PERTANDINGAN KEMAHIRAN KOLEJ VOKASIONAL
PERINGKAT KEBANGSAAN 2024

BIDANG_IT_NETWORK SYSTEMS ADMINISTRATION

SOALAN PRAKTIKAL

MASA : 6 JAM

NAMA: _____

NO K/P: _____

INSTITUSI: _____

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! The machines involved in the automation except MGMT will be reverted to initial state for marking purposes. The default configuration for Cisco devices is included.

Set all user password and credential with Skills39 unless being specifically stated with password.
Please use the information below for all the servers and clients.

This Test Project Proposal consists of the following documentation/files:

- ITNSA-KVSkills2024.pdf
- debian-12.5.0-amd64-DLBD-1.iso
- hosts
- ansible.cfg
- AD-Users.csv

LOGIN

Username Linux:	root / itnsa
Username Windows:	Administrator / itnsa
Username Cisco:	itnsa
Password:	Skills39

All VMs and devices are connected to the management network (10.1.1.0/24) and have a statically configured IP address. The management network will be used for configuring the different hosts. You can login using username and password over SSH or WINRM. You may install any additionally required packages and features on the VMs. The ISO for Debian is included.

System Configuration

Region/timezone:	Asia / Kuala Lumpur
Locale:	English US (UTF-8)
Key Map:	English US

When tasked with configuring SSL or TLS, you use certificates server in the topology. If unable to do so, you can use a self-signed-certificate but you will lose some mark. Please take care to hide any warnings.

Description of project and tasks

You are the IT consultant responsible for KVSKILLS2024 and you have been tasked with implementing a complex IT-environment.

PART A: WINDOWS SERVER

Work Task DC Server
NOTE: Please use the default configuration if you are not given the details.

- This server is already preinstalled (Windows Server 2019 with GUI)
- Configure the server with the settings specified in the diagram at the end of the document
- Modify the default Firewall rules to allow ICMP (ping) traffic

Active Directory Domain Service (ADDS)

- Install and Configure Active Directory Domain Services
  - Set this server as the primary domain controller and Global catalogue for **KVSkills.my**
- Create the following Organizational Units:
  - Managers
  - Competitors
  - Visitors
- Create the following Global AD Groups:
  - KV-Managers
  - KV-Competitors
  - KV-Visitors
- Import users from AD-Users.csv file located in C:\ on DC server.
  - Account placed in appropriate OU
  - Accounts is enabled with all properties in CSV file
  - User principalname with @KVSkills.my suffix
  - User is not required to change password at first login.
  - All users have to use "\\CORE\homes\%username%" as their home drive. Use G:\ as drive letter.

Domain Name System (DNS)

- Install and configure DNS Service
  - Create also a reverse zone for the internal subnet
  - Create static A and PTR records for all servers of KVSkills.my domain
  - Create CNAME records required by services
  - Make sure client able to communicate to mypolcc.my domain
- Configure conditional forwarder with itnsa.my
- Configure records for NCSI server for internet simulation (msftncsi.com, msftconnecttest.com)

Active Directory Certificate Services (ADCS)

- Install and configure Certificate Service
- Install only the "Certificate Authority"
- Create a standalone root certificate with the following properties
  - Common Name = KVSkills-CA
  - Organization Name = KVSkills Malaysia
  - Country Code = MY

GPO

- Install and Configure Policy Management
- Setup the following settings:
    - All users should receive a login banner that reads
        - Title: ”Welcome to KVSkills 2024”
        - Message: ”Only authorized personnel allowed to access”
        - Prohibit this message on all servers!!!
- Disable all first sign-in animation for first time login users.
- Map the shared folder of H:\shares from CORE as shared drive with the letter I:
- Autoenrollment of the ”KV-ClientServerCert” Certificate to all clients and servers

Work Task CLIENT
NOTE: Please use the default configuration if you are not given the details.

- This client is already preinstalled (Windows 10 Enterprise Edition)
- Configure the client with the settings specified in the diagram at the end of the document
- Modify the default Firewall rules to allow ICMP (ping) traffic
- Enable and set the local administrator password to **Skills39**
- Join the computer to the **KVSkills.my** domain
- Set the power configuration so the client will never go to sleep while plugged in
- Install outlook/thunderbird and configure mailbox for user KV10
- Send/Reply email to user KV20

PART B: LINUX SERVER

Work Task LNX1 Server
NOTE: Please use the default configuration if you are not given the details.

