worldskills

Test Project

IT Network Systems Administration
Module A – Linux Environment

Submitted by:
Andreas Strömgren SE
Janos Csoke HU
Wanderlyn Cetauro Raposo Junior BR
Danny Meier CH
Jun Tian CN
Mario González Vásquez CR
Erko Pärna EE
Ander Guerra Larrea ES
Kevin Large UK

Contents

Introduction to Test Project

The following is a list of sections or information that must be included in all Test Project proposals that are submitted to WorldSkills.

- Contents including list of all documents, drawings and photographs that make up the Test Project
- Introduction/overview
- Short description of project and tasks
- Instructions to the Competitor
- Equipment, machinery, installations and materials required to complete the Test Project
- Marking scheme (incl. assessment criteria)
- Other

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 / skill39
Password:	Passw0rd$

System Configuration

Region/timezone:	Russia/Moscow
Locale:	English US (UTF-8)
Key Map:	English US

When tasked with configuring SSL or TLS you can use a self-signed-certificate. Please take care to hide any warnings if instructed to do so.

Software

For testing purpose, all hosts have been installed with the following test tools: **smbclient, curl, lynx, dnsutils, ldap-utils, ftp, lftp, wget, ssh, nfs-common, rsync, telnet, traceroute, tcptraceroute**

You can find a phpldapadm.iso in the datastore which is contains the Debian install package of PhpLDAPAdmin configuration tool.

Description of project and tasks

You're a freelancing IT-professional. Today you have been tasked with implementing a complex IT-environment based on Linux and open source software.

The network consists of an office network with a private cloud for the internal e-mail server and intranet. Remote access allows the employees to work remotely. A public cloud is used for the company's public website. You're also tasked with configuring services provided by the ISP "Fast-Provider".

General configuration

Servers and clients

Fully Qualified Domain Name	IP Address	Services
fw.skill39.net	192.168.1.1 192.168.2.1 200.220.55.1	Firewall, VPN, DHCP
client1.skill39.net	DHCP	---
file.skill39.net	DHCP (192.168.1.2)	SAMBA, NFS, LDAP, DNS
private.skill39.net	192.168.2.2	MAIL, WEB, MONITORING
public.worldskills.org	10.10.10.1	FTP, WEB
fw.worldskills.org	10.10.10.30 200.220.55.2	FIREWALL, VPN
srvpv01.fast-provider.net	200.220.55.3	MAIL, DNS
srvpv02.fast-provider.net	200.220.55.4	BACKUP, DNS
janes-pc.fast-provider.net	200.220.55.5	----

Networks

network	CIDR	domain
OFFICE	192.168.1.0/24	skill39.net
PRIVATE CLOUD	192.168.2.0/25	skill39.net
PUBLIC CLOUD	10.10.10.0/27	worldskills.org
SERVICE PROVIDER / INTERNET	200.220.55.0/28	fast-provider.net

Office Users

username	password	e-mail	home directory
adam	Passw0rd$	adam@skill39.net	/data/home/adam
jane	Passw0rd$	jane@worldskills.org	/data/home/jane

Office Network

The office network is used for office work tasks and consists of a server and clients. Your task is to install and configure services to make it easy for the office workers to collaborate. You're also tasked with configuring a firewall and the connection to the upstream ISP.

Please refer to the "NETWORKS"-table for information about the subnets used.

fw.skill39.net

This is the firewall for the **office network**. It's shared with the **private cloud network**.

Openvpn

Configure site-to-site VPN to fw.worldskills.org using a **tun** device all traffic between the **office network** and the **public cloud network** should be routed through the tunnel. Use **UDP** to minimize overhead in the tunnel.

Configure client VPN for **janes-pc**. When connected the user should have the same access to all resources as clients in the **office network**. This includes the **private cloud network** and **public cloud network**.

DHCP

Configure DHCP-service for the office network. Add all the necessary options to make all services work.

A and **PTR** records of the clients should be dynamically updated for DNS on **file.skill39.net**.

