worldskills

Test Project

Module B – Windows Environment

IT Network Systems Administration

Submitted by
Sim Cher Boon - GrabTaxi Holdings Limited, Independent Test Project Designer
Timon Frey, Independent Test Project Validator

Contents

Introduction 3
Description of project and tasks 3
Part 1: Internal Layer 6
Part 2: DMZ Layer 9
Part 3: Beijing Remote Network 10
Active Directory Domain Service (AD DS) 10
Dynamic Host Configuration Protocol (DHCP) 10
Windows Server Update Services (WSUS) 11
Part 4: The Internet 11
Dyamic Host Configuration Protocol (DHCP) 11
Windows Server Update Services (WSUS) 11
Part 5: VPN 12
Part 6: Automation 12
Part 7: SHANGHAI, BEIJING, and REMOTE Client Network 12

Introduction

Welcome to Module B!

- The competition has a fixed start and finish time. You must decide how to best divide your time
- To successfully complete this Module, please **read** the following instructions **carefully**!

Logins

Please refer to the following table for default password if not specified explicitly:

TYPE	PASSWORD
Server	Skill39@Shanghai
Client	Skill39@Shanghai

Operating Systems

- Windows Server 2025 26100.32230.260111-0550
- Windows 11 Enterprise 26200.6584.250915-1905

Documents / Files

- users.json
- Windows FoD - 26100.1.240331-1435.ge_release_amd64fre_CLIENT_LOF_PACKAGES_OEM.iso
- Windows 11 Enterprise- 26200.6584.250915-1905.25h2_ge_release_svc_refresh_CLIENTENTERPRISEEVAL_OEMRET_x64FRE_en-us (No TPM).iso
- Windows Server 2025 - 26100.32230.260111-0550.lt_release_svc_refresh_SERVER_EVAL_x64FRE_en-us

Description of project and tasks

You have been hired as an external IT consultant by a company called GoldenHorse located in Shanghai.

In July, GoldenHorse took over another company located in Beijing.

As an international company, GoldenHorse also owns an Internet infrastructure.

Your colleague, the system architect, drew a topology diagram how to integrate the IT infrastructure of the acquired company into GoldenHorse.

Your job is to integrate and provision the required infrastructure as required. You can find the topology diagram below.

