EuroSkills Test Project

ICT Specialists (39)
Module A – Linux Environment

Submitted by:

Janos Csoke HU

Andreas Strömgren SE

Ander Guerra Larrea ES

Martin Dagarin SI

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/Vienna
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 10**. 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 the euroskills2020.ict 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 have been installed with the following test tools: **smbclient, curl, lynx, dnsutils, ldap-utils, ftp, lftp, wget, ssh, nfs-common, rsync, telnet, traceroute, tcptraceroute, tcpdump.**

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

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

Our company, the **Skills39 AG** is located in Graz, Austria. The company is mainly focusing on plant engineering and automobile crash tests. The company decided to migrate the on site compute resources to a private cloud a years ago. The migration of the automobile business line is almost complete, while the migration of the plant engineering has been postponed many times - the resources of this line can still be found in the basement of the company headquarters (HQ).

The resources of the company - both in the private cloud and the HQ basement are about to reach the end of life, and a decision has been made that new system will be built conserving the present migration state.

You, as the IT engineers of the local ISP are tasked to implement the server environment of the new system together with the clients needed to test the environment. Being the employees of the local ISP it is your task to configure every necessary resource on the ISP side too.

General Configuration

Set up on all the resources the following:

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

INTERNET

This site is simulating the internet with public server, public client which need to access the company's public services and a remote worker who connect to the company's network.

ispsrv

Install and configure

1. **a certificate authority**. This CA is a root CA:

   (a) C=AT
   (b) O=Globex ISP GmbH
   (c) CN=Globex ISP GmbH Root CA

   Place all related files in the /ca folder. Issued certificates should contain (only and exactly) the following fields:

   - C=AT
   - O=Globex ISP GmbH / Skills39 AG respectively
   - CN=<FQDN>

   Make sure all servers and the client applications used accept the certs issued by this CA.
2. the **rsync** share of the /backup path.
3. **web server** to serve www.globex-isp.com both on HTTP and HTTPS. Display a "Globex Official Website" placeholder message. Use a certificate issued by Globex ISP GmbH Root CA.
4. **DNS-server** to serve the zone of globex-isp.com with all the necessary entries. Lookups to skills39.com should be forwarded to the cloudfw.
5. **WebDAV service** to listen on www.globex-isp.com/webdav.

6. **e-mail service** to send and receive email for the globex-isp.com 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). Use a certificate issued by Globex ISP GmbH Root CA.
7. **SSH access** from pubclient using the username root. SSH access from any other host should be prohibited even when all firewalls are down.

remclient

Install and configure

1. a **Remote Access VPN** connection to cloudfw. VPN connection builds up automatically when starting this computer.
2. **LDAP authentication** using the LDAP server of Skills39 AG and make the NFS-shared home folder of the logged in user available.
   Mount the share "common" to /mnt/documents. Make sure that the logged in user can use this folder to save documents.
   Prevent real local users (i.e. the ones being no service accounts) except root from logging in. Note that root is prevented from login in using the GUI by default, you are not to change this behaviour.
3. a **graphic environment** of your choice.
4. **Thunderbird** e-mail client to use with inge@skills39.com when logging in with LDAP user inge. Install the CA-cert(s) in Thunderbird. Say "Hi!" in a mail to hans@globex-isp.com.
5. **Firefox internet browser**. Install the CA-cert(s) when logged in with inge.

pubclient

Install and configure

1. a **graphic environment** of your choice.
2. logon possibility to **local users**.
3. **Thunderbird** e-mail client to use with hans@globex-isp.com. Install the CA-cert(s) in Thunderbird. Say "Hallo Inge!" in a mail to inge@skills39.com.
4. **Firefox** internet browser. Install the CA-cert(s) when logged in with hans.
5. **ssh access** to hans. Ensure that hans can access dmzsrv1 with public key authentication and without using port forwarding anywhere in between.
6. **WebDAV access** to hans to the shared folder of the ISP using default the File Manager of the graphical environment installed. Make sure that hans can browse the share, and is able to modify and delete his files.

