
marko@10.240.12.56's password:
Number of key(s) added: 1
Now try logging into the machine, with: "ssh 'marko@10.240.12.56'"
and check to make sure that only the key(s) you wanted were added.
marko@pnap:~$
```

Bước 8: Đăng nhập (login) vào máy chủ (server)

Sau khi thực hiện xong Bước 7, nhân sự hệ thống tiếp tục tiến hành đăng nhập vào máy chủ (từ xa), nhập lệnh sau trên hệ thống máy khách:

```
ssh [tên người dùng]@[server-ip]
```

```
marko@pnap:~$ ssh marko@10.240.12.56
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-53-generic x86_64)

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

System information as of Thu Nov 17 03:12:30 PM UTC 2022

System load:  0.0               Processes:            115
Usage of /:   48.1% of 17.77GB   Users logged in:     1
Memory usage: 7%               IPv4 address for docker0: 172.17.0.1
Swap usage:   0%               IPv4 address for enp0s3: 10.240.12.56

Last login: Thu Nov 17 15:12:30 2022 from 10.240.12.34
marko@pnap:~$
```

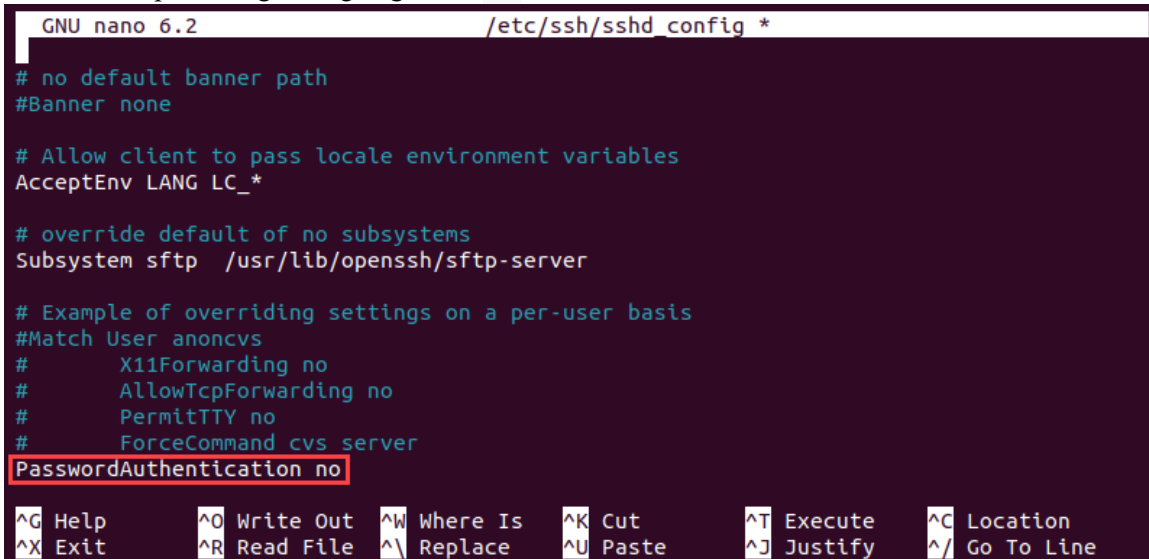
Bước 9: Cắt xác thực mật khẩu (Disable Password Authentication)

Sau khi thực hiện xong Bước 8, nhân sự hệ thống tiếp tục tiến hành làm mất (tắt) khả năng xác thực khóa riêng bằng mật khẩu của dịch vụ SSH. Bước 9 này cho phép tạo ra một lớp bảo mật bổ sung nhưng nếu chỉ có duy nhất một người dùng đăng nhập vào máy chủ thì có thể tắt xác thực mật khẩu. Máy chủ sẽ chỉ chấp nhận thông tin đăng nhập từ máy khách bằng khóa riêng khớp với khóa chung được lưu trữ. Thực hiện tuần tự các hành động sau:

1. Mở tập tin **sshd_config** trong bộ soạn thảo văn bản (text editor):

```
sudo nano /etc/ssh/sshd_config
```

2. Tìm kiếm dòng **PasswordAuthentication** trong tập tin.
3. Sửa đổi tập tin bằng cách gán giá trị: **no**



```
GNU nano 6.2 /etc/ssh/sshd_config *
# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server
PasswordAuthentication no

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

4. Lưu tập tin và thoát (Save the file and exit).

Bước 10: Khởi động dịch vụ SSH

Sau khi thực hiện xong Bước 9, nhân sự hệ thống tiếp tục tiến hành khởi động lại dịch vụ SSH service bằng cách nhập lệnh :

```
sudo systemctl restart ssh
```

Bước 11: Báo cáo, lưu hồ sơ và kết thúc

Sau khi thực hiện xong Bước 10, nhân sự hệ thống tiếp tục tiến hành:

- Soạn và ký trước biên bản nghiệm thu;
- Báo cáo cho Trưởng bộ phận hệ thống quá trình thực hiện, kết quả thực hiện nhiệm vụ;
- Bàn giao biên bản nghiệm thu cho Trưởng bộ phận hệ thống để hậu kiểm và đồng ký xác nhận.
- Lưu hồ sơ gồm tất cả văn bản và biểu mẫu phát sinh từ Bước 1 đến Bước 10.

----- ./ -----