© WorldSkills International

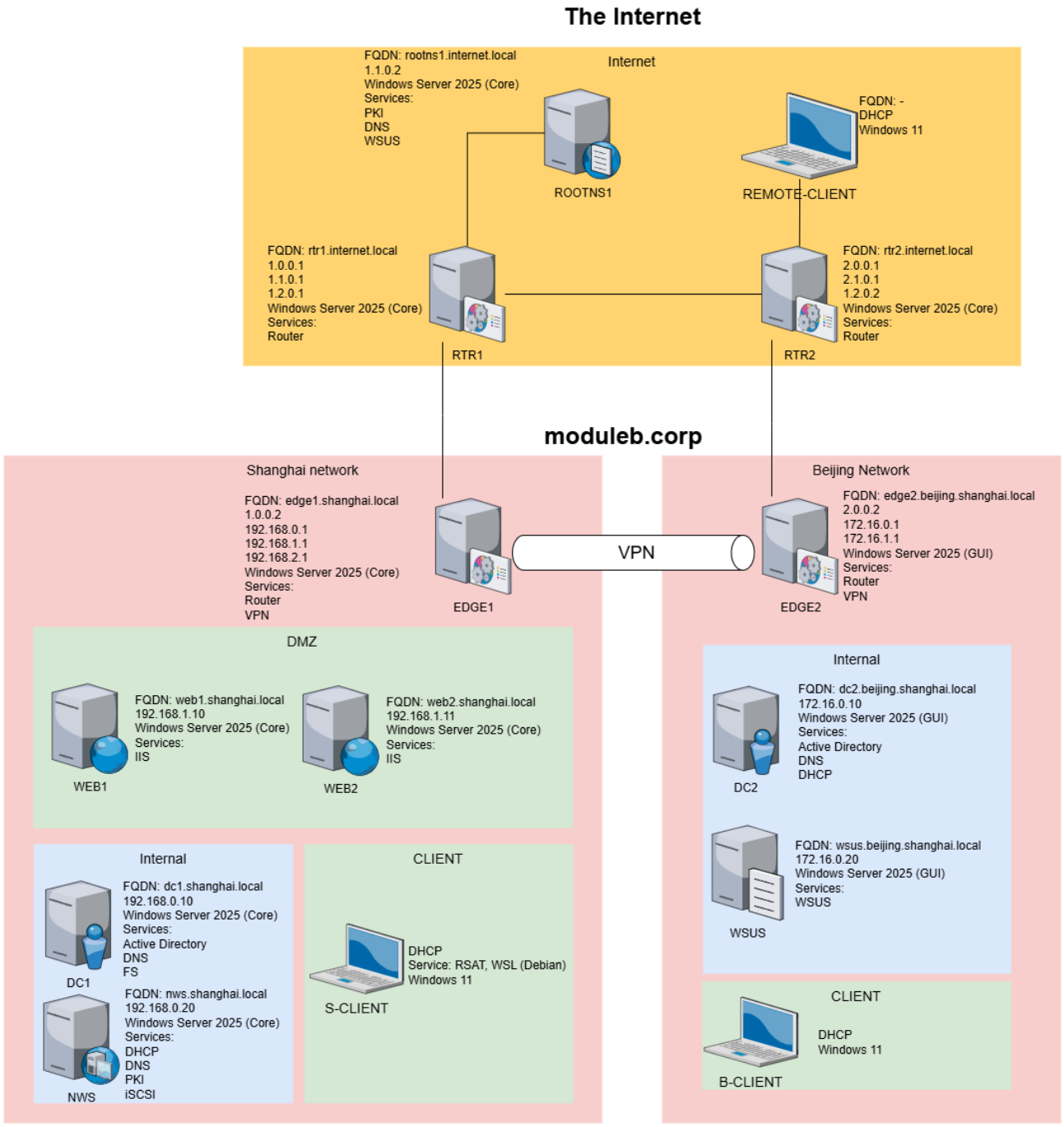
General Configuration

Servers and Clients

HOSTNAME	FULLY QUALIFIED DOMAIN NAME (FQDN)	IPV4	SERVICES
ROOTNS1	rootns1.internet.local	1.1.0.2	PKI, DNS, WSUS
RTR1	rtr1.internet.local	1.0.0.1 1.1.0.1 1.2.0.1	Router
RTR2	rtr2.internet.local	2.0.0.1 2.1.0.1 1.2.0.2	Router
REMOTE-CLIENT	-	DHCP	-
EDGE1	edge1.shanghai.local	1.0.0.2 192.168.0.1 192.168.1.1 192.168.2.1	Router, VPN
NWS	nws.shanghai.local	192.168.0.20	DHCP, DNS, PKI, iSCSI
DC1	dc1.shanghai.local	192.168.0.10	Active Directory, DNS, FSRM
WEB1	web1.shanghai.local	192.168.1.10	IIS
WEB2	web2.shanghai.local	192.168.1.11	IIS
S-CLIENT	-	DHCP	-
EDGE2	edge2.beijing.shanghai.local	2.0.0.2 172.16.0.1 172.16.1.1	Router, VPN
DC2	dc2.beijing.shanghai.local	172.16.0.10	Active Directory, DNS, DHCP
WSUS	wsus.beijing.shanghai.local	172.16.0.20	WSUS
B-CLIENT	-	DHCP	-

© WorldSkills International

Topology



© WorldSkills International

Part 1: Internal Layer

dc1.shanghai.local

This machine is preinstalled with Windows Server 2025 (Core). Ensure the hostname and IP address are configured as per the "Servers and Clients" table.

Active Directory Domain Service (AD DS)

1. Create a new Active Directory domain including a new forest
    a. Root forest: shanghai.local
2. Join the Windows servers located in the Shanghai DMZ and Internal layers to the domain shanghai.local

Domain Name Services (DNS)

1. Create a reverse zone on the primary DNS server.
2. Create additional A Records according to the table below:

RECORD	IP ADDRESS
www	192.168.1.12

1. Forward resolve request for all non-internal domain name records to ROOTNS1.

Group Policy Object (GPO)

1. Create group policies (GPO) with the following requirements found in the table below. GPO name must be followed:

GPO NAME	REQUIREMENT/DESCRIPTION
TierOne	1. All users should receive a login banner that reads: Caption: "Welcome to Shanghai! Only authorised personnel allowed to access. Please bring some tea" Title: Shanghai 2. Set the following system environment variable: Name = ClawMachine Value = Ops6.7 3. Disable the local Administrator Account 4. Prevent LM hash from being stored locally in the SAM Database and Active Directory 5. The computer should check for updates every Monday at 08:00 using internal WSUS server
TierTwo	1. Members of SG-IT group should have notepad.exe launched automatically when logged in.

