Test Project

Module B Windows Environment

IT Networks Systems Administration

Independent Test Project Designer: Sim Cher Boon, Thushjandan Ponnudurai
Independent Test Project Validator: Troy Pretty

Contents

Introduction

Welcome to module B!

To successfully complete this module, please **read** the following instructions **carefully**!

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

Login

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

TYPE	PASSWORD
Server	Skill39@Lyon
Client	Skill39@Lyon

Operating Systems

- Windows Server 2022 21H2
- Windows 11 23H2

Additional Files

The following additional files have been provided to assist with the competition of this module

- WEB-SRV
  - “requestRouter_amd64.msi” located on the Administrator Desktop.
  - “rewrite_amd64_en-US.msi” located on the Administrator Desktop.
  - “HTML templates” located on the Administrator Desktop.
- PARIS-ROUTER
  - “requestRouter_amd64.msi” located on the Administrator Desktop.
  - “rewrite_amd64_en-US.msi” located on the Administrator Desktop.

Description of project and tasks

Intro

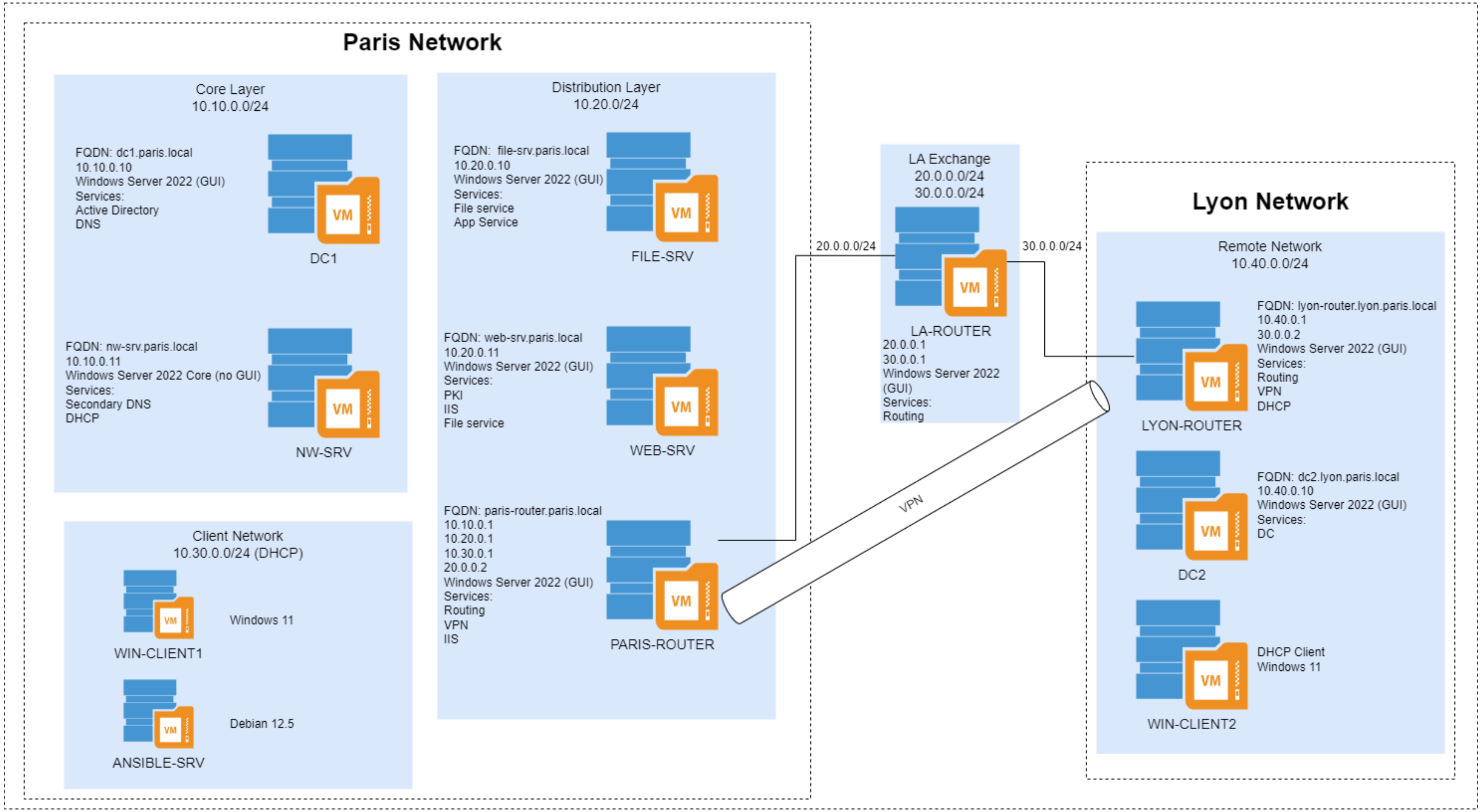
You have been hired as an external IT consultant by a company called ErasTour24 located in Paris. In July, ErasTour24 took over another company located in Lyon. As an international company, ErasTour24 also owns an Internet Exchange located in Los Angeles. Your colleague, the system architect, drew a topology diagram how to integrate the IT infrastructure of the acquired company into ErasTour24. Your job is to integrate and provision the required infrastructure as required. You can find the topology diagram below.

