Tech Startup System Documentation

CONTENTS

INTRODUCTION

This document contains the documentation of the virtual machine setup to csc.fi cloud environment. The documentation provides the technical description and details to setup the virtual machine.

Document change log

Version	Date	Author	Description
1.0.0	22.3.2022	-	Initial version. Server setup with public IP and default user
1.2.0	25.3.2022	Safiul alam	Adding root user; adding users; activating TOTD service
1.3.0	18/4/2022	Safiul Alam	Setup server monitoring to centreon.eduhou.fi and tuni homepages. Update DNS name
1.4.0	1/5/2022	Safiul Alam	Configure NFS server; enable tips folder mounting from NFS host
1.5.0	15/5/2022	Safiul alam	Apache setup
1.60	15/5/2022	Safiul alam	CMBD

1 System overview

1.1 System components

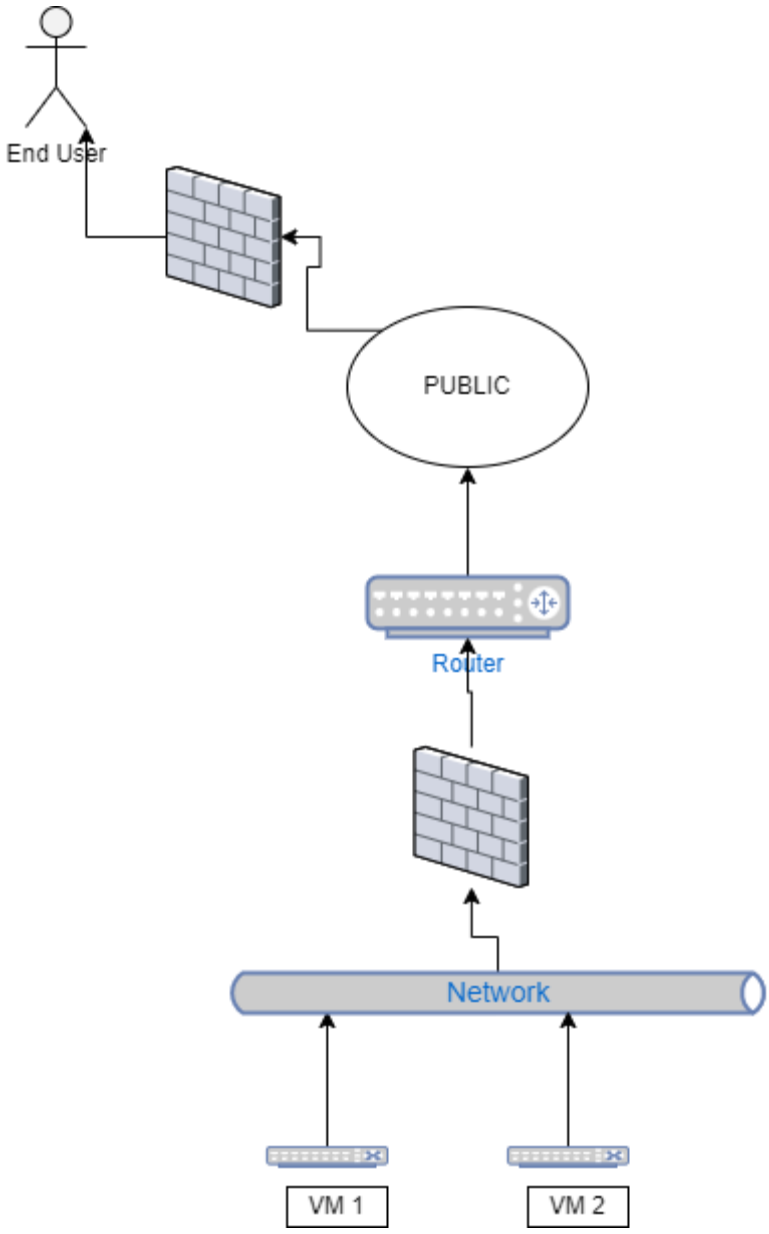
Image size: 70GB

Availability zone: nova

Operating system: Ubuntu-20.04 (2.2 GB)

Security groups: safi-sec-group

1.1.1 System network diagram



2 Security

A lot must be taken into consideration when running your own server. Systems are constantly under attack, therefore ensuring proper security protocols gives it a safe safety net.

Security guidelines for Pouta recommends various security measures to ensure safe running of virtual machines.

