k21 final documentation

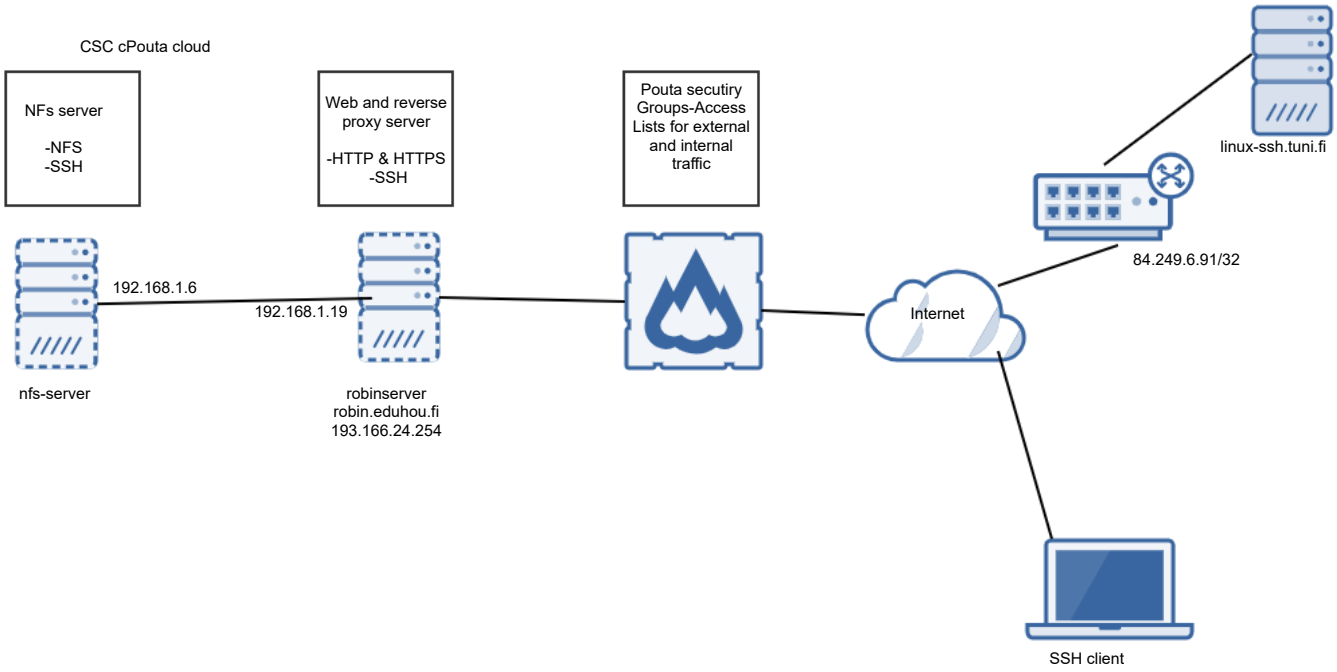
Created by Md Touhidul Islam, last modified just a moment ago

Introduction

This document contains system configuration information for the Server Technologies 2021 course Pouta Cloud server environment setup.

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

System Network diagram



- Introduction
- System Network diagram
- Access list rules
  - Pouta Security Group Configuration
- Users
- System Configuration
- Services
  - Apache
    - Update, backup, dr
    - Testing and diagnostics
  - SSH (all servers)
    - Start and stop
    - Configuration
    - Update - standard OS update
  - Certbot
  - NFS server
    - Start and stop
    - Configuration
    - Misc
    - Prerequisites
    - Deployment
    - The service is a node.js service. Source code recides in the git repository:
    - Start and stop
    - Configuration / location
- Quality and Operations Requirements
  - Security
    - SSH Access
    - Other security concerns
  - Automatic upGo to linkdate
- Backups and disaster recovery
  - Snapshots

Hosts

Host	Public IP and DNS name	Local IP	Description
adaserver	193.166.24.254 robin.eduhou.fi	192.168.1.6	Admin remote connection with SSH Web server for static content Reverse proxy for web services
nfsserver	n/a	192.168.1.19	NFS server for internal network

Access list rules

Pouta Security Group Configuration

Source	Destination	PORT	Description
193.166.164.0/24	195.148.23.213	22 (SSH)	Admin remote SSH connection from Tuni Linux server
84.249.6.91/32	193.166.24.254	22 (SSH)	Admin remote SSH connection from Tuni Network
ALL	193.166.24.254	80 (HTTP)443 (HTTPS)	HTTP-based services access allowed for any client ip.
192.168.1.0/24	192.168.1.0/24	2049 (NFS)	Internal NFS file sharing traffic allowed
192.168.1.6/24	192.168.1.6/24	22 (SSH)	Internal SSH allowed

Users

Username	Host	SUDO	Description
mdti	robin nfs-server	✅	client server
root	robin nfsserver	✅	DR use only. No SSH login enabled.
bob	adaserver	-	Account for the instructor of the course.

System Configuration

This server does not exist. In production environment there should be one repository for server configurations. (Mainly the configurations in /etc).

System configuration is maintained in the main configuration management database server cmdb.eduhou.fi.

Services

Apache

Start and stop

> systemctl start/stop apache2

Configuration

Sites configurations:

> /etc/apache2/sites-enabled

Main configuration:

> /etc/apach2/apache2.conf

Update, backup, dr

Apache is updated and backed up with the OS regular update procedure.

Testing and diagnostics

Smoke test. This responds:

> curl https://robin.eduhou.fi

The virtual servers:

> curl https://robin.eduhou.fi
> curl https://tips.robin.eduhou.fi
> curl https://www.robin.eduhou.fi

Accessing HTTP should redirect to HTTPS

> curl http://tips.robin.eduhou.fi → should redirect to https://tips.robin.eduhou.fi

SSH (all servers)

Start and stop

> systemctl status sshd

Configuration

/etc/ssh/

Update - standard OS update

Testing and diagnostics

.

Certbot

NFS server

Start and stop

> systemctl start nfs-kernel-server

Configuration

/etc/exports

```
/var/nfs/general       192.168.1.19(rw,sync,no_subtree_check) 192.168.1.6(ro,sync,no_subtree_check)
```

Misc

In case of issues, check:

- ufw - local fw allows NFS/2049
- /etc/exports - the IP address is correct and rw/ro correct
- Pouta fw - internal traffic allowed

Quality and Operations Requirements

Security

SSH Access

- SSH access has to be limited for key based authentication only.
- Allowing password based SSH is forbidden.
- SSH access with root username is forbidden.

Snippets from SSH configuration:

```
/etc/ssh/sshd_config:

...

#PubkeyAuthentication yes ← default value

...

#PermitRootLogin prohibit-password ← default value

...

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
```

SUDO privileges

Configuring SUDO access with NOPASSWD is forbidden. If this is needed, the commands must be specified explictly.
Users with SUDO privileges is limited for administrators and must be audited regularly.

Configuration:

```
/etc/sudoers and /etc/sudoers.d/*
```

Host firewall

Host firewall must be enabled and configured to allow only necessary ports. The firewall configuration should be audited regularly.

```
sudo ufw status
```

Automatic update

Automatic update has to be configured at minimum for security updates.

Backups and disaster recovery

For disaster recovery snapshot of the system is taken regularly.

Snapshots

snapshot	server	date	Description
nonstandardport	robinserver	05 May 2021	HTTPS configuration with Let's encrypt
robin	robinserver		Before encrypt
k21-servertechnology-secure configured	robinserver	5/10/21 12:57 AM	HTTPS configuration with Let's encrypt showing tips

No labels