General Configuration

Servers and Clients

HOSTNAME	FULLY QUALIFIED DOMAIN NAME (FQDN)	IPV4	SERVICES	DOMAIN JOINED
DC1	dc1.paris.local	10.10.0.10	Active Directory Domain Service Domain Name Service	paris.local
NW-SRV	nw-srv.paris.local	10.10.0.11	Domain Dname Service DHCP Service	
FILE-SRV	file-srv.paris.local	10.20.0.10	File Service App Service	
WEB-SRV	web-srv.paris.local	10.20.0.11	PKI Certificate Authority IIS Web Service File Service	
PARIS-ROUTER	paris-router.paris.local	10.10.0.1 10.20.0.1 10.30.01 20.0.0.2	Routing and Remote Service IIS Web Service	
LA-ROUTER	-	20.0.0.1 30.0.0.1	Routing and Remote Service	-
LYON-ROUTER	lyon-router.lyon.paris.local	10.40.0.1 30.0.0.2	Routing and Remote Service DHCP Service	lyon.paris.local
DC2	dc2.lyon.paris.local	10.40.0.10	Active Directory Domain Service Domain Name Service	
WIN-CLIENT1	-	DHCP	-	paris.local
WIN-CLIENT2	-	DHCP	-	lyon.paris.local
ANSIBLE-SRV	-	DHCP	Ansible	-

Topology


Paris Network
Core Layer
10.10.0.0/24
FQDN: dc1.paris.local
10.10.0.10
Windows Server 2022 (GUI)
Services:
Active Directory
DNS
VM
DC1
FQDN: nw-srv.paris.local
10.10.0.11
Windows Server 2022 Core (no GUI)
Services:
Secondary DNS
DHCP
VM
NW-SRV
Client Network
10.30.0.0/24 (DHCP)
VM
WIN-CLIENT1
Windows 11
VM
ANSIBLE-SRV
Debian 12.5
Distribution Layer
10.20.0/24
FQDN: file-srv.paris.local
10.20.0.10
Windows Server 2022 (GUI)
Services:
File service
App Service
VM
FILE-SRV
FQDN: web-srv.paris.local
10.20.0.11
Windows Server 2022 (GUI)
Services:
PKI
IIS
File service
VM
WEB-SRV
FQDN: paris-router.paris.local
10.10.0.1
10.20.0.1
10.30.0.1
20.0.0.2
Windows Server 2022 (GUI)
Services:
Routing
VPN
IIS
VM
PARIS-ROUTER
20.0.0.0/24
LA Exchange
20.0.0.0/24
30.0.0.0/24
VM
LA-ROUTER
20.0.0.1
30.0.0.1
Windows Server 2022
(GUI)
Services:
Routing
30.0.0.0/24
VPN
Lyon Network
Remote Network
10.40.0.0/24
FQDN: lyon-router.lyon.paris.local
10.40.0.1
30.0.0.2
Windows Server 2022 (GUI)
Services:
Routing
VPN
DHCP
VM
LYON-ROUTER
FQDN: dc2.lyon.paris.local
10.40.0.10
Windows Server 2022 (GUI)
Services:
DC
VM
DC2
DHCP Client
Windows 11
VM
WIN-CLIENT2

Task 1: Core Layer

dc1.paris.local

This machine is preinstalled with Windows Server 2022 (GUI). Ensure the hostname and IP address are configured as per the “Servers and Clients” table.

Active Directory Domain Service

1. Create a new Active Directory domain including a new forest

   (a) Root forest: paris.local

2. Join the Windows servers located in the Paris Core and Distribution layers to the domain paris.local
3. Create the following organization units (OU):

   (a) MKT
   (b) SALES
   (c) TECH
   (d) HR

4. Create following AD group under their corresponding OUs:

   (a) MKT
   (b) SALES
   (c) TECH
   (d) HR

5. Create a powershell script and save it in C:\create_user.ps1, the script must create the following users according to the table.

USER PREFIX	NUMBERS	PASSWORD	OU	GROUP MEMBERSHIPS
mkt	1 – 20	<<Default Password>>	MKT	MKT
sales	1 – 20	<<Default Password>>	SALES	SALES
tech	1 – 20	<<Default Password>>	TECH	TECH
hr	1 – 20	Skill39@LyonSkill39@Lyon	HR	HR

e.g. username: mkt13

Ensure that your script is runnable, taking in an argument “-count”, when used with “-count X”, X is a number indicating the last number for user creation.

