EuroSkills Test Project

ICT Specialists (39)
Module A – Linux Environment

Submitted by:
Janos Csoke HU
Ander Guerra Larrea ES
Mikko Hiltunen FI
Martin Dagarin SI
Bart Jaminon NL

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 below for all the servers and clients.

LOGIN

Username:	`root`	`localadmin`
Password:	`Passw0rd!`	`Passw0rd!`

Use the string `Passw0rd!` as password everywhere where a password, passphrase etc is needed. **Pay attention to the zero sign in the string that replaces the capital O!**

SYSTEM CONFIGURATION

Region/timezone:	Europe/Warsaw
Locale:	English US (UTF-8)
Key Map:	English US

RESOURCES

You will find the topology and the listing of used IP addresses at the end of this document. The list of the users to be created can be found there too.

PREINSTALLED RESOURCES

Every system in this task uses **Debian 11**. 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 VMware ESXi as a virtualisation platform and you can connect to the resources using your laptops with vSphere Web Client or VMware Workstation also.

You can connect to the ESXi host with esxi.local URL.

The preinstalled VMs contain only the base system and few additional packages (see in the software section), you can install additional software using virtual optical disks.

SOFTWARE

For testing purpose, all VM has been installed with the following test tools: **smbclient, curl, lynx, dnsutils, ldap-utils, ftp, lftp, wget, ssh, nfs-common, rsync, telnet, traceroute, tcptraceroute, tcpdump, net-tools, cifs-utils.**

You can find a Debian install ISOs in the datastore.

INDRUSTY COMPLIANCE

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.

DESCRIPTION OF PROJECT AND TASKS

You are a new IT Engineer of the Firma Tradycyjna Polska Sp. z o.o. company. The goal of your next project is to build the whole IT infrastructure of the company.

General Configuration

Set up all the resources with the following:

- hostname,
- network configuration,
- time zone,
- keyboard layout,
- install SSH server and allow root password access (for the easiest testing).

Corporate HQ

This is the company's headquarters site with limited server services and clients.

fw-hq

This is the edge router and firewall of the HQ site. For this reason, it should allow devices to reach each other between network segments and the Internet.

You must configure the services of this server according to the following requirements.

1. **Create a root certificate authority**. Use the next parameters:

   C=PL, O=Firma Tradycyjna Polska Sp. z o.o., CN=Firma Tradycyjna Polska Sp. z o.o. Root CA

   Place all related files in the /ca folder. Use CA.crt for the name of CA certificate file. Issued certificates should contain (only and exactly) the following fields:

   C=PL, O=Firma Tradycyjna Polska Sp. z o.o., CN=<FQDN>

   Make sure all servers and the client applications used accept the certs issued by this CA.
2. **Make sure, the public services (DNS, mail, web) of the HQ site can accessible from the internet.** Configure firewall with iptables. Incoming packets should be dropped by default. Allow minimal traffic for the services to work. Allow SSH traffic from everywhere. Make sure, that iptables persist across reboots.
3. **Ensure secure channel between the HQ and the datacentre sites.** If this cannel broke, the clients of the HQ site can access the public services of the datacentre.
4. **Configure a remote access VPN service for a remote workers.** Make sure, VPN clients can access to the same resources as the clients of the HQ site.

hq-intra

1. **Deploy a directory service** with LDAP protocol. Create all objects listed in Appendix B.
2. **Create a failover DHCP cluster with hq-noc for the client network of HQ site.** HQ client subnet uses DDNS so make sure that all A and PTR records are dynamically updated.

hq-noc

1. Add 4 new 2GB HDD to a machine. **Configure software-based RAID 5** array and mount this to /share path.

2. **Configure CIFS service** for the profile directory of the corporate users. Use the /share/users/<username> as the path of the profile directories.
3. **Create a failover DHCP cluster with hq-intra**. See details there.

4. **Create monitoring service with Cacti.** Monitor the CPU, memory and disk usage of all servers on the HQ site with SNMP. Send email alert to the admin@firmatpolska.pl if the memory usage of any server more then 80%.
5. **Configure syslog server** to collect logfiles from the servers of the HQ site.