- The base Debian OS has been set up on LINUX SERVER
- Configure the server with the hostname, domain and IP specified in the appendix

Domain Name System

- Install and configure bind9
- Configure itnsa.my name server
    - Create static A and PTR records for all servers of itnsa.my
    - Create CNAME records required by services
- Configure conditional forwarder with KVSkills.my to windows server
- Set the linux server to use own address as DNS server

MAIL

- Install and configure e-mail server (postfix , dovecot)
- Mail User can access webmail using https://mail.itnsa.my
- Create user KV10 to KV20 with password ”Skills39”
- Make sure KV10 to KV20 have access via IMAPS and SMTPS
- Use certificate signed by DC.KVSkills.my server for SSL/TLS encryption
- Use Client Certificate Authentication in addition for IMAP and SMTP services

PART C: NETWORK

SWITCH

- Configure a vlan based on information in IP addressing table
- Create trunking port between switches. Set access port for client endpoints
- Only configure manual for SW1 and SW2 as SW3 will be managed by ansible.
- Configure LACP for link between SW1, SW2 and SW3
    - SW2 will be in passive mode for both link to SW1
- Configure the Virtual Trunking Protocol (VTP)
    - Set the SW2 as VTP server. The others switch will be the VTP Client.

VTP Domain	KVSkills.my
VTP Password	Skills39
VTP Version	3

VLAN10	NAME: SRV
VLAN20	NAME: LAN
VLAN99	NAME: MGMT

PART D: AUTOMATION USING ANSIBLE

Basic Configuration

1. Install and setup Ansible on the involved hosts in the topology. There is a preconfigured hosts file given that contains the onformation of every host. DO NOT CHANGE THIS FILE.
2. Create a folder at /data/ansible for the tasks configuration. All playbooks should be on the root of the directory /data/ansible on MGMT VM. Feel free to add or create any file/folder for running the playbook.
3. For marking, all playbooks will be run in order from each part's respective directory using the command " ansible-playbook *playbookname.yml* " .
4. All tasks should have state of "ok" or "skipped" even after running for more than one time.
5. "All hosts" will be reffering to the devices of LNX2, CORE, HQ, ISP, SW3

00-facts.yml

- Create a plaubook called 00-facts.yml to test the connectivity of devices on all hosts.
    - Configure to test to all connection to all hosts (ping, ios_facts, win_ping)

01-hostname.yml

- Create a playbook called 01-hostname.yml for configuring hostname and domain name.
    - All hosts should received the hostname based on the "hostname" variable include in the hosts file.
    - Linux hosts should have the domain name of itnsa.my
    - Network devices should have the domain name of KVSkills.my

02-ipaddress.yml

- Create a playbook called 02-ipaddress.yml for configuring IP address.
    - Configure IP address for all hosts based on the IP address table including the sub-interfaces.
    - Configure primary DNS server address.
    - **DO NOT** modify the Management network interfaces.

03-switch.yml

- Create a playbook called 03-switch.yml for configuring switching
    - Configure LACP for link between SW1 and SW2 from SW3
        - SW3 will be in passive mode for both link
    - Create trunking ports between switches.
    - Configure to enable VTP client

04-ospf.yml

- Create a playbook called 04-ospf.yml for configuring routing using OSPF.
    - Configure OSPF for the network, use OSPF 100 and area 0 by default
        - Make sure all virtual machines in network can communicate with each other.
        - **DO NOT** advertise management network
        - Protect OSPF link with md5 authentication using password ”Skills39”

05-net-dhcp.yml

- Create a playbook called 05-net-dhcp.yml for configuring DHCP for client subnet on router.
- Create DHCP scope with the following parameter
    - Range: 192.168.20.120/24 – 192.168.20.150/24
    - Set appropriate value for scope options of DNS and Gateway

06-adds.yml

- Create a playbook called 06-adds.yml for installation of Active Directoty Domain Services
    - Configure CORE as the secondary domain controller (No Global Catalogue)

07-files.yml

- Create a playbook called 07-files.yml for configuring file sharing on Windows
    - Configure the RAID 5 for the disk. The three 1G disk is should be installed on the VM.
        - Format the disks as NTFS and mount the drive as H:\
    - Configure the file share of home folder.
        - Create a directory with the local path of H:\homes and share folder
        - Create a directory with the local path of H:\shares and make it publicly accessible

