Test Project

IT Network System Administration

Module B – Windows Environment

Submitted by:

Contents

Introduction to Test Project

Contents

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

1. WSC2021_TP39_ModuleB_PRA_TC_ID
2. WSC2021_TP39_ModuleB_PRA_TC_ID_Users.xlxs
3. profileXML.ps1
4. profileXML.xml
5. Import-BulkUserFromCsv.ps1
6. Extra.html, DC.html, Public.html, Manager.html

These files can be found in C:\ModuleB on DC1.

This implementation uses nested virtualization and all project VM's are hosted inside an ESXI machine; credentials for the ESXI machine are **root\[secret]**

You are the IT consultant responsible for Skill39. Use the password "**P@ssw0rd**" without quotes) when no specific password has given. Windows server **administrator/P@ssw0rd**, Windows client local account **competitor/P@ssw0rd**.

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 migrate DC2 to the Cloud. Please follow the instructions that follow to complete the project.

Description of project and tasks

Part 1. DC – On-premises

You need to upgrade the infrastructure in the network to the existing domain. Systems will be provided in various states of install and configuration. Examine the diagrams at the end of this project and the VM Configuration Table for clarification. Some of the tasks will need to be completed after all of the infrastructure and servers have been added, be sure to return to the earlier tasks to make sure you have completed all requirements.

NOTE –We have tried hard to make sure all hostnames and IP's etc. are set correctly, and believe this to be the case, but you are still responsible to verify the machine configuration matches what is required in the test project. If you have difficulty or are unable to configure or work with a machine which is a "Core" server with no GUI, you may re-install any machine as a server with the "desktop experience" at a small marking penalty (and of course – the time it takes to carry out the install).

DC1–Preconfigured

Configure existing machine to match the requirements

- Verify server name and IP matches that in the configuration table and diagram at the end of this document.
- This server is pre-configured as the domain controller of wsc2021.cn.
- Configure Active Directory.
- **Active Directory.**
  - Fix the PowerShell script from C:\ModuleB\ on DC1 and import users from included csv file supplied from this folder. Accounts should be enabled, have the properties listed in the spreadsheet including group membership, userprincipalname with a @wsc2021.cn suffix, be placed into the appropriate OU, and NOT be required to change password at first login.
- **Configure DNS service.**
  - Add the following records in addition to the domain joined servers.
  - A record of 20.20.1.101
    - adfs
  - CNAME record of dc2.wsc2021.cn:
    - work
  - CNAME records of web.wsc2021.cn:
    - csweb, www, dc, 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.**
  - Total scope Range: 20.20.1.51 - 20.20.1.75
  - Scope Options
    - DNS: 20.20.1.1, 20.20.1.101, Gateway: 20.20.1.254
    - Enable DHCP scope protection so that if DHCP service is restarted. The DHCP configuration will be restored to previous backup state.

- **Configure Network Policy Server** to authorize network access for VPN-connected users..
  - Users who are member of the Agents and Experts groups can create VPN connection by using 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 called “managers” to automatically issue a certificate for the "Manager" group members using the _RU_Managers template.
  - Create a GPO policy called “work” which will automatically connect the work folder when "Experts" group members logged on.

    N.B. Create another GPOs if needed so all services in this domain will work as expected.
- Create and share a C:\backups folder as\\DC1\Backups.
- Create a “Public” folder at C:\Public and Share it as “Public”.
  - Allow read-only access for domain users.

- **Install and configure the Certification Authority service.**
- Certification Authority service.
  - Use certificate issued from "CORE-CA".
  - Common Name: "WSC2021-CA".
  - Enable extensions for CDP and AIA URL through HTTP.
  - URL for CDP: http://cert.wsc2021.cn/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
  - URL for AIA: http://cert.wsc2021.cn/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
- Create the following templates:
  - "_RU_Manager"
    - For users in the "Manager" group.

- “Manager”
- "_RU_Server"
  - To provide a certificate for servers/services in wsc2021.cn domain.
- "_External_Client"
  - To provide a certificate for computers on the Internet.
  - Enable key-based renewal.
  - Enable certificate manager approval to issue a certificate.

INTCLT

Configure to match the following requirements

- Verify host name and IP configuration matches the configuration table and diagram at the end of this document.
- Join to wsc2021.cn domain.
- Use this machine to:
  - Test access to Manager/DC/Extranet websites.
  - Test GPOs.
  - Test home and Work Folders.
  - Ensuring users have been imported correctly.

Part 2. CLOUD

You have completed the core domain infrastructure configuration.

You now need to migrate DC2 to the CLOUD.

Follow the instructions given to complete the task.

DC2 – CLOUD

Configure to match the following requirements

- Verify server name and IP matches that in the configuration table and diagram at the end of this document.
- Configure this server as a second domain controller for the wsc2021.cn domain.

