LOMBA KOMPETENSI SISWA

SEKOLAH MENENGAH KEJURUAN

TINGKAT NASIONAL XXVIII 2020

TEST PROJECT

IT NETWORK SYSTEMS ADMINISTRATION

LKSN2020_WINDOWS_Actual

Contents

Introduction to Test Project

Contents

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

1. LKSN2020_Windows_Actual.docx

This implementation uses nested virtualization and all project VM's are hosted inside a "Host" machine; credentials for the Host machine are **administrator\Skills39**

You are the IT consultant responsible for Skill39. Use the password "**Passw0rd$**"(without quotes) when no specific password has given. Use the password "**Skills39**" for local accounts.

You have inherited a Windows Domain with some users and configurations already set up but have decided to perform further tasks to improve the network. You will need to host a number of websites securely for people inside and outside the domain to access. In order to do this, you have decided to provide a high availability system based on Hyper-V amongst other improvements. You will use this Hyper-V infrastructure to improve the server infrastructure in the existing domain. Please follow the instructions that follow to complete the project.

Description of project and tasks

Part 1. Intranet

You need to upgrade the infrastructure in the network to the existing domain. Systems will be provided in various states of install and configuration. Make sure all hostnames and IP's etc. are set correctly

DC1– Preinstalled

Configure existing machine to match the requirements

- This server already has Active Directory installed.
- Configure Active Directory.
  - Import users from included csv file. Accounts should be enabled, have the properties listed in the csv, including group membership, and NOT be required to change password at first login.
- Configure DNS service.
  - Create all appropriate A records for all servers on 192.161.139.0/24 subnet.
  - Create all appropriate CNAME records according to the tasks.
    - A record of 192.161.139.101
      - adfs
    - CNAME record of dc2.garuda.id:
      - work
    - CNAME records of web.garuda.id:
      - csweb, www, intra, extra
  - Configure root hint as "ns.msftncsi.com" and remove other root hints.
  - Create a reverse lookup zone creating PTR records for all servers.
- Configure DHCP service.
  - Configure failover scope with DC2 once it is installed. Set DC1 as the active server.
  - Total scope Range: 192.161.139.51 - 192.161.139.75
  - Give DC1 70% of this scope to DC1, and the rest to DC2
  - Configure the failover to use Hot Standby mode
  - Scope Options
    - DNS: 192.161.139.1, 192.161.139.101, Gateway: 192.161.139.254

- Configure Network Policy Server to authorize network access for VPN-connected users.
  - Users in the Competitor group are not allowed to connect to VPN server.
  - Agents and Experts can use VPN connection by username and password.
- Configure and apply the following group policies:
  - Create a GPO called “banner” that will ensure that all users will be greeted with a login banner that says “Welcome to Skill 39”.
  - Create a GPO policy called “work” which will automatically connect the work folder when "Experts" group members logged on.
- Create and share a C:\backups folder as \\DC1\Backups\
  - Create a backup job to backup all users home folders located on DC2 at 4 PM daily.
  - Make sure the backup job is written to the event log.

DC2

Configure to match the following requirements

- Rename, and Set IP address according to configuration table and network diagram at end of project.
- Configure this server as a second domain controller for the garuda.id domain.
- Configure DNS service.
  - The records of Active Directory-Integrated zones should be replicated.
- Configure DHCP service.
  - Configure failover scope - refer to the description for DC1.
- Configure Active Directory Federation Service.
  - This server provides federation service.
  - URL: "https://adfs.garuda.id"
  - Display Name: "LKSN2020-Kazan Single Sign-On"
- Add three extra 10G drives
- Format the attached disks with NTFS into a single RAID 5 array (G:\) and enable de-duplication on this volume.
- Create file share for user's home drives.
  - Access URL: dc2.garuda.id\homes
  - Local path: "G:\homes\"

- Configure Work Folders.
  - Access URL: https://work.garuda.id/
  - Local path: "G:\work\"
- Create a file share for each group.
  - Access URL: dc2.garuda.id\WSC
  - Local path: "G:\WSC\"
  - Create three subfolders and configure access control:
    - Junior Skills
      - Allow read-only access for users who have "Junior" as the job title.
      - Allow full access to the users who are also part of the "WSJ" organizational unit and also belong to the "Manager" group.
    - Secret Challenges
      - Allow access only for "Agent" group.
      - This folder should be hidden for the user who has insufficient permission.
    - Public
    - Allow read-only access for domain users.
    - Create a file share for local path G:\witness and share it as \\DC2\witness.

INTCLIENT – BASE Install

Configure to match the following requirements

- Rename, and Set IP address according to configuration table and network diagram at end of project.
- Join to garuda.id domain.
- Use this machine to:
  - Test access to Manager/Intranet/Extranet websites.
  - Test GPOs.
  - Test home and Work Folders.
  - Ensuring users have been imported correctly.