© WorldSkills International

GPO NAME	REQUIREMENT/DESCRIPTION
NOTECH	1. Users in groups SG-SALES, SG-MKT, and SG-HR only (a) Disable ability to edit registry (b) "cmd", "run" and "powershell" should be disbaled (c) File history should be turned off

File Server Resource Manager (FSRM)

1. In C:\GroupShare\ create the following shares

SHARENAME	ACCESS CONTROL
SALES	SG-SALES (read, write) only
MKT	SG-MKT (read, write) only
HR	SG-HR (read, write) only
IT	SG-IT (read, write) only

   (a) GroupShare should be automatically mapped to G:\
   (b) Executable files should be prevented from being saved to on GroupShare

2. Each user will recieve an individual personal network drive

   (a) The personal drives should be created in C:\UserShare\
   (b) The personal drives should be automatically mapped to T:\
   (c) All current and future personal drives should have a quota with a hard limit of 50MB
   (d) Executable files should be prevented from being saved to personal drives

nws.shanghai.local

This machine is preinstalled with Windows Server 2025 (Core). Ensure the hostname and IP address are configured as per the "Servers and Clients" table.

Domain Name Services (DNS)

1. Configure NWS as Secondary DNS server.

   (a) Forward zones and reverse zone hosted by the primary DNS server must be synchronized from the primary DNS server.

Dynamic Host Configuration Protocol (DHCP)

1. Configure a DHCP server on NWS and configure the following DHCP range

- DHCP range for 192.168.2.0/24
- Default gateway: 192.168.2.1
- DNS: 192.168.0.10
- Lease: 192.168.2.100 – 200
- Scope name: shanghai
- Exclude: 192.168.2.100 – 150
- Duration: 8 days, 8 hours, 8 minutes

2. Ensure hosts in the Client Network can obtain IP addresses from the DHCP server

Public Key Infrastrucutre (PKI)

1. Configure an Enterprise Subordinate CA for shanghai.local on NWS
2. Ensure your CA is signed by ROOTNS1
3. Common Name: Shanghai-CA
4. URL for CDP: http://nws.shanghai.local/CertEnroll/Shanghai-CA.crl
5. URL for AIA: http://nws.shanghai.local/CertEnroll/Shanghai-CA.crt
6. Create following certificate templates:

   (a) Skills Users – For user certificates; certificate needs to be auto-enrolled for all users
   (b) Skills Computers – For computer certificates; certificate needs to be auto-enrolled for all Computers
   (c) Skills Web Server – For web server certificates

iSCSI

1. Install iSCSI Target on NWS

   (a) Use the location E:/iSCSI/WebCluster.vhdx for Virtual Disk
   (b) Use the name WebClusterTarget
   (c) Use 10 GB as the size

2. Add Web1 and Web2 as Inititators with IP Address

edge1.shanghai.local

This machine is preinstalled with Windows Server 2025 (Core). Ensure the hostname and IP address are configured as per the "Servers and Clients" table.

Routing

1. Configure EDGE1 to serve as default gateway for 192.168.0.0/24, 192.168.1.0/24 and 192.168.2.0/24 subnets
2. Configure NAT, ensure that internal networks going to internet uses NAT on 1.0.0.2 to reach the internet.
3. Configure NAT such that traffic from internet hitting 1.0.0.2 port 80 and 443 goes to 192.168.1.12 address.

© WorldSkills International

Part 2: DMZ Layer

web1.shanghai.local

This machine is preinstalled with Windows Server 2025 (Core). Ensure the hostname and IP address are configured as per the "Servers and Clients" table.

web2.shanghai.local

This machine is preinstalled with Windows Server 2025 (Core). Ensure the hostname and IP address are configured as per the "Servers and Clients" table.

Failover Cluster

iSCSI

1. Install Windows Feature Multipath-IO on both WEB1 and WEB2
2. Enable MSDSMAutomationClaim with Bustype iSCSI
3. Connect persistent iSCSI from nws.shanghai.local using iscsicpl.exe
4. Initialize the disk with MaximumSize and Drive Letter E and Format File System NTFS

Failover Cluster

1. Install Failover Cluster Server Role on both WEB1 and WEB2
2. Create Cluster with Cluster IP 192.168.1.12, Node WEB1 and WEB2, Cluster Name WEBCluster
3. Add iSCSI Target as Cluster Storage

Internet Information Services (IIS)

1. Install IIS Web Server and ASP.NET 4.8 on WEB1 and WEB2
2. Create site www.shanghai.local
3. The web server should display the following page saved on the iSCSI drive E:/WEB/default.aspx

```
<!DOCTYPE html>
<html>
<body>
   <h1>Active IIS Node</h1>
   <p><%= Environment.MachineName
%></p>
</body>
</html>
```

4. All users accessing /www.shanghai.local should not encounter any certificate errors in the edge web browser

© WorldSkills International

Part 3: Beijing Remote Network

edge2.beijing.shanghai.local

This machine is preinstalled with Windows Server 2025 (GUI). Ensure the hostname and IP address are configured as per the "Servers and Clients" table.