- Secure the virtual machine with strict firewalls as they are connected to the public internet.
- Enable automatic updates to stay up to date on any security update.
- Subscribe to security announcements for your OS to be notified of any security compromise or recent updates to be able to take early steps to ensure your machines safety.
- Run a strict firewall – instances should be configured to allow minimum required outside access to run the service.
- Disable any unused or unnecessary accounts from the machine and services.
- Use keys to login as they provide more security over conventional password login.

Full csc security guidelines here

2.1 Security settings

3 Pouta cloud

3.1 Settings

3.1.1 Host

Name	IP	Description
Safiul Alam	128.214.255.79	vm4390.kaj.pouta.csc.fi.

3.1.2 Users

User	Sudo	Contact	Description
Safiul	Yes	Safiul.alam@tuni.fi	Root user; TOTD disabled
Anmol	No	Anmol.arora@tuni.fi	Guest user; TOTD enabled
Elina	No	elina.widdowson@tuni.fi	Guest user; TOTD enabled
Nikke	No	nikke.karaksela@tuni.fi	Guest user; TOTD enabled
Sam22	No		Instructor; TOTD enabled

3.2 Access list

From	To	Description
80.220.251.92/32	0.0.0.0/0	Safiul home IP
0.0.0.0/0	::/0	Temporary access for users

From	Ports / protocols	Description
128.214.252.51 / 32	ICMP: ALL SSH, HTTP, HTTPS, NFS	centreon.eduhou.fi - Monitoring server access
193.166.164.193 / 24	SSH	Access from Tuni linux and homepages servers

3.3 SSH configuration

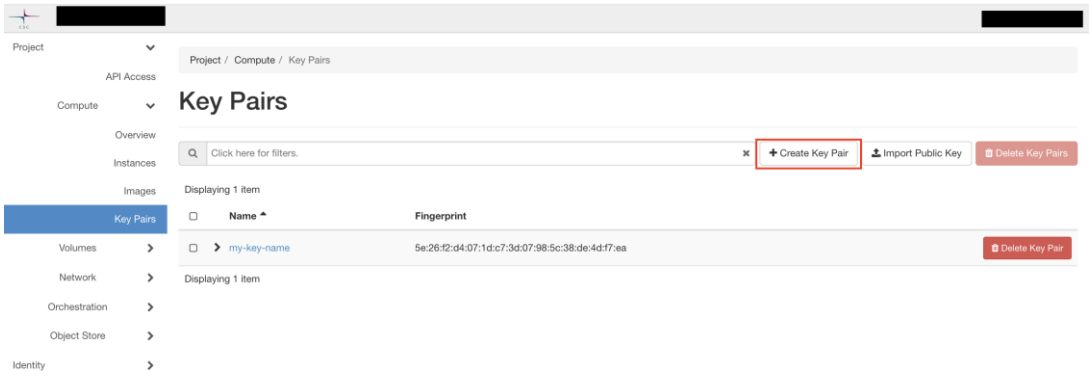
To setup SSH based login

- Create a SSH key #give a passphrase

  $ Ssh-keygen

Pouta key pair

- Add the .pub key to Pouta



3.3.1 Adding users using SSH

Add user:

```
$ sudo useradd -m -u 1722 -s /bin/bash meuser
```

Configuring SSH based login:

```
$ sudo -i
# cd ~pal
# mkdir .ssh
# touch .ssh/authorized_keys
# chown -R pal:pal .ssh
# chmod 600 .ssh/authorized_keys
```

Copy SSH key to

```
.ssh/authorized_keys
```

SSH rules:

- Store your private ssh key somewhere safe.
- Root access restricted
- SSH timeout period set

3.4 Setting up automatic updates

- Upgrading system

sudo apt update && sudo apt upgrade

sudo apt install unattended-upgrades

configuring automatic updates

making changes to “/etc/apt/apt.conf.d/50unattended-upgrades” to automatically update, upgrade and reboot

- turning on automatic reboot for kernel updates

turning auto updates to “true” in /etc/apt/apt.conf.d/20auto-upgrades

3.5 Setting NFS server

3.5.1 Host

Name	IP	Description
Nfshost	192.168.1.22	Server to host TOTD service on to sakip machine

3.5.1 Users

User	Sudo	Contact	Description
Safiul	Yes	Safiul.alam@tuni.fi	Root user;