Web

Configure to match the following requirements

- Rename, and Set IP address according to configuration table and network diagram at end of project.
- Install and configure IIS and its websites using given HTML files. (from USB)
  - Use a single certificate that only has "www.garuda.id" as a common name.
  - Configure the "Default Web Site" as described below.
    - Path for website root: "C:\inetpub\intranet\".
    - Enable Windows Internal authentication.
      - Use certificate authentication for "/manager/" subdirectory.
  - Create "https://extra.garuda.id" website with the name "Extranet".
    - Path for website root: "C:\inetpub\extranet\".
    - Enable ADFS web authentication via the Web Application Proxy for clients on the Internet.
  - Create "https://www.garuda.id"website with the name "Public".
    - Path for website root: "C:\inetpub\internet\".
- Configure IP Address and Domain Restrictions.
  - The "https://intra.garuda.id" website can be accessible from: 192.161.139.0/24, 192.168.219.0/24

Part 3. Perimeter and Internet

You need to build a web application proxy and remote access service that allows you to use the internal resources of the domain outside the domain. Follow the instructions to complete the task.

FIREWALL – BASE

Configure to match the following requirements

- Rename, and Set IP address according to configuration table and network diagram at end of project.
- Enable routing.
- Configure DNS server for the public Internet.
  - Create primary zone "garuda.id" and add these A records of 192.161.140.100.
    - ns, vpn, csweb, extra, work.
  - Add an A record "www.garuda.id" of 192.161.139.103
  - SOA record of the "garuda.id" should be "ns.garuda.id".
- Configure Routing and Remote Access Service.
  - Users and computers on the Internet should be able to establish VPN connection to this server.
  - IKEv2 clients can connect to the intranet through this server.
  - Authorize VPN access through the NPS.
  - IP address pool for remote access clients: 192.168.219.1 - 192.168.219.254
- Configure the Web Application Proxy.
  - Clients on the Internet should be able to:
    - Access "https://extra.garuda.id" website after passing the ADFS web authentication.
    - Access "https://work.garuda.id" to use work folders for each user.
    - Configure firewall rules to prevent unauthorized access.
    - Allow HTTPS traffic from 192.161.140.0/24 to 192.161.139.103.
    - Block any other traffics sourced from 192.161.140.0/24 to 192.161.139.0/24.

REMCLIENT - BASE

Configure to match the following requirements

- Rename, and Set IP address according to configuration table and network diagram at end of project.
- Join in garuda.id domain through VPN.
- Configure the Always-on VPN/Device tunnel.
    - Domain users should be able to log in via this tunnel.
    - Only the dc1 and dc2 can be accessed through this tunnel (not other servers/resources).
- Deploy App-triggered VPN.
- Create an IKEv2 VPN connection named "AppVPN" for "Managers" group members only that automatically connects to "vpn.garuda.id" when a member of the Managers group runs Internet Explorer."
- After connection to the VPN, the user should have access to all resources of the intranet.
- Use bitlocker to encrypt the drive of REMCLIENT. Save the bitlocker recovery key to your USB.

PUBCLIENT – NOT INSTALLED

Install/Configure

- Install, rename, and set IP address according to configuration table and network diagram at end of project.
- Do not join this client to the domain.
- Set the firewall on this machine to allow inbound and outbound “ping” traffic.
- Set the power settings to “never sleep”.
- Test Work Folders service is available via "https://work.garuda.id".
    - ADFS web authentication should be work.
    - Work Folders should be accessible and writable.
- Create an IKEv2connection "LKSN2020-VPN" for test purpose and make don't remember credential.

INET

Configure to match the following requirements

- Host NCSI website.

    - Clients on the Internet should indicate network connection as the "Internet".
- Configure DNS server.
    - Create zones and records for NCSI.
    - Add an A record "cs.msftncsi.com" of 192.161.140.1.
    - Add an A record "ns.msftncsi.com" of 192.161.140.1.
    - SOA record of the "msftncsi.com" should be "ns.msftncsi.com".
    - Create a root zone(.) to simulate the root DNS server.
        - Create appropriate delegations to resolve DNS records.
- Configure DHCP service.
    - Range: 192.161.140.151 - 192.161.140.175
    - DNS: 192.161.140.1
    - Gateway: 192.161.140.100
- Configure the Certification Authority.
    - Common name: ISP-CA
    - Enable extensions for CDP and AIA URL through HTTP.
        - URL for CDP: http://cs.msftncsi.com/CertEnroll/ISP-CA.crl
        - URL for AIA: http://cs.msftncsi.com/CertEnroll/ISP-CA.crt

Create these templates:

- "_ID_Server"
    - To provide a certificate for servers/services in garuda.id domain.
- "_ID_Client"
    - To provide a certificate for clients.