Make sure that file.skill39.net are always assigned the same address.

IPTABLES

All traffic through the firewall should be blocked by default.

Traffic originating from the **office network** is always allowed.

Traffic originating from the **office network** and **private cloud network** should be translated to the external IP-address when visiting the internet.

The **HTTPS** traffic sourced from OpenVPN client destinated to **public cloud network** should not go through the Site-to-site VPN. Other traffics sourced from OpenVPN client destinated to **public cloud network** should go through the Site-to-site VPN.

Add all necessary rules for the services to work as intended.

file.skill39.net

This is the local file and authentication server for the office network. Please install and configure the following services on the server.

LDAP

Install an LDAP-server using OpenLDAP. The LDAP server will be used for authentication for users to login to the local clients. Add all office users to the LDAP database.

RAID

Add three extra hard drives each 1GB in size. Configure a RAID 5 array **/dev/md0**.

LVM

Add **/dev/md0** as physical volume and make logical volume **/dev/file/data**. Create necessary volume group and mount the logical volume on **/data**.

SAMBA

Share the folder **/data/public-files** with **public.worldskills.org**. Make the access read-only and that no other hosts can access the folder.

NFS

Create a shared folder called **documents** that all authenticated users can access with both read and write permissions. Create and share a home directory for each of the office users in **/data/home**. The home directory should only be accessible by the respective users. You only need to create home directories to the users found in the table **office users** above.

All shared folders should be located within **/data**.

DNS

Configure DNS zone for skill39.net and add all necessary entries. Lookups to all other zones should be forwarded to srvpv01.fast-provider.net.

Configure reverse lookup zone for the **office network** and **private cloud network** subnets.

client1.skill39.net

Use **GNOME** as the desktop environment. Login as the user **adam**.

Users login in to the client (both command line and graphical interface) should be authenticated to the LDAP-server on **file39.skill39.net**. Prevent real local users (that are no service accounts) except root from logging in. Note that root is prevented from login in using the GUI per default, you are not to change this behavior.

The shared folder "documents" should be mounted for all office users in **/mnt/documents**. Each user should have access to their home share using NFS.

Configure the mail client **Thunderbird** for the user **adam** to send and receive mail. Make sure the certificate is trusted by the client. Note that you'll always get a warning for using a self-signed certificate.

It should be possible to send e-mails to users in the **worldskills.org** domain.

Home network

This network is used to simulate a remote worker.

janes-pc

Use **GNOME** as the desktop environment. Create a local user **jane** and login.

Create a script **/usr/local/bin/startup.sh** that is automatically run through **systemd** at startup. Name the service **loglastboot**. The script should touch **/last-boot**. We will test this by restarting the service.

Configure the mail client **Thunderbird** to allow Jane to send and receive emails. Make sure no certificate warnings are displayed.

It should be possible to send e-mails to users in the **skill39.net** domain.

Setup an **OpenVPN** connection to **fw.skill39.net**, that **jane** can open after logging into **GNOME**. Use the **GNOME network-manager**.

Private cloud

The private cloud is used to provide public services to the office users. For security purposes it's isolated in its own network segment.

Please refer to the "NETWORKS"-table for information about the subnets used.

private.skill39.net

This is the local mail and web server. It serves the office users under the domain skill39.net.

The office user **adam** should be able to login using SSH to the **root** account from **client1.skill39.net** using private-key authentication.

Email

Configure the server to send and receive emails for all the office users under the domain **skill39.net**. The users should be able to access their mailbox via IMAP. All communication between this server and the clients should be secured with TLS (STARTTLS).

It should be possible to send e-mails to users in the **worldskills.org** domain.

MYSQL

Install a MySQL database server. Use the root user with the password **Passw0rd$** to login.

Import the database **skill39** found in **/root/skill39-backup.sql** found on your host.

Web server

Install an Apache2 webserver and serve the site **intranet.skill39.net**. Use **/www/intranet** as the document root. The office users should be authenticated using the LDAP-server on **file.skill39.net**.