The script should ensure that users created do not need to change password on next logon, and it should ignore creating a user if it already exists.

Sample run: C:\create_user.ps1 -count 5

Note: If you are unable to create the powershell script the users can be created manually but you will not receive marks for the creation of the automated script

6. Create a fine-grained password policy, which requires 16 characters complex password for all users from HR.

Domain Name Services (DNS)

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

RECORD	IP ADDRESS
www	10.20.0.11
external	
help	
app	10.20.0.10

Group Policy (GPO)

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

GPO NAME	REQUIREMENT/DESCRIPTION
Desktop	1. All users should receive a login banner that reads: "Welcome to Lyon! Only authorised personnel allowed to access. Should you try to break in, I knew you were trouble" 2. Set the following system environment variable: Name = TheErasTour Value = 2024 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 Friday at 13:00
TECH	Members of TECH group should have powershell.exe launched automatically when logged in.
NOTECH	Strictly users in SALES, MKT, and HR only: 1. Disable ability to edit registry 2. "cmd", "run" and "powershell" should be disbaled 3. File history should be turned off

nw-srv.paris.local

This machine is preinstalled with Windows Server 2022 (core). Ensure the hostname and IP address are configured as per the “Servers and Clients” table.

Domain Name Services (DNS)

1. Configure NW-SRV 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 NW-SRV and configure the following DHCP range

- DHCP range for 10.30.0.0/24
- Default gateway: 10.30.0.1
- DNS: 10.10.0.10
- Secondary DNS: 10.10.0.11
- Lease: 10.30.0.100 – 200
- Scope name: client
- Exclude: 10.30.0.100 – 150
- Duration: 13 days, 13 hours, 13 minutes

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

Task 2: Distribution Layer

file-srv.paris.local

This machine is preinstalled with Windows Server 2022 (GUI). Ensure the hostname and IP address are configured as per the “Servers and Clients” table.

RemoteApps

1. Prepare FILE-SRV machine to publish RemoteApps
2. Publish notepad.exe

   (a) NOTE: HTTPS compliance is not required, a self signed certificate can be used

3. RemoteApps should be accessible from both the Paris and Lyon client networks

File Server Resource Manager (FSRM)

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

SHARENAME	ACCESS CONTROL
CommonShare	All users (read, write) except HR
MKT	MKT (read, write) only
SALES	SALES (read, write) only
TECH	TECH (read, write) only
HR	HR (read, write) only

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

Distributed File System (DFS)

1. Install distributed file system on file-srv
2. All DFS Roots are to be saved in C:\DFSRoots\
3. Create a DFS namespace named “CSDrive”
4. Create a DFS share for each share as follows:

NAMESPACE	SHARENAME	DFS SHARENAME	MAPPED DRIVE LETTER
CSDrive	CommonShare	CommonShare	Z:\
	MKT	MKT	X:\
	SALES	SALES	
	TECH	TECH	
	HR	HR	

5. The DFS CommonShare should be automatically mapped to all authorized users as Z:\
6. The individual department DFS shares should be automatically mapped to their respective groups as X:\
7. Configure DFS replication for all DFS shares.
   (a) Primary DFS: file-srv.paris.local, Replication Server: web-srv.paris.local
8. Shares for DFS namespaces should be created in FILE-SRV and replication shares created on WEB-SRV.

web-srv.paris.local

This machine is preinstalled with Windows Server 2022 (GUI). Ensure the hostname and IP address are configured as per the “Servers and Clients” table.

PKI

1. Configure a Root CA for paris.local on WEB-SRV
2. Enroll certificates for www.paris.local and help.paris.local and distribute them domain wide.

Internet Information Services (IIS)

1. Install and configure the web server running on WEB-SRV
2. Ensure that the web server default site for www.paris.local uses internal.html from the template directory.
3. Create a virtual host for help.paris.local and ensure the page uses help.html from the template directory.
4. Create a virtual host for external.paris.local and ensure the page uses external.html from the template directory.
5. Ensure that HTTP is redirected to HTTPS automatticaly for www.paris.local and help.paris.local

   (a) All users accessing www.paris.local and help.paris.local should not encounter any certificate errors in the edge web browser

paris-router.paris.local

This machine is preinstalled with Windows Server 2022 (GUI). Ensure the hostname and IP address are configured as per the “Servers and Clients” table.

Routing

1. Configure PARIS-ROUTER to serve as default gateway for 10.10.0.0/24, 10.20.0.0/24 and 10.30.0.0/24 subnets

Reverse Proxy

1. Configure PARIS-ROUTER as a reverse proxy for the “external” website hosted on WEB-SRV

Task 3: Lyon Remote Network

lyon-router.lyon.paris.local

This machine is preinstalled with Windows Server 2022 (GUI). Ensure the hostname and IP address are configured as per the “Servers and Clients” table.

