EuroSkills Test Project

ICT Specialists (39)
Module B – Microsoft Environment

Submitted by:

Gen Lee EE

Silvio Papic HR

Svetlana Lapenko KZ

Nitheesh Murugan Kaliyamurthy UK

CONTENTS

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

Please **carefully read** the following instructions!

This Test Project consists of the following documentation/files:

1. ES2023_TP39_ModuleB_v0.2.docx
2. ES2023_TP39_ModuleB_Users.xlsx

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!*

LOGIN

Username:	Administrator
Password:	Passw0rd!

SYSTEM CONFIGURATION

Language:	English US
Time format:	Polish / Danish
Key Map:	English US

INTRODUCTION

You have been hired as an IT-professional by a Multinational Corporation called Skill39. Skill39 operates currently at two countries: Poland and Denmark.

Your job is to bring up a Forest Root Domain with two Child Domains and services associated with them.

DESCRIPTION OF PROJECT AND TASKS

Part 1 – SKILL39.WSE

You will need to set-up the Skill39 Enterprise Forest Root Domain in Cloud Environment. This includes the whole Enterprise Forest monitoring and Root Certificate Authority.

CLOUD-FW

a. Install/Configure
   i. Install RRAS
   ii. Modify the default Firewall rules to allow ICMP traffic
b. Site-to-Site VPN to PL-FW and DK-FW servers
   i. Set the connection type to "persistent connection"
   ii. All traffic bound to PL.SKILL39.WSE and DK.SKILL39.WSE will be placed in the VPN tunnel

CLOUD-DC

a. AD DS
   i. Create a forest named skill39.wse
b. DNS
   i. Create all appropriate A records for all Cloud servers on 10.1.0.0/24
   ii. Create a reverse lookup zone creating PTR records for all servers
   iii. Create following CNAME records
      - crl.skill39.wse IN CNAME cloud-dc.skill39.wse
      - cacerts.skill39.wse IN CNAME cloud-dc.skill39.wse
   iv. Create Stub Zones for pl.skill39.wse and dk.skill39.wse
c. IPAM
   i. Provide IPAM Service using Group Policy based provisioning
   ii. Provision the IPAM Service for skill39.wse, pl.skill39.wse and dk.skill39.wse
   iii. Discover the servers with roles – Domain controller, DHCP server and DNS server
d. IIS
   i. Host Skill39 Corporate Root CA CDP & AIA

CLOUD-ROOTCA

a. Root CA machine should be turned on only for issuing new certificates and updating CRL
b. Make sure that your Root CA machine is turned off at the end of the day
c. Common Name: Skill39-CA
d. URL for CDP: http://crl.skill39.wse/Skill39-CA.crl
e. URL for AIA: http://cacerts.skill39.wse/Skill39-CA.crt
f. Issue certificates for Skill39-PL-CA and Skill39-DK-CA

Part 2 – PL.SKILL39.WSE

PL-FW

a. Install/Configure
   i. Install RRAS
   ii. Modify the default Firewall rules to allow ICMP traffic

b. Site to Site VPN to CLOUD-FW server
   i. Set the connection type to "persistent connection"
   ii. All traffic bound to SKILL39.WSE and DK.SKILL39.WSE will be placed in the VPN tunnel

PL-DC

a. AD DS
   i. Create a child domain pl.skill39.wse in skill39.wse tree
   ii. Create user accounts that belong to pl.skill39.wse domain with all parameters defined in ES2023_TP39_ModuleB_Users.xlsx. Use first two letters from first_name combined with dot and last_name as SAMAccountName. John Doe -> Jo.Doe.
   iii. Update ADMX administrative template files for Windows 10 22H2

b. Subordinate Certificate Authority
   i. Distribute Skill39 Root CA to all domain machines
   ii. Common Name: Skill39-PL-CA
   iii. CRL should be automatically published to its locations
   iv. URLs for CDP:
      - http://crl.pl.skill39.wse/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
      - http://crl.skill39.wse/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
   v. URLs for AIA
      - http://cacerts.pl.skill39.wse/Skill39-PL-CA.crt
      - http://cacerts.skill39.wse/Skill39-PL-CA.crt
   vi. Create following templates:
      - PL-Users: Used for issuing certificates to all PL users
      - PL-Server: Used for issuing certificates for PL servers and services

PL-SRV

a. Mount second disk drive to C:\Files

b. Configure IIS
   i. Create "https://web.pl.skill39.wse" website
   ii. Enable Windows Internal Authentication
   iii. Make sure that PL and DK Skill39 users can authenticate
   iv. Authenticated users should be presented a text "Welcome to PL Skill39 HQ Website"

c. DFS

i. Create a Namespace with the name "dfs"

ii. Add PL-DC as the second server for this Namespace

iii. Create DFS links for the department shares (Experts, Competitors, Managers)

iv. Create a DFS Replication like this:

- PL-SRV: C:\Files\Experts -> PL-DC: C:\Files\Experts
- PL-SRV: C:\Files\Competitors -> PL-DC: C:\Files\Competitors
- PL-SRV: C:\Files\Managers -> PL-DC: C:\Files\Managers

v. Map the department shares depending on the corresponding group (PL-Users_Experts, PL-Users_Competitors, PL-Users_Managers) to drive G: using the DFS Namespace

d. DHCP

i. Range: 10.2.0.100-10.1.0.150

ii. Configure needed DHCP options based on the PL infrastructure

PL-CLIENT

Using Group Policies configure following policies:

a. Disable the First Sign-in Animation

b. Set the Telemetry level to Enhanced

c. Hide the "Most used" list from Start Menu

d. Set the Edge homepage and start-up page as https://web.pl.skill39.wse

Part 3 – DK.SKILL39.WSE

DK-FW

a. Install/Configure

i. Install RRAS

ii. Modify the default Firewall rules to allow ICMP traffic

b. Site to Site VPN to CLOUD-FW server

i. Set the connection type to "persistent connection"

ii. All traffic bound to SKILL39.WSE and DK.SKILL39.WSE will be placed in the VPN tunnel