HQ

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

hqfw

Install and configure

1. **NFS file server** to host the home folder for all users in the company. All home folders are created on this server in the /data/home folder. Make sure that no user can access in any way the home folders of other users.
2. **DCHP server** for the client subnet of the HQ. HQ client subnet uses DDNS so make sure that all A and PTR records are dynamically updated.

3. **Backup.** Backup the contents of /data to /backup on ispsrv.globex-isp.com. Use the /usr/local/bin/backup.sh name for your script that runs in every minute making the backup.
4. **proxy** server for the client subnet. Clients on this subnet can open HTTP servers only using this proxy server, so make sure they cannot reach any web server directly. HTTPS servers can be reached directly.
   By default the clients needn't to be authenticated by the proxy. Requiring authentication is a better solution.
5. **firewall**, that allows all traffic between the HQ client network and the Private Cloud, even if the Site-to-Site VPN is down. When opening non-HTTP sites from the client network, internet servers should see all requests as if they were originating from the hqfw server. Make sure that all services of hqfw are available only from where they should be available. The hqfw itself is able to build connections to everywhere.
6. **Site-to-Site VPN** to cloudfw. All traffic between the Private Cloud and the HQ uses this connection. Try to use an authentication method considered to be more secure. If the VPN go down for a minute or two, HQ clients should still be able to browse the internet including the public website of Skills39 AG.

hqclient

Install and configure

1. **LDAP authentication** using the LDAP server of Skills39 AG and make the NFS-shared home folder of the logged in user available. Only users from the management OU and management group should be able to log in.
2. Mount **the share** "common" to /mnt/documents. Make sure that the logged in user can use this folder to save documents.
3. Prevent real local users (i.e. the ones being no service accounts) except root from logging in. Note that root is prevented from login in using the GUI by default, you are not to change this behaviour.
4. a **graphic environment** of your choice.
5. **Thunderbird** e-mail client to use with fritz@skills39.com when logging in with LDAP user fritz. Install the CA-cert(s) in Thunderbird. Say "Meeting time!" in a mail to inge@skills39.com.
6. **Firefox internet browser**. Install the CA-cert(s) when logged in with fritz.

Private Cloud

This is the newest part of the company's network. This site contains the internal servers which serve internal services only and DMZ servers which serve internal and public services also.

cloudfw

Install and configure

1. **Site-to-site VPN** to hqfw.
2. **Remote access VPN** to use with remclient. Some solutions tend to accept self-sign certifications too. Better solutions examine if the issuer can be trusted and/or both side of the VPN is validate the packages. Make sure that the user of this VPN connection can reach every resource in the company.
3. **syslog server** to collect logfiles from the DMZ.
   (a) logs coming from dmzsrv1 related to web access should be written to /log/dmz1-web.log
   (b) logs coming from dmzsrv2 related to FTP transfers should be written to /log/dmz2-ftp.log
   (c) all other incoming logs from DMZ subnet should be written to /log/dmz-dump.log

4. **Cacti monitoring service**, and monitor dmzsrv1 and dmzsrv2 servers memory usage via SNMP. Add the two relevant graphs to default tree and do not forget to publish the tree. The SNMP protocol is widely known for being insecure. Better solutions use newer versions and more secure encryption.
5. **firewall**, that allows all traffic between the HQ client network and the Private Cloud. Make sure that all services of cloudfw and the Skills39 AG network are available only from where they should be available. The cloudfw itself is able to build connections to everywhere. When opening internet connections from anywhere in the Skills39 AG network, internet servers should see all requests as if they were originating from the cloudfw server. Servers in the DMZ can initiate connections only in the DMZ and to the internet.

intsrv

Install and configure

1. **RAID6** with 4 hard drives 1 GB each and mount the device to /data.
2. an **LDAP server** capable to handle the authentication and authorization users need in the company. Create the container and the objects listed at the end of the document in the LDAP database.
3. **DNS server** for the zone skills39.local and create entries for all servers and services. Lookups to skills39.com should be forwarded to the DMZ servers, all other requests should be forwarded to the ISP server. Configure DDNS for HQ client network.
4. **CIFS server** to share /data/common as //intsrv.skills39.local/common The share is hidden and is only accessible from the HQ client subnet. No authentication required. Make sure that all the users can create, delete and modify files and can delete and modify files created by other users.
5. **NFS server** to share /data/www making it only accessible from the DMZ.
6. **an intermediate CA using the ISP CA as root CA**. The CA certificate contains the following fields:

   (a) C=AT
   (b) O=Skills39 AG
   (c) CN=Skills39 AG Intermediate CA

   Place all related files into /ca directory. Make sure that all intranet services use certificates signed by this CA. Certificates signed by this CA must be marked as trusted by all intranet servers and clients. Issued certificates should contain (only and exactly) the following fields:

   - C=AT
   - O=Skills39 AG
   - CN=<FQDN>

7. a **web server** to serve https://intranet.skills39.local. Use /data/intranet as the document root, and create a placeholder HTML-file displaying the server name. Visitors of this page should be authenticated using the LDAP-server on this server. Use a certificate signed by the intermediate CA. Redirect users trying to open any URL using HTTP to the HTTPS root.

dmzsrv1

Install and configure

1. **web server** to serve https://www.skills39.com (both IPv4 and IPv6) and https://ipv6.skills39.com (IPv6 only). Use the NFS share of intsrv as the document root. Use certificates issued by the ISP CA. This and the other web server on dmzsrv2 are the two parts of a fault tolerant web server solution. If any of the two servers go down, the web queries sent to www.skills39.com still need to get an answer.
2. **syslog service** sending the messages of /var/log/syslog and the webserver access log to the syslog server on cloudfw using UDP.

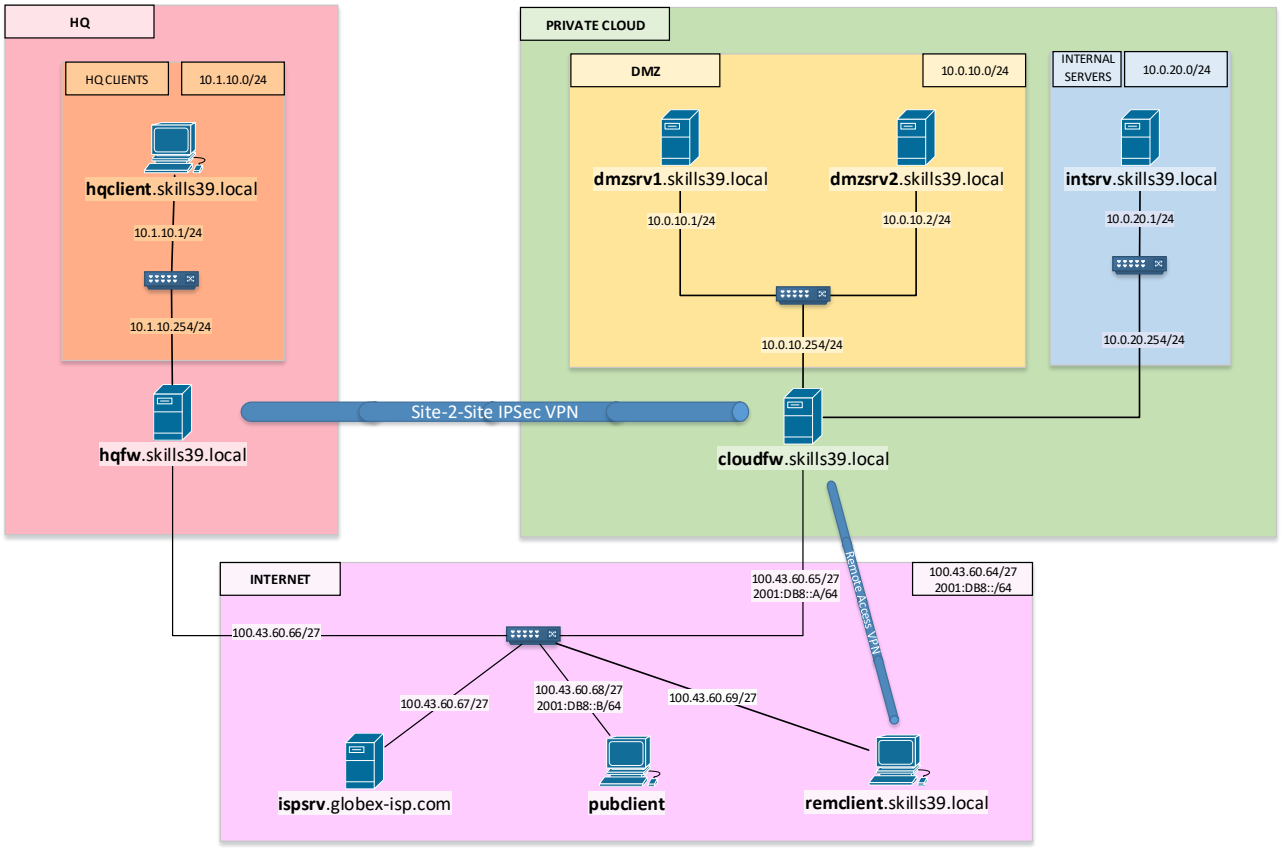
3. **e-mail service** to send and receive email for the skills39.com domain. Users access their mailboxes using TLS-secured IMAP (port 143) and send emails using STARTTLS-secured SMTP (port 587). No unencrypted traffic from mailer clients are allowed. Both services require authentication. Port 25 is only used to accept mails from other SMTP servers (both encrypted and unencrypted).
4. **DNS server** for the forward zone skills39.com and create necessary entries. Do not allow recursive queries. This and the other DNS server on dmzsrv2 are the two parts of a fault tolerant DNS solution that listens on the IP address of 10.0.10.100. If any of the two servers go down, the queries for zone skills39.com form the internet and from the corporate network still need to get an answer.