   (a) Logs coming from hq-intra related to DHCP should be written to /log/dhcp.log
   (b) Logs coming from dmz-host related to e-mail should be written to /log/mail.log
   (c) All other incoming logs from the HQ site should be written to /log/dump.log

dmz-host

1. **Deploy a DNS server of the firmatpolska.pl domain.** Serves the reverse records of the HQ networks also.
   This server needs to reply to DNS requests from the other sites and from the Internet also, but not allow to serve a private IPs outside of HQ site. Create entries for all servers (both sites) and services.
2. **Configure DDNS for HQ client network.**
3. **Install and configure web service.** Serve the https://internal.firmatpolska.pl . Use client certificate authentication. Only the users with a valid certificate signed by the company's CA can access to this site.
4. **Configure e-mail service** to send and receive email for the firmatpolska.pl domain. Users access their mailboxes using TLS-secured IMAP (port 143) and send emails using STARTTLS-secured SMTP (port 587). No unencrypted traffic from mailer clients are allowed. Both services require authentication. Port 25 is only used to accept mails from other SMTP servers (both encrypted and unencrypted).

hq-clt01

1. Install a **graphic environment** of your choice.
2. **Configure LDAP authentication** using the LDAP server and make the CIFS-shared home folder of the logged in user available.
   Prevent user to use local user account to login to the system except root and LDAP users.
   The LDAP users which is logged in previously to this machine, can log in also when the LDAP server is not available.
3. **Install Thunderbird** e-mail client to use with admin@firmatpolska.pl. Send an e-mail message to maja.

Software Defined Data Center

This is the datacentre of the company. You need to build the services of the datacentre (except services of fw-sddc and iaac-mgmt) using Ansible.

Use Ansible to configure bck-srv[01-n] and frt-web[01-n] servers from iaac-mgmt. There is a preconfigured hosts file located under /etc/ansible/hosts. Do not change this file. Before assessment all bck-srv[01-n] and frt-web[01-n] VMs will be reset to the original state. Your playbooks need to work with any $n >= 2$ integer number. You can find 6 VM for testing on the ESXi host.

All bck-srv and frt-web VMs preconfigured. Which means IP address, SSH service and SSH key authentication configured. You can connect with a user called 'ansible' from the iaac-mgmt to the destination VMs with a preinstalled private key.

The bck-srv VMs IP address last octet from 101 to 101+n. The frt-web VMs IP address last octet from 201 to 201+n in the fw-sddc front subnet and the last octet from 11 to 11+n in the backend subnet.

For marking, all playbooks will be run in order using the command "ansible-playbook playbookname.yml" in the /ansible directory.

You can connect the Debian ISOs 1-4 to the VMs.

1. **Create a directory /ansible.** All playbooks should be located at the root of this directory. All tasks should have state "ok" or "skipped" after running the playbooks a second time.
2. **Create a playbook called 1-hostname.yml** for configuring the hostname and timezone. All hosts should receive the hostname based on the "hostname" variable in /etc/ansible/hosts file
3. **Create a playbook called 2-firewall.yml for filtering incoming traffic on all VMs with nftables.** Incoming packets should be dropped by default. Allow minimal traffic for the services to work. Allow SSH traffic only from the iaac-mgmt. Make sure, that nftables persist across reboots.
4. **Create a playbook called 3a-backend.yml for configuring one or more web servers.** Install a web service on all hosts in the group "backend". Display the following content:
   „Linux - Because there is more than one way.
   This site was served by <hostname>"
5. **Create a playbook called 3b-backend.yml for configuring FTP server** that allows only one user called webmaster to log in. The ftp-home of this user is the web document root and the user is not allowed to leave his/her home folder. All uploaded files get the uid and gid of www-data. Use implicit SSL for the connection.
6. **Create a playbook called 4-frontend.yml for configuring two or more HA webservers.** Install HAProxy and VRRP services on all hosts in the group "frontend". Configure HAProxy to load balance "https://www.firmatpolska.pl" between all available web servers using round robin. Use certificate signed by the company's CA. The website need to available from internal and internet clients also.

fw-sddc

This is the edge router and firewall of the datacentre site. For this reason, it should allow devices to reach the services of the datacentre form the HQ site and from the Internet also.

1. **Ensure secure channel between the HQ and the datacentre sites.** If this cannel broke, the clients of the HQ site can access the public services of the datacentre.
2. **Configure firewall with nftables**. Incoming packets should be dropped by default. Allow minimal traffic for the services to work. Allow SSH traffic from everywhere. Make sure, that nftables persist across reboots.