3.5.2 Security

Name	IP	Security group
Nfshost	192.168.1.22	Safi-sec-group; Sakip nfs

3.5.3 Access

Name	IP	Service
Sakip	128.214.255.79	Personal VM

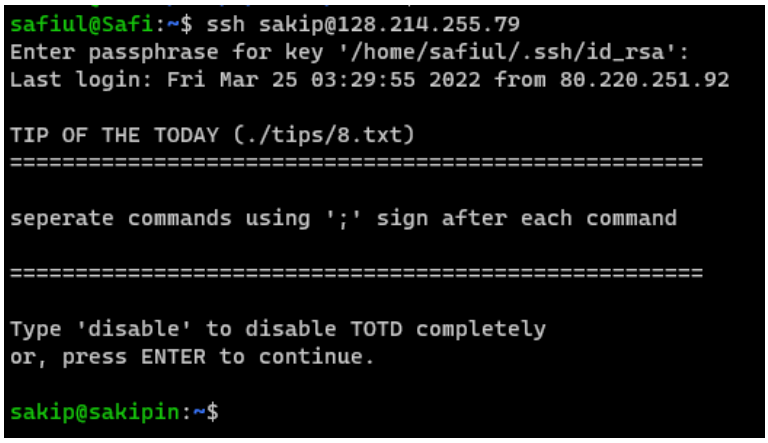
4 Services

4.1 Tip of the day v1

It is a service to prompt user with a helpful tip every time they SSH in to the Linux machine. The resources to enable the service can be here.

It contains a bash script in the /etc/profile. It also has a functionality to disable upon users request.

Example:



4.2 Tip of the day NFS

For the following service we initialize the same Tip of the day bash script to show a new linux tips on every login. But for this service instead of reading the tips files locally, we store the tips files in a NFS server as a host and on every login the NFS disk mounts with our main cPouta client virtual machine and reads the tips off the mounted folder

Initializing the mount on the host and client server. In this context the host is the NFS server and the client is the sakip virtual machine

Installing components

On the host

```
sudo apt update
sudo apt install nfs-kernel-server
```

on the client

```
sudo apt update
sudo apt install nfs-common
```

Creating the share directorires on the host with tips text files

```
sudo mkdir /home/sakip/totd/tips/{1..10}.txt -p
```

converting root operations on the client to nobody:nobody credentials as security measure

```
sudo chown nobody:nogroup /home/sakip/totd/tips/
```

configure NFS exports on the host server

```
sudo nano /etc/exports
```

edit the exports file by adding this

the line below essentially gives the client computer read and write permissions.

```
home/sakip/totd/tips  client_ip(rw,sync,no_subtree_check)
```

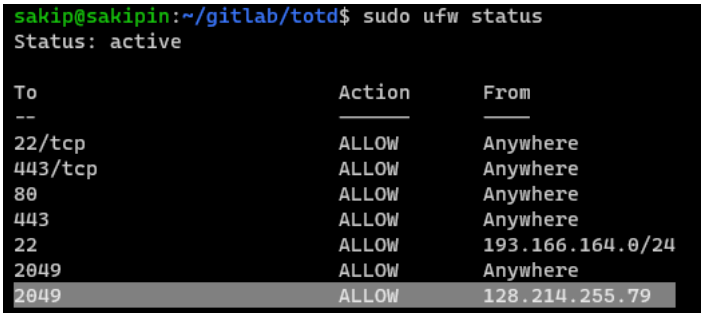
Restart server to apply changes

```
sudo systemctl restart nfs-kernel-server
```

Firewall settings

Check firewall status

```
sudo ufw status
```



Allow traffic from client on the host server

```
sudo ufw allow from client_ip to any port nfs
```

verify change

```
sudo ufw status
```

Client-side mount

After creating the directories where you will be mounting the files from NFS server, run the mount command as follows

```
sudo mount host_ip: home/sakip/totd/tips /home/sakip/gitlab/totd/v1tips
```

check the mount status

```
df -h
```

```
192.168.1.23:/var/nfs/general        78G  1.9G   76G   3% /nfs/general
tmpfs                               973M     0  973M   0% /run/user/1361
192.168.1.23:/home/sakip/totd/tips   78G  1.9G   76G   3% /home/sakip/gitlab/totd/v1tips
```

Changes to TOTD script

Only change made to the linuxtips.sh script in /etc/profile.d is whenever the script Runs, it will first mount with the host in case any new tips files were added and then continue to run the script of reading and displaying the tips messages on every login.

Find the shell repo here

```
 GNU nano 4.8                                    linuxtips.sh
!/bin/bash
whoami=$(whoami)
sudo mount 192.168.1.23:/home/sakip/totd/tips /home/sakip/gitlab/totd/v1tips
 cd /home/$whoami/gitlab/totd/

CURTIP=$(cat ./.curtip)
TIPFILE=./tips/$CURTIP.txt
NUMTIPS=`ls ./tips/*.txt | wc -l`
```

Totd – HTTP static

The following config fetches the tips from a webserver such as from http://tips.sakip.ilab.fi/tips/1.txt and displays it in the Totd on system start up.