Backup

Backup **/important-data** to **srvpv02.fast-provider.net** using rsync. This should be done **every 10 minutes** (use the crontab of root). Create a script **/usr/local/bin/backup.sh** that can be used to run the backup manually.

Monitoring

To monitor the network setup Icinga2. The web-interface must be accessible on **port 8080** and listen for any hostname /ip. Use the username **icingaadmin** with the password **Passw0rd$**. Add the following checks:

- Monitor **fw.skill39.net** using ICMP.
- Monitor the status of the website **intranet.skill39.net**.

SSH

To make it possible to manage the website **intranet.skill39.net** add a user called **webmaster** with the password **Passw0rd$** and give it SSH access. The users home directory should be the same as the document-root of the website. The user should not be allowed to leave the home directory. The user should only be allowed to use the command **ping**.

Public cloud

The public cloud is used for production services.

Please refer to the "NETWORKS"-table for information about the subnets used.

fw.worldskills.org

Openvpn

Configure site-to-site VPN to fw.skill39.net - **office network**.

IPTABLES

All traffic through the firewall should be blocked by default.

Traffic to and from **public.worldskills.org** should be hidden behind the external IP-address.

Add all necessary rules for the services and tunnels to work as intended.

Reverse-Proxy

Install nginx and create HTTPS reverse-proxy for **public.worldskills.org** and **www.worldskills.org.** To external users the websites should only be accessible securely. Use a self-signed certificate and make sure that no certificate warnings are shown when browsing from **janes-pc** (user jane) using **Firefox** when not connected to the VPN.

public.worldskills.org

SAMBA

Mount **/data/public-files** on **file.skill39.net** to the local directory **/data/public-files.** Make sure the traffic is routed through the site-to-site tunnel.

Web server

Install an **Apache2** webserver and add two sites: **public.worldskills.org** and **www.worldskills.org**. Both sites must be HTTP only. The web-root directory for **www.worldskills.org** must be set to **/var/www**.

When visiting **public.worldskills.org** a directory listing of **/data/public-files** should be displayed.

As a basic security measure, make sure that no sensitive information is displayed in the HTTP headers and the footer.

FTP

Install an FTP-server using **proftpd** and add a user called **webmaster** with the password **Passw0rd$**. Make sure the root directory is the same directory as the web-root for **www.worldskills.org**. The user must not leave its home directory.

When uploading files, make sure the owner is set to **www-data** and group **www-data**.

All communication to the FTP server should be encrypted (Explicit SSL).

Use **Fail2Ban** to block a user after three (3) failed login attempts. The user should be blocked for 1 minute. The time limit will not be subject to marking.

Service provider

The service provider network represents the internet in this scenario.

srvpv01.fast-provider.net

Provides ISP-services.

DNS

Configure DNS zones for **worldskills.org** and **fast-provider.net**. Add all necessary entries. Requests for **skill39.net** should be forwarded to **file.skill39.net**.

Email

Configure the server to send and receive emails for **worldskills.org**. The users should be able to access their mailbox via IMAP. All communication between this server and the clients should be secured with TLS.

Add a user **jane@worldskills.org**.

It should be possible to send e-mails to users in the **skill39.net** domain.

When receiving a mail to **echo@worldskills.org** an auto-reply should be sent back to the sender.

srvpv02.fast-provider.net

This server is used only for remote backup.

DNS

Setup the DNS-server to be a secondary server for the zone **worldskills.org**. When adding entries to the primary server, they should automatically synchronize.

rsync backup

Install and configure rsync backup service. The server **private.skill39.net** should be configured to make scheduled backups (use the crontab of root) to the **/backup/private-skill39-net** folder. Perserve the directory structure.

Make sure that only the file owner can read the files in **/backup**.

As a basic security measure, make sure that only clients from the **private cloud** are allowed to synchronize. Unauthorized access should be logged to **/var/log/rsync/rsync-access.log**.

Appendix: Topology