Remote Worker

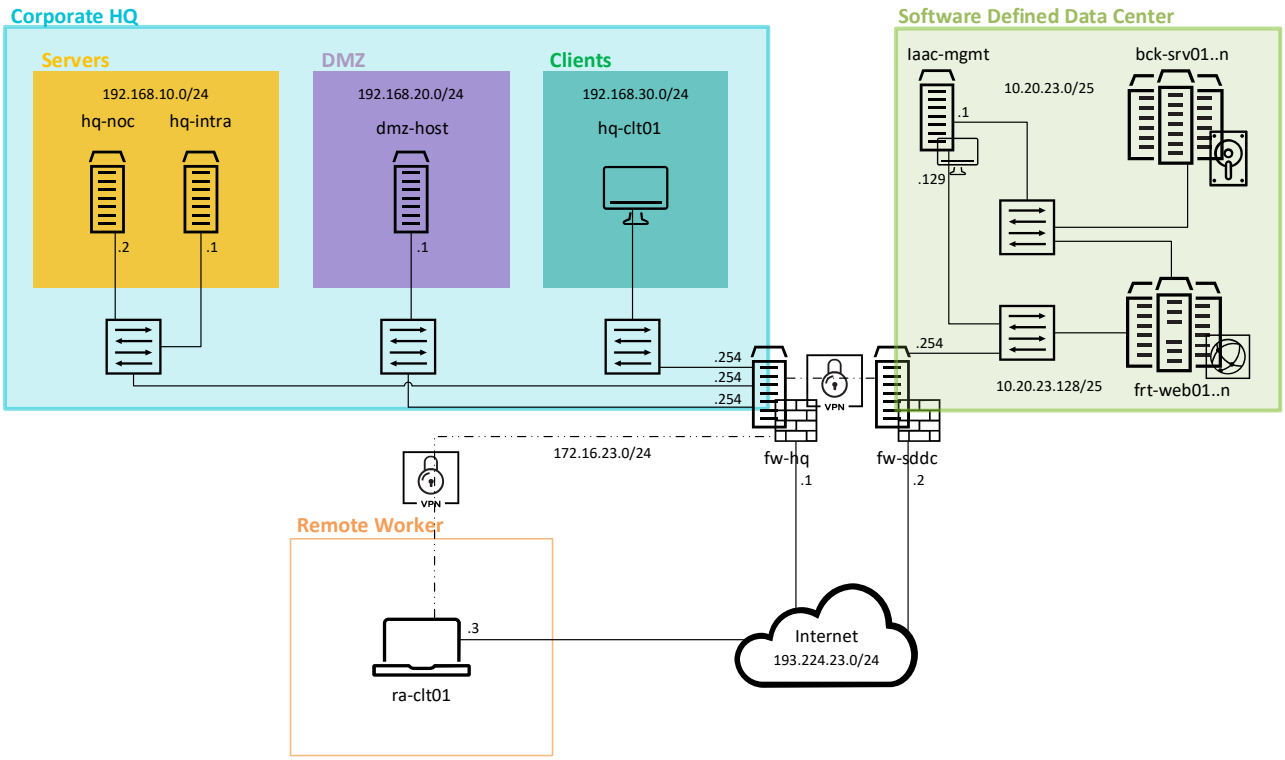
ra-clt01

1. Install a **graphic environment** of your choice.
2. **Configure a Remote Access VPN connection to fw-hq.** VPN connection builds up automatically when starting this computer.
3. **Configure LDAP authentication** using the LDAP server and make the CIFS-shared home folder of the logged in user available. Prevent users using local user accounts to log in to the system except root and LDAP users.

The LDAP users which is logged in previously to this machine, can log in also when the LDAP server is not available.

4. **Install Thunderbird** e-mail client to use with maja@firmatpolska.pl. Send email to admin.

Appendix A: Topology



Appendix D: Containers, Objects and Users

LDAP OUs

OU name
Network Admins
Management

LDAP Groups

Groups	DN
admins	CN=admins,OU=Network Admins,DC= firmatpolska,DC=pl
superusers	CN=superusers,OU=Network Admins,DC=firmatpolska,DC=pl
management	CN=management,OU=Management,DC=firmatpolska,DC=pl

LDAP Users

Username	E-mail Address	Home Directory Location on hq-noc	OU Membership	Group Membership
admin	admin@firmatpolska.pl	/share/users/admin	Network Admins	admins
maja	maja@firmatpolska.pl	/share/users/maja	Management	management
jan	jan@firmatpolska.pl	/share/users/jan	Network Admins	superusers