EuroSkills Test Project

ICT Specialists (39)
Module B – Microsoft Environment

Submitted by:

Christian Schöndorfer (AT)

Igor Bumanis (LV)

Timotej Gruden (SI)

Stefan Wachter (LI)

Almut Leykauff-Bothe (DE)

INTRODUCTION

You have been hired as an IT consultant by a Company called Skills39 located in Austria.

Your job is to bring up a Domain infrastructure with administration solutions and a remote access solution for the salespeople so that they can connect to the company's network.

Your client attaches importance to safety. Therefore, configure the topology required below and secure it according to best practice industry standards **.**

TEST PROJECT OVERVIEW

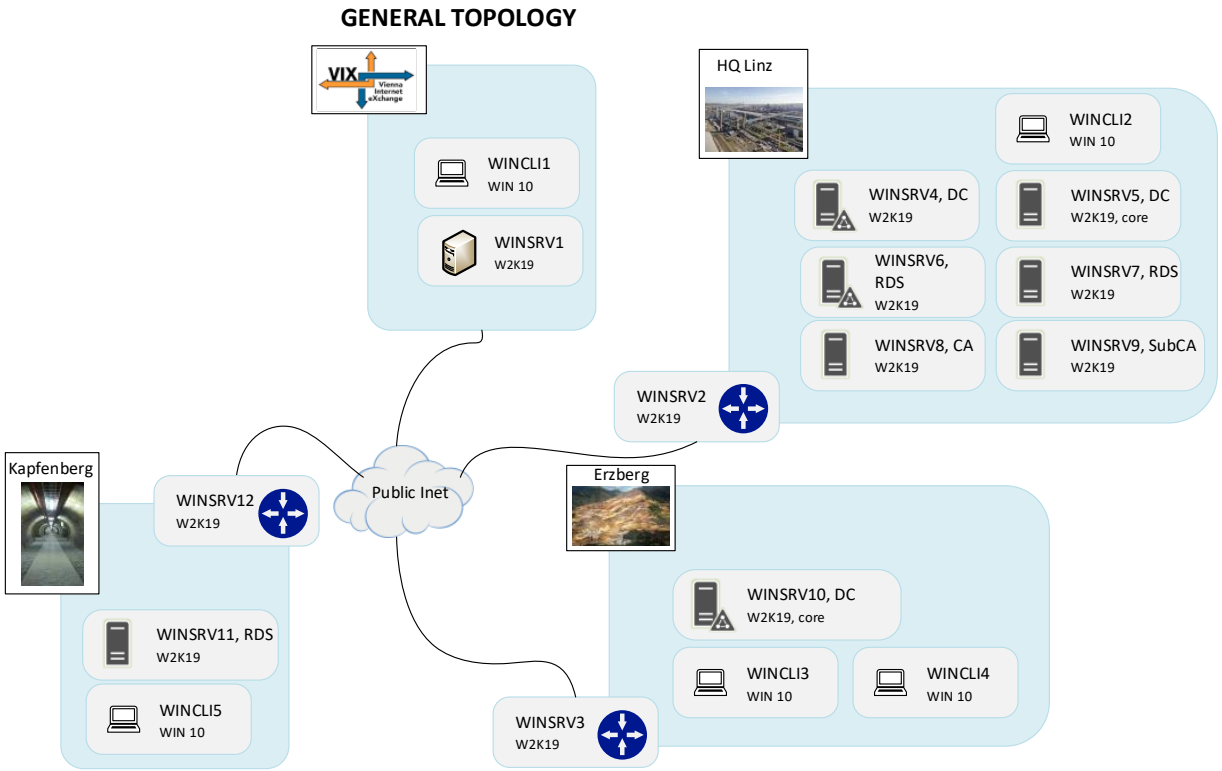
The headquarters are situated in Linz. Active Directory is primary implemented at this location. There is also an offline root CA, and RDS Services for Remote stuff.

Skills39 operates a location in Erzberg; here you can also find a DC, but it is RO.