08-lnxweb.yml

- Create a playbook called 08-lnxweb.yml for configuring the Apache Web Server services.
    - Make the webpage is secured with TLS/SSL certificated generated from ADCS

- The website on LNX2 with URL of https://www.itnsa.my showing the hostname of server.
- ”<h1> Welcome to the ITNSA.MY </h1>”

09-ftp.yml

- Create a playbook called 09-ftp.yml for configuring the ftp service.
  - Install and configure vsftpd in Linux
  - Create user ftpuser with password of Skills39
  - Make sure the users are jailed in their respective home directory
  - Use certifcate generate by ADCS

10-net-backup.yml

- Create a playbook called 10-net-backup.yml to save and backup all of the configurations of network devices.
  - Create a folder at /data/ansible/backup. Save the configuration in the folder with the format ”{{hostname}}.cfg”
  - Make sure every network devices configuration is saved.

NETWORK ADDRESS TABLE

Device	Operating System	Interface	Address
DC	Windows Server 2019 (GUI)	Ethernet 1	172.16.10.10 /24
CORE	Windows Server 2019 (Core)	Ethernet 1	172.16.10.11 /24
LNX1	Debian 12.5 CLI	Ethernet 0	172.16.20.10 /24
LNX2	Debain 12.5 CLI	Ethernet 0	172.16.20.11 /24
CLIENT	Windows 10 Enterprise	Ethernet 0	192.168.20.XXX /24 (DHCP)
HQ	Cisco vIOS Router	GigabitEthernet 0/1.10	172.16.10.254 /24 (SRV)
		GigabitEthernet 0/1.20	192.168.10.254 /24 (LAN)
		GigabitEthernet 0/1.99	172.16.99.6 /29 (MGMT)
		GigabitEthernet 0/0	24.48.72.1 /28
		Loopback 100	1.1.1.1 /32
ISP	Cisco vIOS Router	GigabitEthernet 0/0	24.48.72.14 /28
		GigabitEthernet 0/1	172.16.20.254 /24

		Loopback 100	2.2.2.2 /32
SW1	Cisco vIOS Switch L3	VLAN 99	172.16.99.1 /29
SW2	Cisco vIOS Switch L3	VLAN 99	172.16.99.2 /29
SW3	Cisco vIOS Switch L3	VLAN 99	172.16.99.3 /29
SW4	GigabitEthernet 0/1 -0/3	VLAN 30	172.16.20.0/24

