Tech Startup System Documentation template

**Table of contents**

[**Introduction**](#_e0t82526ch48)[**1**](#_kfivubjt0pu1)

[Document change log](#_oi7or99nczuu) [1](#_oi7or99nczuu)

[**System overview**](#_b8xdekdp5wh8)[**2**](#_b8xdekdp5wh8)

[System components](#_8uznas2p7rf8) [2](#_8uznas2p7rf8)

[System network diagram](#_wivt6pnzgtx8) [2](#_8uznas2p7rf8)

[Hosts](#_c0v2dlrnnh4) [3](#_c0v2dlrnnh4)

[Access List Rules](#_8mufas5wpdt4) [3](#_8mufas5wpdt4)

[Users](#_9i4cnxli1hav) [3](#_9i4cnxli1hav)

[System security configuration](#_gifs6icsvjbd) [4](#_gifs6icsvjbd) SSH configuration 4

Automatic Updates 4

Host firewall configuration 4

[Installed Packages](#_51py791jcxl1) 4

[Backup and disaster recovery](#_ur7b5ahs8d4o)  [4](#_x6nhz8q7m9lv)

[**Services**](#_r4gzl4k9qzi2)[**4**](#_r4gzl4k9qzi2)

Tip of the day service 4

Apache Web server 4

Start/Stop 4

Configuration 4

Logs 5

NFS 5

Start/Stop 5

Configuration 5

Logs 5

Let’s Encrypt & Certbot 6

Configuration 6

Test 7

Logs 7

CMDB **7**

[**Quality and operation requirements**](#_vn48b1f3gr0s) **9**

[Security](#_622x3vytnsz2) 9

# 

# 

# Introduction

This document contains the system operations documentation for the Cabba Services.

The environment has been built in the Server Technologies 2022 course by Anmol Arora.

It contains information required for operating the system and describes the network setup, hosts, services and users of the system.

## Document change log

| **Version** | **Date** | **Author** | **Description** |
| --- | --- | --- | --- |
| 1.0 | 15.3.2022 | Anmol Arora | Initial version. Server setup with public IP and default user. |
| 1.1 | 24.3.2022 | Anmol Arora | Set up SSH and deleted the default user, also made 6 new users, one with sudo access rest as guest users. |
| 2.1 | 18.04.2022 | Anmol Arora | Set up nfs server, http and https apache web server |
| 2.2 | 24.04.2022 | Anmol Arora | CMDB, disaster recovery added |
| 3.0 | 15.05.2022 | Anmol Arora | Added details for services: start/stop, configuration, testing, logs. Apply and add sub headings as needed |

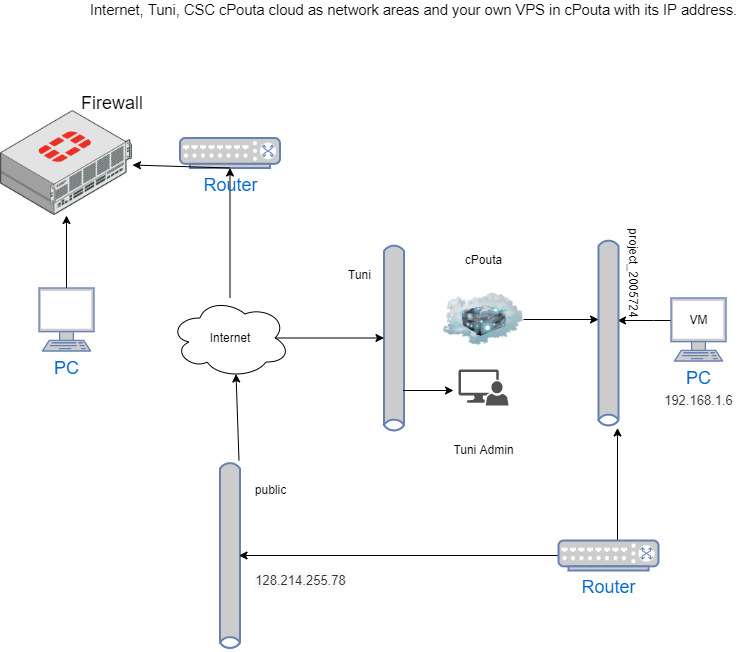
# System overview

## System components

The system resides in the CSC cPouta IaaS cloud service in a single cPouta project.

cPouta uses the OpenStack technology.

