# WorldSkills Germany Test Project

## *IT Network Systems Administration (39)*
## *Module A – Linux Environment*

Submitted by:

Kai Schell
Roman Steinhart

# Introduction to Test Project

## Contents

This Test Project proposal consists of the following documentations/files:

1. WSG2025_TP_39_Modlule_A.docx

## Introduction

The competition has a fixed start and finish time. You must decide how to best divide your time.

**Please carefully read the following instructions!**

When the competition time ends, please leave your station in a running state. The assessment will be done in the state as it is. No reboot will be initiated as well as powered off machines will not be powered on!

Please use the information in the appendix to access your virtual machines as well as the virtual machines themselves.

## System Configuration

All virtual machines are configured as follows:

- Region/timezone: Europe/Berlin
- Locale: English US (UTF-8)
- Key Map: German
- IP address: 10.0.0.x (see appendix)
- Operating System: Debian 12
- User: root
- Password: Passw0rd!

Every VM you see in the topology chart at the end of this document is preinstalled on the physical host, named accordingly. The hosts use Proxmox VE 8.4 as a virtualisation platform and you can connect to the resources using your browser.

Your credentials have been provided separately.

The preinstalled VMs contain only the base system and some basic packages, you can install any additional package you want.

The test project does not always give you an exact specification. In these situations, you have the chance to choose which software to use, which path to follow - you will find information at the tasks about the paths you can choose from. The more sophisticated a solution is the better mark you are going to get for it.

# Instructions to the Competitor

You have three hours to complete the task.

All work steps / your entire procedure are to be roughly documented by you in a file documentation.txt on the Desktop of your local workstation. The documentation can be made in bullet points and should contain the relevant steps, reasons for certain decisions, but also all possibly occurring problems and other conspicuities.

Read all tasks thoroughly before starting your work.

**See every bullet point as a separate task. If you're unable to solve one sub-task, you can still complete the other tasks and gain points for them.**

### Defaults

If not specified otherwise, use the password Passw0rd! for all users and services.

## Internet Access

### Package installation

Your virtual machines are able to access online apt repositories. You can use the apt command to install any additional packages you need. Connectivity to the internet is provided via the router VM, which has been preconfigured to accordingly. The router VM is not part of the competition and should not be modified, but you can login and check its configuration if you need to.

### Personal internet access

You are not allowed to access the internet on your local workstation.

# Description of project and tasks

## Situation

You work at the company Floss-IT. The company is a service provider for open source computer systems. For a product demonstration, you're supposed to set up a basic computer network for a small company.

## Tasks

### 3.1 General tasks

*These tasks apply to all VMs.*

- Configure networking as outlined in the appendix.
- Configure the hostname as outlined in the appendix.
- Administrative user
  - Create a user called admin (User is already created on the client)
  - The user should have sudo privileges
  - The user should be able to log in via SSH
  - The public SSH key of the user admin on the client should be copied to all VMs, enabling passwordless SSH login.

#### SSHd

*These tasks apply to all VMs except the client.*

- Disable root login entirely
- Disable password login entirely

### Client

#### SSH key

- Create an SSH key pair for the user admin
- The public key should be copied to the administrative user on all VMs
- The keypair should be of type ecdsa

#### SSH config

- Ensure admin can SSH into on to the web server by typing ssh webserver without specifying the IP address and/or port

### Storage server

#### Data volume

- Create a mirrored volume spanning the two empty disks
- Use a technique of your choice: LVM, mdadm
- The volume should be mounted at /mnt/data
- Ensure that the volume is available after a reboot

#### Fileshare

- Create a directory for an NFS share under /srv/nfs/intranet in /etc/exports
- The share should only be accessible by the web server
- Create a dummy file called intranet.data in the share

**Backup**

- Create a simple backup script to backup the content of /var/log of the web server
- It should be located at /usr/local/bin/logs-backup.sh
- It should be executed every day at 2:00 AM
- The script should log to the system journal
- The backup should be stored in a tar archive
- The backup should be compressed with bzip2
- The backup should named in the form backup_fileshare_YYYYMMDD.tar.bz2, where YYYYMMDD is the timestamp when the backup was created
- The backup should be encrypted with gpg so that only the user admin on the client can decrypt it
- The backup should be placed in /backup on the web server

## Web server

**SSHd**

- Should listen exclusively on the primary IP
- Should listen exclusively on Port 2222

**Web server**

- Should listen exclusively on the secondary IP
- Default website:
  - Install a webserver of your choice: nginx, apache, lighttpd etc.
  - The webserver should be accessible in a browser by calling http://<IP>/ from the client
  - The webserver should serve an index.html page with the content "Hello World"
- Intranet website:
  - The site should be accessible in a browser by calling http://<IP>/intranet from the client
  - Mount the NFS share /srv/nfs/intranet on the webserver
  - The root of the intranet website should be the mounted NFS share
  - Enable directory listing so that the content of the directory of the NFS share is visible

**Firewall**

- Allow incoming connections to the webserver on the secondary IP
- All other incoming connections on the secondary IP should be blocked
- Incoming connections on the primary IP should not be blocked
- You don't need to configure any other firewall rule for any other server or service

## DHCP server

- Install a DHCP server of your choice: isc-dhcp-server, dnsmasq, kea-dhcp etc.
- The DHCP pool ranges from 10.0.0.200 to 10.0.0.250
- Configure static IP assignment for the client as per the appendix
- 10.0.0.1 should be provided as the default gateway

## Appendix

### Hostnames and IP addresses

| VM | hostname | IP (Current State) | IP (Target State) |
|---|---|---|---|
| router | router | 10.0.0.1 | 10.0.0.1 |
| web | web | 10.0.0.2 | 10.0.0.2 (primary),<br>10.0.0.102 (secondary) |
| storage | storage | 10.0.0.3 | 10.0.0.3 |
| dhcp | dhcp | 10.0.0.4 | 10.0.0.4 |
| client | client | 10.0.0.5 | 10.0.0.105 (via dhcp) |

### Topology