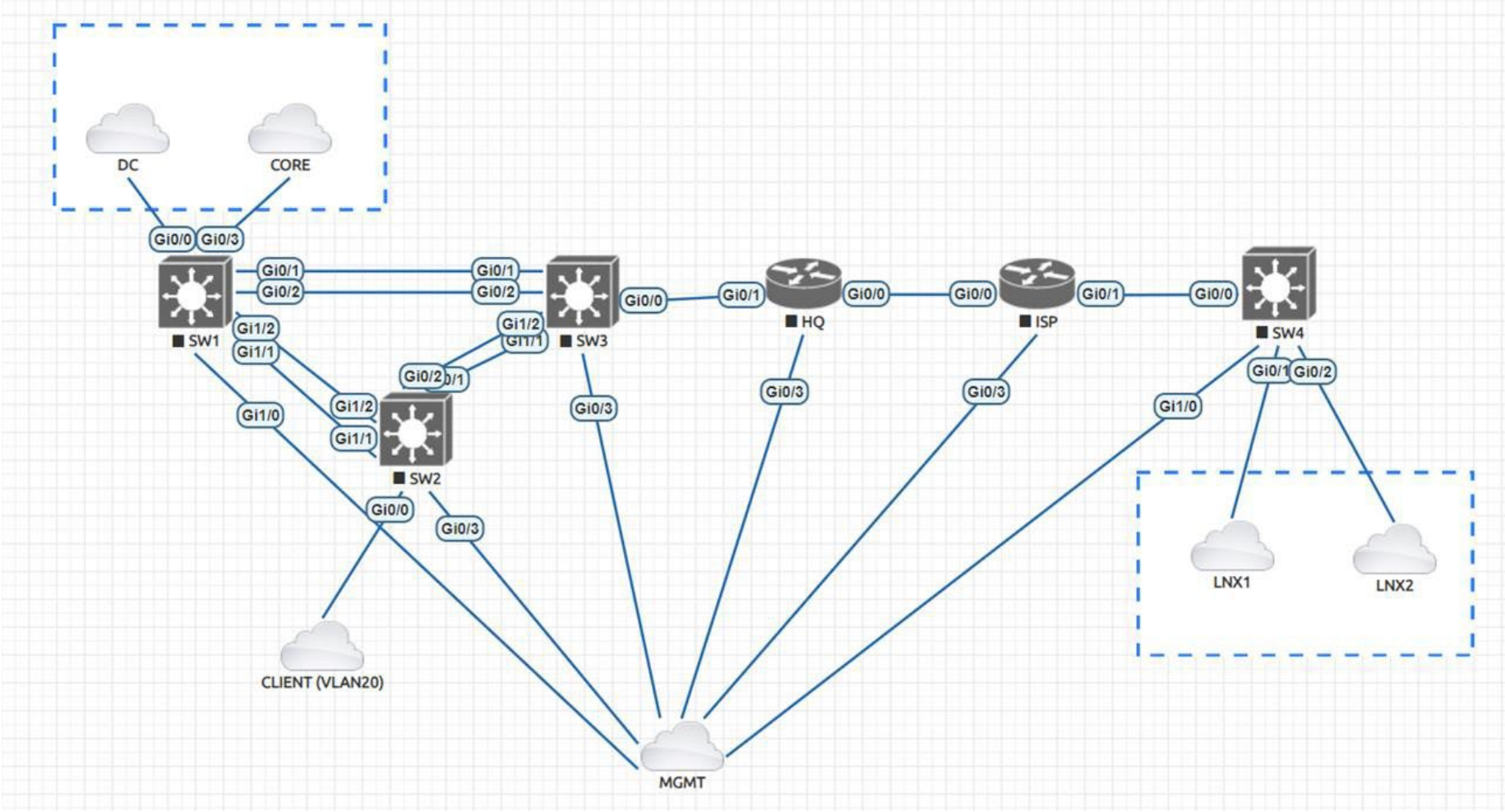
MANAGEMENT NETWORK ADDRESS TABLE

Device	Address
DC	10.1.1.11 /24
CORE	10.1.1.12 /24
LNX1	10.1.1.21 /24
LNX2	10.1.1.22 /24
SW1	10.1.1.31 /24
SW2	10.1.1.32 /24
SW3	10.1.1.33 /24
SW4	10.1.1.34 /24
HQ	10.1.1.41 /24
ISP	10.1.1.42 /24
MGMT	10.1.1.10 /24

INSTRUCTIONS TO THE COMPETITOR

- Warning: **SAVE ALL YOUR CONFIGURATIONS!!!** Every device will be rebooted before marking.
- Do not bring any materials with you to the competition.
- Mobile phones and any electric devices are prohibited.
- Do not disclose any competition material / information to any person during each session's competition.
- Read the whole competition script prior to starting your work.
- Be aware of different tasks attract a percentage of the overall mark. Plan your time carefully.

TOPOLOGY


DC
CORE
Gi0/0
Gi0/3
SW1
Gi0/1
Gi0/2
Gi1/2
Gi1/1
Gi1/0
SW2
Gi0/0
Gi0/3
CLIENT (VLAN20)
SW3
Gi0/0
Gi0/3
HQ
Gi0/1
Gi0/0
Gi0/3
ISP
Gi0/0
Gi0/1
Gi0/3
SW4
Gi0/0
Gi0/1
Gi0/2
Gi1/0
LNX1
LNX2
MGMT

PRE-CONFIG

/etc/ansible/ansible.cfg

```
[defaults]
inventory=/etc/ansible/hosts
remote_user=root
host_key_checking=False
become=True
become_user=root
become_ask_pass=False
ansible_python_interpreter=/usr/bin/python3
```