## System network diagram



## 

## 

## 

## 

## 

## Pouta Cloud

### Hosts

| **Name** | **IP** | **Description** |
| --- | --- | --- |
| my-test-env | 128.214.255.78 | My pouta environment |
| nfshost | 192.168.1.34 | My nfs server for TotD 2.0 |

# 

### Access List Rules

| **Enforcement** | **From** | **To** | **Ports** | **Description** |
| --- | --- | --- | --- | --- |
| Pouta(default) | Internal | Internal | \* | Internal traffic between servers allowed |
| Pouta(Monitoring) | centreon.eduhou.fi | my-test-env | SSH,HTTP,HTTPS | Course monitoring allowed |
| ufw(my-test-env) | External | my-test-env | ICMP,SSH,HTTP,HTTPS,NFS,Apache | Firewall for pouta main machine |
| ufw(nfshost) | Internal | Internal | SSH,Nfs | Firewall nfs server |

### Users

| **User** | **Sudo** | **Description** | **Tuni Email** |
| --- | --- | --- | --- |
| cabba | Yes | Main user on the machine | anmol.arora@tuni.fi |
| sakip | No | Guest user, TOTD enabled | safiul.alam@tuni.fi |
| nikke | No | Guest user, TOTD enabled | nikke.karaksela@tuni.fi |
| elina | No | Guest user, TOTD enabled | elina.widdowson@tuni.fi |
| sam22 | No | Instructor, TOTD disabled | petteri.jekunen@tuni.fi |
| joe22 | No | Instructor, TOTD enabled | petteri.jekunen@tuni.fi |
| nfs | Yes | Sudo user on nfs server | anmol.arora@tuni.fi |
|  |  |  |  |

### System security configuration

#### SSH configuration

SSH is open on port 22 and is only accessible by users which have been added by the root user.

Login via username-password is disabled and only possible via ssh key authentication.

#### Automatic Updates

Automatic updates have been enabled, security updates will be done automatically and can also reboot the system if there is a kernel update.

Guide followed -> <https://www.cyberciti.biz/faq/how-to-set-up-automatic-updates-for-ubuntu-linux-18-04/>

However there will be no email generation as email service has not been setup yet.

#### Host firewall configuration

The main-test-env firewall has been enabled and is set to disallow all inbound connections unless they are on services which are exposed to the internet(web server, nfs server)

To allow a connection go to the security group section in pouta environment and add the port and ip specifications.

## Installed packages

*For example:*

| Host | Packages | Description |
| --- | --- | --- |
| my-test-env | nfs-common | NFS client |
| nfshost | nfs-kernel-server | NFS server |
| ALL | git | Code, version tracking |
| my-test-env | apache2 | Web server |
| my-test-env | certbot | Renews HTTPS certificate |
| my-test-env | nmap | Port scanning |
| my-test-env | tree | Cmdb repo |

### Backup and disaster recovery

In case of any incident backup can be done through backup images maintained in the pouta environment.

Load a snapshot of the backup and another instance of your server will be up and running in a few minutes.

# Services

1. SSH Login using keys  
   Although SSH port is open for all ip addresses, login is only possible by ssh-keys.
2. Automatic Updates  
   Installs unattended updates and security upgrades

Automatically reboots system if there is kernel update

1. **Tip of the Day**  
   Prompts a new linux tip on every ssh login, can be disabled by users by changing the .TOTD file contents.   
   Since it's a global service the command runs from the /etc/profile file and is only read on new global logins. Can be made to work for internal new terminal spawns.