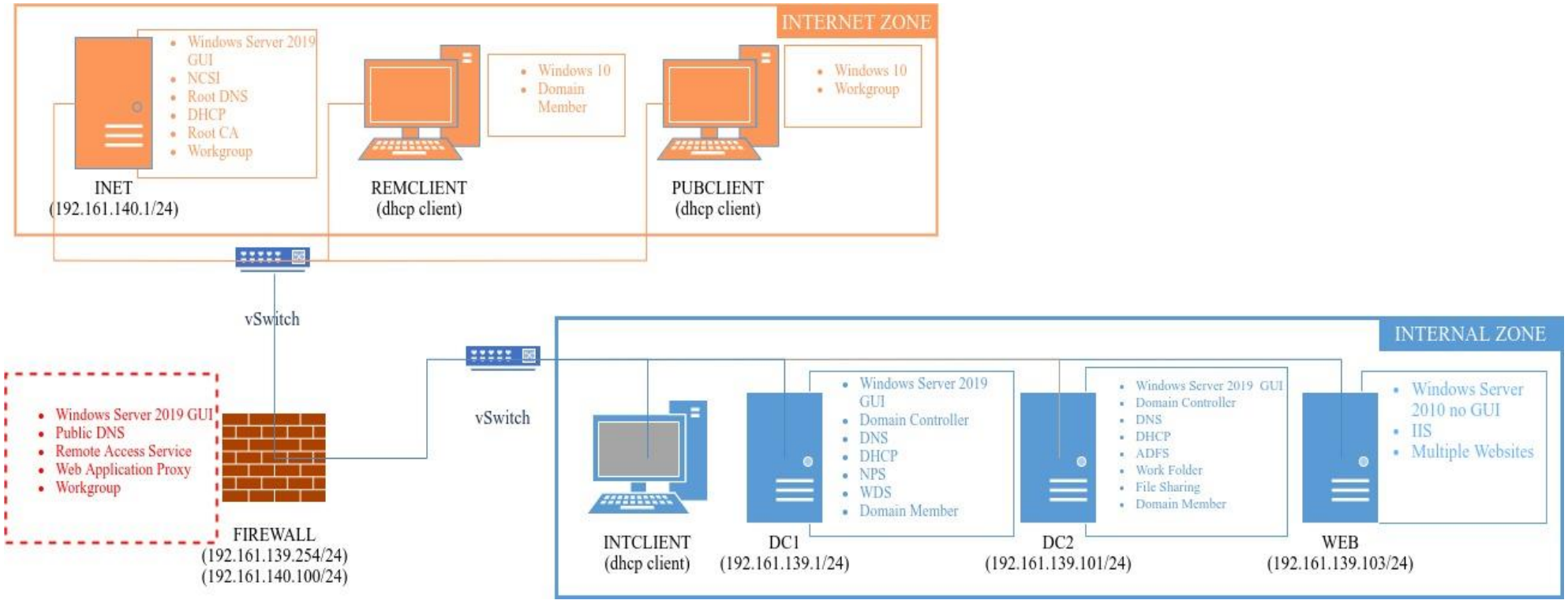
Appendix

Configuration Table

Hostname	Operation System	Domain	IP Address(es)	Preinstalled
DC1	Windows Server 2019Desktop	garuda.id	192.161.139.1	Yes
DC2	Windows Server 2019Desktop	garuda.id	192.161.139.101	Yes
INTCLIENT	Windows 10 Enterprise	garuda.id	DHCP	Yes
WEB	Windows Server 2019Core	garuda.id	192.161.139.103	Yes
FIREWALL	Windows Server 2019Desktop	WORKGROUP	192.161.139.254 192.161.140.100	Yes
REMCLIENT	Windows 10 Enterprise	garuda.id	DHCP	Yes
PUBCLIENT	Windows 10 Enterprise	WORKGROUP	DHCP	Yes
INET	Windows Server 2019Desktop	WORKGROUP	192.161.140.1	Yes

Machines indicated as being preinstalled with "**Yes**" will have the operating system installed.

Topology


INTERNET ZONE
Windows Server 2019 GUI
NCSI
Root DNS
DHCP
Root CA
Workgroup
INET
(192.161.140.1/24)
Windows 10
Domain Member
REMCLIENT
(dhcp client)
Windows 10
Workgroup
PUBCLIENT
(dhcp client)
vSwitch
Windows Server 2019 GUI
Public DNS
Remote Access Service
Web Application Proxy
Workgroup
FIREWALL
(192.161.139.254/24)
(192.161.140.100/24)
vSwitch
INTERNAL ZONE
INTCLIENT
(dhcp client)
Windows Server 2019 GUI
Domain Controller
DNS
DHCP
NPS
WDS
Domain Member
DC1
(192.161.139.1/24)
Windows Server 2019 GUI
Domain Controller
DNS
DHCP
ADFS
Work Folder
File Sharing
Domain Member
DC2
(192.161.139.101/24)
Windows Server 2010 no GUI
IIS
Multiple Websites
WEB
(192.161.139.103/24)