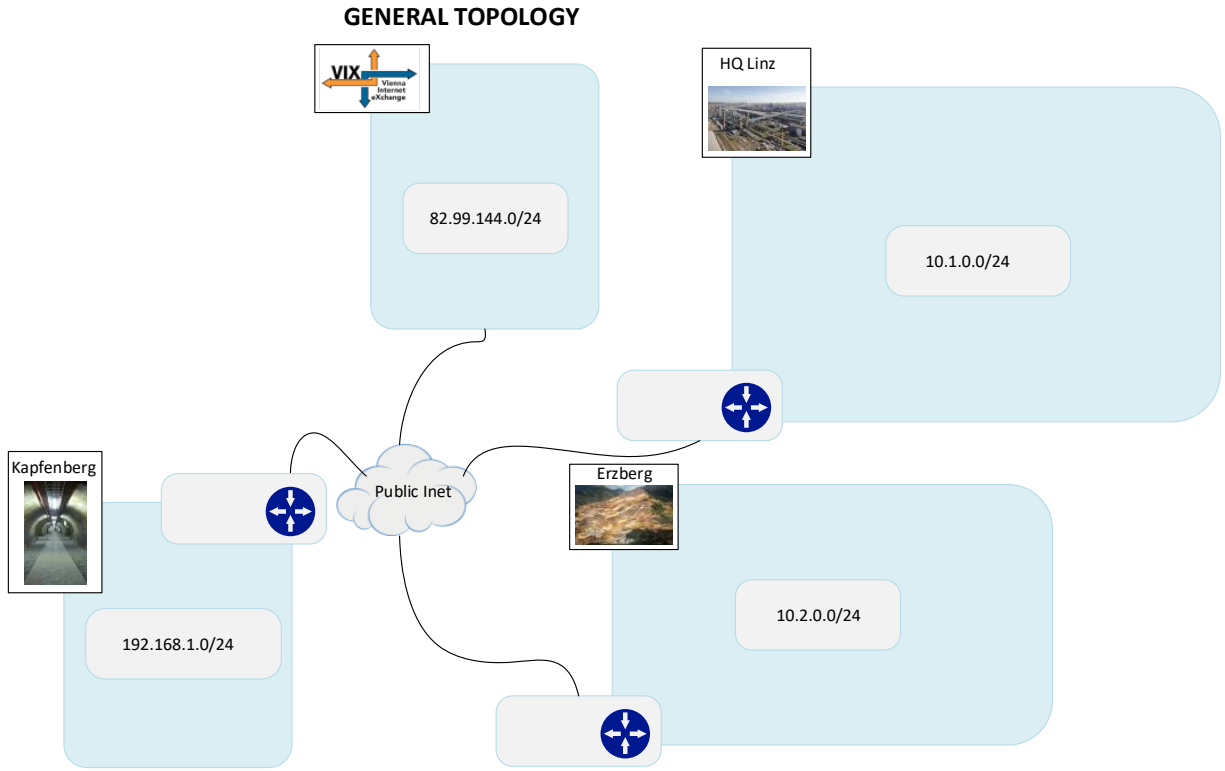
After all installations are complete, your team is in a protected data center in the bunker in Kapfenberg. In the end, the entire operational management of the AD should be carried out from here. The workstation used for daily administration should be secured in an industrial best practice way.

Internet-breakout is hosted by Vienna Internet Exchange; behind VIX, in another AS, we can find a "Road warrior", and also a "Web Server".

GENERAL TOPOLOGY



LOGICAL DIAGRAM



INSTRUCTIONS TO THE COMPETITOR

- Whenever you are required to configure a password, use password Passw0rd! (with zero between w & r) if otherwise is not stated.
- Your fist task is to bring up the needed Workstations and servers.
- Use localuser\Passw0rd! local credentials to access workstations and Laptop or administrator\Passw0rd! for Servers.
- Do not change the passwords.
- Except for IP, hostnames, User accounts, DNS records and this kind of details, the TP will not indicate every detail and technology to use. It will be up to you to come up with a solution which will meet the requirements.
- Most of the tests done to assess your work will be functional, it is your responsibility to make it work as expected.
- In a general way, do things clearly and cleanly in such a way not to give experts any doubt when assessing your work.
- Implement all tasks to the best of your ability, in line with industry best practices (in terms of security, high availability and scalability) within the limitations imposed by the equipment.
- Save your configurations frequently; accidents do and will happen.
- Make sure that all your configurations are still working after equipment reboot.
- At the end of this document, you will find the address table. Also, there are free places for comments and for the installed features and services from you. For easier assessment you must fill out these tables! (especially missing or assumed IP's and configured roles and services).
- Complete self-assessment questionnaire. Answers in this questionnaire will be used by experts as a time saver for judgment marking. If you mark a section as Not implemented (or no answer/details specified) configuration check

for this section will be skipped. If you mark a section as done (or any answer/details specified) experts will double check your configuration against your answer.