dmzsrv2

Install and configure

1. **web server** together with dmzsrv1 - see details there.
2. **DNS server** together with dmzsrv1 - see details there.
3. **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. Ensure that the server logs all file transfers and that these logs are sent over to the syslog server on cloudfw.

Appendix A: Topology



Appendix B: Network Settings

Servers and Clients

Fully Qualified Domain Name	IP Address
remclient.skills39.local	**100.43.60.69/27**
pubclient	**100.43.60.68/27** **2001:DB8::B/64**
ispsrv.globex-isp.com	**100.43.60.67/27**
cloudfw.skills39.local	**100.43.60.65/27** **2001:DB8::A/64**
	10.0.10.254/24
	10.0.20.254/24
dmzsrv1.skills39.local	**10.0.10.1/24**
dmzsrv2.skills39.local	**10.0.10.2/24**
intsrv.skills39.local	**10.0.20.1/24**
hqfw.skills39.local	**100.43.60.66/27**
	10.1.10.254/24
hqclient.skills39.local	**DHCP**

Networks

Network	CIDR	Domain
INTERNET	**100.43.60.64/27** **2001:DB8::/64**	globex-isp.com
DMZ	**2001:DB8:A:A::/64** **10.0.10.0/24**	skills39.local
INTERNAL SERVERS	**2001:DB8:A:B::/64** **10.0.20.0/24**	skills39.local
HQ CLIENTS	**10.1.10.0/24**	skills39.local

Appendix C: Containers, Objects and Users

LDAP OUs

OU name
management
sales

LDAP Groups

Groups	DN
management	CN=management,OU=management,DC=skills39,DC=local
sales	CN=sales,OU=sales,DC=skills39,DC=local
staff	CN=staff ,DC=skills39,DC=local

LDAP Users

Username	E-mail Address	Home Directory Location on hqfw	OU Membership	Group Membership
fritz	fritz@skills39.com	/data/home/fritz	management	management, staff
inge	inge@skills39.com	/data/home/inge	sales	sales, staff

Local users on ispsrv and pubclient

Username	E-mail Address
hans	hans@globex-isp.com
anna	anna@globex-isp.com