Setup

Install apache2

```
$ sudo apt install apache2
```

Configuration

```
$ cd /var/www/
$ mkdir tips.sakip.ilab.fi
```

Make some default content to index.html

```
$ cd /var/www/
$ sudo vi tips.sakip.ilab.fi/index.html
$ cat tips.sakip.ilab.fi/index.html
TotD - Hello!
```

```
$ cd /etc/apache2/sites-available
$ sudo cp -p 000-default.conf tips.ada.ilab.fi.conf
$ sudo vi tips.sakip.ilab.fi.conf
...
$ cat tips.sakip.ilab.fi.conf

<VirtualHost *:80>
       ServerName tips.sakip.ilab.fi
       ServerAdmin webmaster@localhost
        DocumentRoot /var/www/tips.sakip.ilab.fi
        ErrorLog ${APACHE_LOG_DIR}/tips.sakip.error.log
       CustomLog ${APACHE_LOG_DIR}/tips.sakip.access.log com-
bined
</VirtualHost>
```

Enabling site

```
$ sudo a2ensite tips.sakip.ilab.fi
$ sudo systemctl reload apache2
```

Serving Totd from webserver

```
$ cd /var/www/tips.sakip.ilab.fi
$ ln -s /opt/stec/<your repo name>/tips
$ ln -s /opt/stec/<your repo name>/tips txt
$ ln -s /opt/stec/<your repo name>/tips files
```

5 CMDB

The CMDB service is responsible to keep track of changes to the server contents. It automates the tedious tasks of manually ssh into every file and make changes to the systems.

How it works

The configuration files of the server are hosted on a VCS repo, everytime an update is to made it is made in the repo. Thus the system receives the update automatically. CMDB is especially vital when it comes to maintain a large infra-structure

5.1 Folder Structure

The following is the folder structure of the configuration of SAKIPIN system in Gitlab repo to be managed and maintained

```
.
├── nfs
│   ├── etc
│   │   ├── exports
│   │   ├── sudoers.d
│   │   │   └── 91-stec22-users
│   │   └── ufw
│   │       ├── ufw.conf
│   │       ├── user.rules
│   │       └── user6.rules
│   └── var
└── sakipin
    ├── etc
    │   ├── apache2
    │   │   ├── apache2.conf
    │   │   └── sites-enabled
    │   │       ├── 000-default.conf -> ../sites-available/000-default.conf
    │   │       └── tips.sakip.ilab.fi.conf -> ../sites-available/tips.sakip.ilab.fi.conf
    │   ├── apt
    │   │   └── apt.conf.d
    │   │       └── 50unattended-upgrades
    │   ├── bash.bashrc
```

```
│   ├── fstab
│   ├── hosts
│   ├── inputrc
│   ├── passwd
│   ├── ssh
│   │   └── sshd_config
│   ├── sudoers.d
│   │   └── 91-stec22-users
│   └── ufw
│       ├── ufw.conf
│       ├── user.rules
│       └── user6.rules
└── var
    └── www
        ├── html
        │   └── index.html
        └── tips.sakip.ilab.fi
            ├── files -> /home/sakip/gitlab/totd/tips
            ├── index.html
            ├── tips -> /home/sakip/gitlab/totd/tips
            └── txt -> /home/sakip/gitlab/totd/tips
```

Quality and operation requirements

- In cPouta virtual machines (VM) can be directly connected to the internet. The user is responsible for the security of their VM's.
- Users are responsible for managing their access control list, firewall, user accounts and all other access control methods.
- Users are responsible for maintaining operating systems and applications.
- Users can do the following guidelines to secure their VM:
    - All OS have the ability to update automatically.
    - Upgrade the kernel.
    - If there is a security flaw in the system, it is essential to find and resolve it asap. Turn on products mailing list to stay up to date on security information.
    - Run a restrictive firewall and use host based firewall.

REFERENCES

Petter jekunen – guidelines - https://docs.google.com/document/d/e/2PACX-1vRSO0e7jbySOXeVBBTUb-PZJh5hOuNVh1nc9I2Fv3QmKQ1vekjpo8P3MWmENwnxwMoUQ1i6BSlQCPWWO/pub

Csc.fi - security guidelines - https://docs.csc.fi/cloud/pouta/security/?pk_vid=2e24cc96607a302716161371410e04d7