TEST PROJECT OBJECTIVES

BASIC INFRASTRUCTURE

1. Basically, Skill39 attaches great importance to security.
2. Name all Network interfaces with useful names.
3. Ensure, that active hours are configured between 08.00 – 14.00 – on all WIN Clients.
4. WINSRV1
   a. This server represents the “Internet”, its main purpose lies in the provisioning of a test environment.
   b. Note that this server is exposed to the Internet.
   c. Modify the default firewall rules to allow ICMP traffic only for known hosts in our skills topology; all hosts and clients must be able to reach this server.
   d. WINSRV1 provides DNS service for all public machines in our skills environment.
   e. Add an additional virtual hard drive (10GB) as D: drive
   f. WINSRV1 is the primary time server for all Windows devices.
   g. The FQDN of the server is www.skill39.at.
5. **WINCLI1**
   a. This client represents the “Road warrior”.
   b. Note that this client is also exposed to the Internet.
   c. This client should be able to access Files on “his” DFS Folder via secured web access gateway.
6. **WINSRV2, WINSRV3 & WINSRV12**
   a. These three servers represent the “Gateways”, their main purpose is provisioning of internet access.
   b. Note that these servers are exposed to the Internet.
   c. Modify the default Firewall rules to allow ICMP traffic only for the respective WINSRV (so only between WINSRV2, WINSRV3 and WINSRV12).
   d. Provide necessary configuration steps to allow the needed communications.
7. **WINSRV4 & WINSRV5**
   a. These two servers represent ADDS servers.
      i. Create a forest named “intra.skill39.at”.
      ii. WINSRV4 and WINSRV5 are both DC’s.
   b. Create a DFS
      i. Domain-Based Namespace is “Skill39-space”
      ii. Location: %Systemdrive%\Skills-Data\Skills39-space.
      iii. Only Skill39\Administrator has full permissions.
      iv. Domain-users have read-only rights.
      v. User called “Roadw_Skill39” from “Road warrior” has full permissions on his Data-folder called “Roadw_Data”.

c. Provision IPAM-Services for DNS and DHCP
    i. IPAM-Server is WINSRV4
    ii. Account is Skill39\Administrator
    iii. Provide IPAM Service by GPO (named “Skill39-IPAM”).
    iv. Configure DHCP for the local clients in HQ Linz.
    v. DHCP Mode: Load balancer with Partner Server: WINSRV4/5.
    vi. DHCP State Switchover: 10 minutes.
    vii. Range 10.1.0.100-10.1.0.200.
    viii. Configure DNS for intra.skills39.at and the necessary DNS delegations at the upstream DNS.
    ix. Create the necessary zones.
    x. Add records for all servers at the company.
    xi. Set the appropriate options for both DNS servers and default gateway.

8. WINSRV 10

a. This server is a RO-DC in intra.skill39.at.
b. Connectivity between WINSRV10 and HQ Linz should be implemented in a proper way.

9. WINCLI3 & WINCLI5

a. Basic configuration for Windows10 Clients.

Active Directory – Deep dive

1. Implement the following GPO’s:

a. Disable “first sign in Animation” on all Clients.
b. Members of the “IT-Staff” group must be members of the local admin group on all computers in the domain.
c. Make www.skill39.at the default website in Edge browser; therefore create a simple website (content and style of website would not be marked!).
d. Disable Recycle Bin on the desktop for all users.
e. Computer Certificates should be registered by auto-enrolment.
f. Digitally encrypt domain traffic.

2. Shared folder for userprofiles

a. Create a multipurpose replication folder.
b. Name of the replication-group: “Skill39-Profiles”.
c. Replication group is provided by all DC’s in skill39.at.
d. Primary member is WINSRV1.intra.skill39.at.