Routing

1. Configure EDGE2 to serve as default gateway for 172.16.0.0/24 and 172.16.1.0.
2. Configure NAT, ensure that internal networks going to internet uses NAT on 2.0.0.2 to reach the internet.

dc2.beijing.shanghai.local

This machine is preinstalled with Windows Server 2025 (GUI). Ensure the hostname and IP address are configured as per the "Servers and Clients" table.

Active Directory Domain Service (AD DS)

1. Create a new active directory child domain

   (a) Child Domain: beijing.shanghai.local

2. Join the Windows servers located in the Beijing Internal net to the domain beijing.shanghai.local

Group Policy Object (GPO)

1. Link the GPO's (TierOne, TierTwo, NOTECH) from shanghai.local to beijing.shanghai.local

Dynamic Host Configuration Protocol (DHCP)

1. Configure a DHCP server on DC2 and configure the following DHCP range

- DHCP range for 172.16.1.0/24
- Default gateway: 172.16.1.1
- DNS: 172.16.0.10
- Lease: 172.16.1.100 – 200
- Scope name: beijing
- Exclude: 172.16.1.100 – 150
- Duration: 8 days, 8 hours, 8 minutes

2. Ensure hosts in the Client Network can obtain IP addresses from the DHCP server

wsus.beijing.shanghai.local

This machine is preinstalled with Windows Server 2025 (GUI). Ensure the hostname and IP address are configured as per the "Servers and Clients" table.

Windows Server Update Services (WSUS)

1. Install WSUS service
   (a) Database type: WID
   (b) Store contents in C:\WSUS
   (c) Use ROOTNS1 as master WSUS and configure this server as downstream
2. Synchronize the update from ROOTNS1
3. Install KB5094126 2026-06 Cumulative Update on B-Client so that it appears in update History on client

Part 4: The Internet

RTR1

RTR1 has been preconfigured and is locked down preventing any changes to its configuration

Routing

1. Routing services has been installed on the RTR1 server. It is the default gateway for the 1.0.0.0/24 and 1.1.0.0/24 network.

RTR2

RTR2 has been preconfigured and is locked down preventing any changes to its configuration

Routing

1. Routing services has been installed on the RTR2 server. It is the default gateway for the 2.0.0.0/24 network.

Dyamic Host Configuration Protocol (DHCP)

1. DHCP has been configured for RTR2 on 2.0.0.0/24 network.

ROOTNS1

The ROOTNS1 server is preinstalled with Windows Server 2025 (Core). Ensure the hostname and IP address are configured as per the "Servers and Clients" table.

Note: **DO NOT** join the server to any domain, leave the server in a workgroup.

Windows Server Update Services (WSUS)

Note: WSUS has been configured and acts as the upstream server, no configuration changes are required to the WSUS service.

Domain Name Services (DNS)

1. Install DNS, create a forward zone for "shanghai.local" and add the following record:

RECORD	IP ADDRESS

www	1.0.0.2

2. The website www.shanghai.local should be accessible from REMOTE-CLIENT Microsoft Edge browser.
3. All DNS records that are non internal, residing in internet, should be resolved by ROOTNS1.

Public Key Infrastrucutre (PKI)

1. ROOTNS1 is Root CA for the entire network. It acts as the internet RootCA, and all Enterprise CA in SHANGHAI and BEIJING certificates are signed by ROOTNS1.
2. ROOTNS1 CA should not issue certificates directly to internal network. Internal certificates must be issued by Enteprise CA.
3. CA type: Standalone Root CA
4. Common Name: Internet-CA
5. URL for CDP: http://rootns1.internet.local/CertEnroll/Internet-CA.crl
6. URL for AIA: http://rootns1.internet.local/CertEnroll/Internet-CA.crt

Part 5: VPN

1. Set up an IKEv2 IPsec Site-to-Site VPN tunnel between the locations SHANGHAI and BEIJING using the machines EDGE1 and EDGE2. It is authenticated using preshared key that is the same as the default password.
2. Make sure that all subnets in SHANGHAI can reach the network in BEIJING and vice versa.

Part 6: Automation

S-Client

1. Every Playbook should be saved in C:\playbooks
2. Use inventory.yaml to configure the hostname to DC1
3. create an anisble playbook called main.yml that creates the users listed in the users.json file on DC1.

   (a) If the OU and Security Group don't exist, create it.
   (b) Every user should be in the correct OU and Security Group
   (c) Every user should be enabled, have a personal drive and passwords should not be changed on next logon

Part 7: SHANGHAI, BEIJING, and REMOTE Client Network

1. Install Windows 11 on B-CLIENT machine
2. Ensure each client computer obtains an IP address automatically from the respective DHCP servers
3. Join S-CLIENT and B-CLIENT machines to their respective domains.
4. S-CLIENT is pre-installed with RSAT and Ansible