DK-DC

a. AD DS

i. Create a child domain dk.skill39.wse in skill39.wse tree

vii. Create user accounts that belong to pl.skill39.wse domain with all parameters defined in ES2023_TP39_ModuleB_Users.xlsx. Use first three letters from last_name combined with dot and first_name as SAMAccountName. John Smith -> Smi.John

b. Subordinate Certificate Authority

i. Distribute Skill39 Root CA to all domain machines
ii. Common Name: Skill39-DK-CA
iii. CRL should be automatically published to its locations
iv. URLs for CDP:
- http://crl.dk.skill39.wse/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
- http://crl.skill39.wse/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

v. URLs for AIA
- http://cacerts.dk.skill39.wse/Skill39-DK-CA.crt
- http://cacerts.skill39.wse/Skill39-DK-CA.crt

vi. Create following templates:
- DK-Server: Used for issuing certificates for PL servers and services

vii. Certification and CRL validity period:
- CRL Period: Weeks
- CRLPeriodUnits: 2
- CRLDeltaPeriodUnits: 1
- CRL DeltaPeriod: Days
- CRL OverlapPeriod: Hours
- CRL OverlapPeriodUnits: 12
- ValididityPeriodUnits: 5
- ValididityPeriod: Years

c. Create an SMB based witness disk for Failover Cluster located at \\DK-DC\witness
d. Remote Desktop Services
i. Configure web-access for terminal services
ii. The RDS login page should be accessible through https://rds.dk.skill39.wse
iii. Use certificates signed by Skill39-DK-CA for all terminal services components
iv. Publish Notepad on web-portal from Session Host "DK-APP" for all dk.skill39.wse "Experts" department users
v. Publish Wordpad on web-portal from Session Host "DK-APP" for all dk.skill39.wse "Competitors" department users

DK-STORAGE

a. iSCSI Target
i. Add new disk of 150 G for storing the virtual machines
ii. Format disk using ReFS and mount as "E:\" drive
iii. Create 100G iSCSI virtual disk "E:\iSCSIVirtualDisks\ES2023-VM.vhdx"

DK-SRV1 and DK-SRV2

a. Configure iSCSI initiator

i. Connect iSCSI disk "ES2023-VM" and create ReFS partition using maximum available size

ii. Mount the volume as "S:\" drive

b. Configure Hyper-V Failover Cluster

i. Name: DK-CLUSTER

ii. IP address: 10.3.0.15

iii. Create role "Skill39-DK-Infra" that contains the virtual machines

iv. Skill39-DK-Infra has to primarily run on HYPERV2 unless it fails

DK-APP

c. Hosted on Hyper-V Cluster

d. Functions as Remote Desktop Session Host for Notepad and Wordpad

DK-CLIENT

Using Group Policies configure following policies:

a. Make sure that user is shown detailed status messages at sign-in and sign-out

b. Allow ICMP from DK, PL and CLOUD internal subnets

c. Allow Remote Administration with PowerShell from DK domain

CONFIGURATION TABLE

Hostname	Operating System	Domain	IP Address(es)	Configuration
CLOUD-FW	Windows Server 2022 21H2 Desktop	WORKGROUP	198.51.100.11 10.1.0.254	Base
CLOUD-DC	Windows Server 2022 21H2 Desktop	SKILL39.WSE	10.1.0.1	Base
CLOUD-ROOTCA	Windows Server 2022 21H2 Desktop	WORKGROUP	10.1.0.5	Base
PL-FW	Windows Server 2022 21H2 Desktop	WORKGROUP	198.51.100.21 10.2.0.254	Base
PL-DC	Windows Server 2022 21H2 Desktop	PL.SKILL39.WSE	10.2.0.1	Base
PL-SRV	Windows Server 2022 21H2 Core	PL.SKILL39.WSE	10.2.0.20	Base
PL-CLIENT	Windows 10 Enterprise 22H2	PL.SKILL39.WSE	DHCP	Base
DK-FW	Windows Server 2022 21H2 Desktop	WORKGROUP	198.51.100.31 10.3.0.254	Base
DK-DC	Windows Server 2022 21H2 Desktop	DK.SKILL39.WSE	10.3.0.1	Base
DK-SRV1	Windows Server 2022 21H2 Desktop	DK.SKILL39.WSE	10.3.0.11 172.16.3.11	Base
DK-SRV2	Windows Server 2022 21H2 Core	DK.SKILL39.WSE	10.3.0.12 172.16.3.12	Base
DK-STORAGE	Windows Server 2022 21H2 Desktop	WORKGROUP	172.16.3.10	Base
DK-APP	Windows Server 2022 21H2 Desktop	DK.SKILL39.WSE	10.3.0.25	No
DK-CLIENT	Windows 10 Enterprise 22H2	DK.SKILL39.WSE	DHCP	Base

Machines indicated as "**Base"** are standard installs which have been sysprepped and generalized to save installation time across the project. These machines still need to be configured.

NETWORK DIAGRAM