==========

/etc/ansible/hosts

```
all:
  hosts:
    #Linux Hosts
    LNX1:
      ansible_host: 10.1.1.21
      hostname: "LNX1"
      network_addr: "172.16.20.10"
      webmessage: "<h1><center>Welcome to the world of automation with ansible"
      webcolor: "red"
    LNX2:
      ansible_host: 10.1.1.22
      hostname: "LNX2"
      network_addr: "172.16.20.11"
      webmessage: "<h1><center>How exciting to deploy services using automation"
      webcolor: "green"
    #Windows Hosts
    WIN1:
      ansible_host: 10.1.1.11
      hostname: "DC"
      network_addr: "172.16.10.10"
    WIN2:
      ansible_host: 10.1.1.12
      hostname: "CORE"
      network_addr: "172.16.10.11"
    #Cisco Switch Hosts
    RTR1:
      ansible_host: 10.1.1.41
      hostname: "HQ"
    RTR2:
      ansible_host: 10.1.1.42
      hostname: "ISP"
    SW1:
      ansible_host: 10.1.1.31
      hostname: "SW1"
    SW2:
      ansible_host: 10.1.1.32
      hostname: "SW2"
    SW3:
      ansible_host: 10.1.1.33
      hostname: "SW3"
    SW4:
      ansible_host: 10.1.1.34
      hostname: "SW4"
  children:
    linux:
      hosts:
        LIN1:
        LIN2:
    windows:
      hosts:
        WIN1:
        WIN2:
    cisco:
      children:
        routers:
          hosts:
            RTR1:
```

```
        RTR2:
    switches:
      hosts:
        SW1:
        SW2:
        SW3:
        SW4:
```

"/etc/ansible/group_vars/cisco"

```
ansible_user: itnsa
ansible_ssh_pass: Skills39
ansible_password: Skills39
ansible_become: yes
ansible_become_method: enable
ansible_connection: network_cli
ansible_network_os: cisco.ios.ios
ansible_network_cli_ssh_type: libssh
```

==========

"/etc/ansible/group_vars/linux"

```
ansible_user: root
ansible_password: Skills39
ansible_become: true
ansible_become_method: su
ansible_become_password: Skills39
```

==========

"/etc/ansible/group_vars/windows"

```
ansible_user: Administrator
ansible_password: Skills39
ansible_connection: winrm
ansible_winrm_server_cert_validation: ignore
ansible_ssh_port: 5986
```

==========

CISCO PRE-CONFIG

```
hostname DSW1
ip domain name example.net
username itnsa privilege 15 secret Skills39
crypto key generate rsa general-keys modulus 2048 label BOOTKEYS
ip ssh version 2
line vty 0 530
        transport input ssh
        login local
ip http secure-server
ip http authentication local
interface GigabitEthernet 1/0
no sw
ip address 10.1.1.31 255.255.255.0
no shutdown
exit

hostname DSW2
ip domain name example.net
username itnsa privilege 15 secret Skills39
crypto key generate rsa general-keys modulus 2048 label BOOTKEYS
ip ssh version 2
line vty 0 530
        transport input ssh
        login local
ip http secure-server
ip http authentication local
interface GigabitEthernet 0/3
no sw
ip address 10.1.1.32 255.255.255.0
no shutdown
```

```
exit

hostname DSW3
ip domain name example.net
username itnsa privilege 15 secret Skills39
crypto key generate rsa general-keys modulus 2048 label BOOTKEYS
ip ssh version 2
line vty 0 530
        transport input ssh
        login local
ip http secure-server
ip http authentication local
interface GigabitEthernet 0/3
no sw
ip address 10.1.1.33 255.255.255.0
no shutdown
exit

hostname DSW4
ip domain name example.net
username itnsa privilege 15 secret Skills39
crypto key generate rsa general-keys modulus 2048 label BOOTKEYS
ip ssh version 2
line vty 0 530
        transport input ssh
        login local
ip http secure-server
ip http authentication local
interface GigabitEthernet 1/0
no sw
ip address 10.1.1.34 255.255.255.0
no shutdown
exit

hostname DRTR1
ip domain name example.net
username itnsa privilege 15 secret Skills39
crypto key generate rsa general-keys modulus 2048 label BOOTKEYS
ip ssh version 2
line vty 0 530
        transport input ssh
        login local
ip http secure-server
ip http authentication local
interface GigabitEthernet 0/3
ip address 10.1.1.41 255.255.255.0
no shutdown
exit

hostname DRTR2
ip domain name example.net
username itnsa privilege 15 secret Skills39
crypto key generate rsa general-keys modulus 2048 label BOOTKEYS
ip ssh version 2
line vty 0 530
        transport input ssh
        login local
ip http secure-server
ip http authentication local
interface GigabitEthernet 0/3
ip address 10.1.1.42 255.255.255.0
no shutdown
exit
```