3. Users and Groups

a. Create OUs named “Management”, “IT-Experts”, “Controlling”, “Staff”.
b. Create the users from the attached XLS; fill up missing information and add the users to the corresponding groups and OUs.
c. Every user should have a home drive on the “Skill39-Profiles” folder.
d. The home drive should be connected automatically as drive X.

4. REMOTE Desktop SERVICES

a. The “Road warrior” WINCLI10 should be able to access his workload on the DFS-Folder via RDS.
b. Implement a session based RDS deployment scenario.
    i. Configure a RD Session broker on WINSRV7.
    ii. Configure a RD Web Access server on WINSRV11.

iii. Configure a RD Session Host on WINSRV6.
iv. RD Licensing Server should be installed on WINSRV11, deployment per user.
v. Configure a RD Gateway on a suitable server.
vi. Use Skill39-SSC for the certificate.
vii. Create the external FQDN rds.skill39.at for the session broker.

CERTIFICATION AUTHORITY

a. Create a Root-CA - that can be offline – and a Sub CA.
b. Create a Standalone Root CA.
c. Common name is “Skill39 RootCA”.
d. Prepare the Root CA for later shutdown.
e. Prepare WINSRV9 for use as Sub CA.
f. Use “C:\Cert-Skills2020-Enrollment” as distribution folder; use less privileged as useful.
g. Install IIS on WINSRV9.
h. Rename virtual directory on WINSRV9 to “Certs_Skill39”.
i. Enable directory browsing for the virtual directory.
j. Enable double escaping in WINSRV9.
k. Create a subordinate CA on WINSRV9, named “Skill39-Intra-CA”.
l. On path WINSRV9\C should exist no cert files.
m. Certification and CRL validity period:
n. CRL Period: Weeks
    i. CRLPeriodUnits: 1
    ii. CRLDeltaPeriodUnits: 1
    iii. CRL DeltaPeriod: Days
    iv. CRL OverlapPeriod: Hours
    v. ValididityPeriodUnits: 5
    vi. ValididityPeriod: Years
o. Configure Key Recovery Agent “Skill39-Key Recovery Agent”.
p. Activate Key Archival.

Secure Administration-Host

a. For secure Administration of Skills2020, implement a “Secured Workstation”:
b. Create OU “Skill39-Tier1-Administration”.
c. Create OU “Hosts” and “Users” below “Skill39-Tier1-Administration”.
d. Move WINCLI15 to “Hosts”.
e. Create a user “PAW-Maintainer” and a user “PAW-user”; both in the OU “Users” created before.
f. Create a GPO, that only members of the group “Local Administrators” can log on the WINCLI10.
g. Also create a GPO, that all other local groups have no members.
h. Import restricted Firewall-rules “pawfirewallupdate.wfw”.
    i. Use only IPv4 security rules.
    ii. Adapt the other rules, as necessary.
i. No one, except Skill39-PAW-Administrators can change IE Automatic configurations.
j. Also, only Skills2020-PAW-Administrators can browse the internet.
k. Logon as batch-job to the PAW Workstation is not allowed – also implemented using GPO.
l. Enable credential guard using GPO for PAW Workstation.
m. Create necessary firewall rules.
n. Implement further safeguards according to industry standards.

SELF ASSESSMENT QUESTIONNAIRE

How did you secure the connection between WINSRV2 and WINSRV3?

How was the access to WINCLI5 (secure workstation) implemented?

How did you secure the connection between WINSRV2 and WINSRV12?

Describe the security solution for the RDS-Gateway:

Describe the security solution for your secure administration host.

SELF ASSESSMENT :: PART II

Device	IP-Address	Configured roles and features	Comments
WINSRV1	82.89.144.100		
WIINCLI1	82.89.144.101		
WINSRV4	10.1.0.1		
WINSRV5	10.1.0.2		
WINSRV6	10.1.0.3		
WINSRV7	10.1.0.4		
WINSRV8	10.1.0.5		
WINSRV9	10.1.0.6		
WINSRV2	10.1.0.254, 82.89.144.110		
WINSRV10	10.2.0.1		
WINSRV3	10.2.0.254, 82.89.144.111		

Device	IP-Address	Configured roles and features	Comments
WINSRV11	192.168.1.1		
WINSRV12	192.168.1.254, 82.89.144.112		