Routing

1. Configure LYON-ROUTER as network default gateway for 10.40.0.0/24.

DHCP

1. Configure a DHCP server on LYON-ROUTER and configure the following DHCP range

- DHCP range for 10.40.0.0/24
- Default gateway: 10.40.0.1
- DNS: 10.40.0.10
- Lease: 10.40.0.100 – 200
- Scope name: client
- Exclude: 10.40.0.100 – 150
- Duration: 13 days, 13 hours, 13 minutes

dc2.lyon.paris.local

This machine is preinstalled with Windows Server 2022 (GUI). Ensure the hostname and IP address are configured as per the “Servers and Clients” table.

Active Directory Domain Service

1. Create a new active directory child domain

   (a) Child Domain: lyon.paris.local

2. Join the Windows servers located in the Lyon Remote net to the domain lyon.paris.local
3. Create the following organization units (OU):

   (a) REMOTE

4. Create following AD group under their corresponding OU:

   (a) REMOTE

5. Create the following users according to the table.

USER PREFIX	NUMBERS	PASSWORD	OU	GROUP MEMBERSHIPS
remote	1 – 20	<<Default Password>>	REMOTE	REMOTE

Task 4: ISP Routing

LA-Router

The LA-ROUTER server is preinstalled with Windows Server 2022 with GUI.

1. Configure the server with the settings specified in the diagram at the top of the document.

- DO NOT join the server to any domain, leave the server in a workgroup.

2. The name of host is LA-Router, and workgroup: ISP.

Domain Name Services (DNS)

1. Install DNS, create a forward zone for “paris.com” and add the following record:

RECORD	IP ADDRESS
external	20.0.0.2

2. The website external.paris.com should be accessible from LA-Router Microsoft Edge browser.

Routing

1. Install routing services on LA-ROUTER server and make sure it is the default gateway for the 20.0.0.0/24 network with the allocated 20.0.0.1 address, and 30.0.0.0/24 network with the allocated 30.0.0.1 address.
2. Make sure PARIS-ROUTER & LYON-ROUTER can reach other (e.g. ping).

Task 5: VPN

1. Set up a IKEv2 IPsec Site-to-Site VPN tunnel between the locations PARIS and LYON using the machines PARIS-ROUTER and LYON-ROUTER.

- Named interface: IKEv2
- Username: Administrator
- Domain: PARIS
- Password: Skill39@Lyon
- Pre-Shared-Key: AllTooWell13@
- Set Persistent Connection

2. Make sure that all subnets in PARIS can reach the network in LYON and vice versa.

Task 6: Paris and Lyon Client Network

1. Install Windows 11 on WIN-CLIENT1 and WIN-CLIENT2 machines
2. Ensure each client computer obtains an IP address automatically from the respective DHCP servers
3. Join WIN-CLIENT1 and WIN-CLIENT2 machines to their respective domains.

Task 7 (Automation)

ErasTour24 has requested to create an additional Windows share, but you are fed up to create another one manually as they were requesting new Windows Share in a daily basis. You have decided to use Ansible to manage these project shares. For convenience reason, you are using a Debian machine called ANSIBLE-SRV to run the Ansible playbooks. VS Code and Zeal Docs with Ansible offline docs are ready to use on ANSIBLE-SRV

Your colleague wrote a script, which exported the file shares and the corresponding AD groups as a YAML file (/opt/ansible/inventory/group_vars).

The variable "file_shares" holds a list of file shares and their corresponding AD groups for the NTFS permission. The attribute "name" contains the Windows file share name, the attributes "read" & "write" hold the AD group for the corresponding NTFS permission.

This information is available as Ansible group variables. In addition, he prepared the Ansible environment and the Ansible inventory under /opt/ansible/inventory/ansible_hosts.

1. Initialize a git repository in /opt/ansible/
2. Create an Ansible playbook called /opt/ansible/manage-shares.yaml on ANSIBLE-SRV to manage Windows shares

   (a) Create the domain AD groups used to control the access to the project shares
   (b) Create the file shares on the corresponding server
   (c) For Paris on FILE-SRV and for LYON on DC2
   (d) Configure the NTFS permissions on the file shares corresponding to the defined values in the group variables.
   (e) The key "read" means ReadAndExecute and the key "write" means Modify
   (f) Use FILE-SRV to create file shares located in PARIS and DC2 for shares in LYON. Create the project shares under the folder C:\project_share
   (g) Give "Everyone" full file share permission on the Windows shares
   (h) Make sure that the Ansible playbook can run without entering any credentials. The experts will execute the playbook within the /opt/ansible/ folder as follows: ansible-playbook manage-shares.yaml

3. Create a git commit with the message "final commit" with all your changes.