#### TotD - local file based (or NFS based)

The tips are both present locally and on the NFS server, the directory for those are

Locally - /opt/totd/TipOfTheDay/Tips

NFS - /nfs/home/Tips

#### TotD - HTTP static

For the HTTP/S static webserver Totd the files are in local folder but are pointed to using symbolic links

cabba@my-test-env:/var/www/tips.cabba.ilab.fi$ ls -l

total 4

lrwxrwxrwx 1 root root 26 Apr 18 20:11 Tips -> /opt/totd/TipOfTheDay/Tips

lrwxrwxrwx 1 root root 26 Apr 12 15:21 files -> /opt/totd/TipOfTheDay/Tips

-rw-r--r-- 1 root root 17 Apr 11 12:49 index.html

lrwxrwxrwx 1 root root 26 Apr 12 15:20 txt -> /opt/totd/TipOfTheDay/Tips

1. **NFS server**  
   Instead of reading tips from directories on the main machine now there is a separate nfs server which mounts 2 drives to the main machine and the tips are read from there.

The tips are in the home directory of the nfs user /nfs/home/Tips

1. **Apache2 server**  
   Configured to work on both http(redirect to https) and https, the webserver also reads the tips and can present them over the web browser or curl.

Files are in the /var/www/tips.cabba.ilab.fi folder and the configuration files are in /etc/apache2/ folder

1. **Lets Encrypt & Certbot**

HTTPS self signed certificates are enabled through certbot which renews them after 364 days of issuing.

To check status issue the command - sudo systemctl status certbot.timer

To dryrun renew command - sudo certbot renew –dryrun

1. **CMDB**

Git repo tracks all configuration files that are added by the server admin so that configurations are not lost/ can be transferred to new servers. Git repo link - https://gitlab.tamk.cloud/servertech/servertechnologies-cmdb-5g00dl95-3003

# Quality and operation requirements

## Security

1. SSH is done using keys and not username-password combination because brute forcing ssh is always an option that hackers might take.
2. Automatic updates have been enabled for the entire system.
3. HTTP redirects to HTTPs
4. NFS server is accessible only internally in the pouta network
5. Certbot enables SSL for HTTPS certificates and renews them
6. UFW firewall allows ranges of IP instead of any IP

Pouta Link for best practices - <https://docs.csc.fi/cloud/pouta/security/?pk_vid=2e24cc96607a302716161371410e04d7#enable-automatic-updates>

* No Mail Servers

We hate spam as much as you do. Unfortunately, it is very easy to configure a mail server so that it can be used by spammers. So, please instead use an existing SMTP server outside the cloud (see section 6.1).

* Upgrade your kernel

Some updates, such as kernel upgrades, require rebooting the virtual machines. Please schedule this into your regular maintenance.

* Subscribe to security announcements for your OS

If there is a security problem in your operating system, you need to find it out as soon as possible. Find the appropriate mailing list and keep an eye out for anything that requires urgent action.

* Run a restrictive firewall

Your instances should be configured so that they allow the minimum access required to run the service. Please use a host-based firewall, in conjunction with the cloud-provided firewall to manage access.

* Disable/remove unneeded accounts

Keep an eye on the user accounts enabled in your system. Some applications create default accounts which are insecure. An ideal scenario might be three accounts: root (with ssh disabled), a user account for a sysadmin (key login only) and a user-level account for a service (login disabled).

* Disable password login – use keys

Passwords can be, with enough time and compute power, attacked with brute force. The average SSH server deals with thousands of such attacks every week, so use keys to have one less worry.

* Do not store keys on the image

The cloud provides a metadata service so that you can download keys on boot. This is recommended. It ensures that if your key is compromised, not all running instances of that image are compromised.

* Use tools like denyhosts

Tools such as denyhosts, which look at log files for attempted breaches and then firewall out IP addresses, can take your security approach to a more active level.

* Disable unneeded services

Know what services run on your image and disable the unnecessary ones before you upload it. This reduces the attack surface.

* Use encrypted communications

Wherever possible, use encrypted communications to avoid attacks which intercept data.

* Use the best practices for logging

Make sure that the services are logging to a secure location, that is as tamper-proof as possible. Keep the logs for a reasonably long. Consider logging to a remote server as well.