DNS

- Configure DNS service.
  - Use an Active Directory-Integrated zone.
  - Configure root hint as "ns.msftncsi.com" and remove other root hints.

ADFS

- Configure Active Directory Federation Service.
- Active Directory Federation
  - This server provides federation service.
  - URL: "https://adfs.wsc2021.cn"
  - Display Name: "WSC2021-China Single Sign-On"

FILE SHARING

- Add three extra 5G 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 UNC path: \\dc2.wsc2021.cn\homes
  - Local path: "G:\homes\"
  - Limit home folders so that users can not store more than 10 MB of data and cannot save bitmap (*.bmp) files.
- Create a backup job to backup all users home folders located on DC2 at 4 PM daily.
- Configure Work Folders.
- Work Folders
  - Access URL: https://work.wsc2021.cn/
  - Local path: "G:\work\"
- Create a file share for local path G:\witness and share it as \\DC2\witness.
- Create file share for local path G:\WSC and share it as \\DC2\WSC.
  - Create two subfolders inside G:\WSC\ and share and configure access control on each folder as follows:

- Create a “Junior Skills” folder.
- “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.
- Create a “Secret Challenges” folder.
  - Allow modify access only for "Agent" group.
  - This folder should be hidden for all users who have insufficient permission to access the folder.

DFS

- Install and configure DFS so that the “WSC” share and “Public” share from DC1 are accessible by accessing \\wsc2021.cn\shares.

WEB

- Install and configure IIS and its websites using given HTML files. (from C:\ModuleB on DC1)
  - Use a single certificate that only has "www.wsc2021.cn" as a common name.
  - Configure the "Default Web Site" as described below.
- Path for website root: "C:\inetpub\DC\".
- Use the DC.html web file for the default page.
- Enable Windows Internal authentication.
  - Create the folder "C:\inetpub\DC\manager”
  - Add the manager.html to manager subdirectory.
  - Use certificate authentication for "manager" subdirectory.
- Create "https://extra.wsc2021.cn" website with the name "Extranet" using extranet.html webfile.
- Path for website root: "C:\inetpub\extranet\".
- Enable ADFS web authentication via the Web Application Proxy for clients on the Internet.
  - Create "https://www.wsc2021.cn"website with the name "Public" using the public.html webfile.
- Path for website root: "C:\inetpub\internet\".
- Configure Certificate Enrolment Web Service (CES) and Certificate Enrolment Policy Web Service (CEP).
  - URL: "https://csweb.wsc2021.cn" for both CES and CEP.
  - Computers that are not in wsc2021.cn domain should be able to get a certificate through this server.
  - Authentication should be done by username and password.
  - Friendly Name: "WSC2021 Enrollment Policy"
  - Make only "_External_Client" template visible.

- create web virtualhost on port 8080 with a simple html webpage "WFH using Cloud".
- Configure IP Address and Domain Restrictions.
  - The "https://dc.wsc2021.cn" website can be accessible from:20.20.1.0/24, 20.20.70.0/24, and 192.168.219.0/24

Part 3. Perimeter and Internet

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

- Verify server name and IP configuration matches that in the configuration table and diagram at the end of this document.

FW1 – On-Premises

Configure to match the following requirements

- Enable routing.
- Configure DNS server for the public Internet.
  - Create primary zone "wsc2021.cn" and add these A records of 20.20.2.100.
    - ns, vpn, csweb, extra, work.
  - Add an A record "www.wsc2021.cn" of 20.20.1.103
  - SOA record of the "wsc2021.cn" should be "ns.wsc2021.cn".
  - Configure root hint as "ns.msftncsi.com" and remove other root hints.
- 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 DC 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.
- Web Application Proxy
  - Clients on the Internet should be able to:
  - Access "https://extra.wsc2021.cn" website after passing the ADFS web authentication.

- Access "https://csweb.wsc2021.cn" to reach to the Certification Enrolment Policy and Certification Enrolment Service.
- Access "https://work.wsc2021.cn" to use work folders for each user.

- Configure firewall rules to prevent unauthorized access.
  - Allow HTTPS traffic from 20.20.2.0/24 to 20.20.1.103.
  - Block any other traffic sourced from 20.20.2.0/24 to 20.20.1.0/24.

FW2 – CLOUD

- Enable routing.
- Site-to-Site VPN (IKEv2).
- Configure Site-to-Site VPN between FW1 and FW 2.
- Use pre-shared key P@ssw0rd for the authentication.
- Set the connection type to persistent connection.
- All traffic bound for DC and Cloud Network will be placed in the VPN tunnel.
- Configure static NAT DC2:8080<->FW2:80.

REMCLT – Working From Home (WFH)

Configure to match the following requirements

- Join in wsc2021.cn domain through VPN.
- Configure the Always-on VPN/Device tunnel.
  - Domain users should be able to log in via this tunnel.
  - After connection to the VPN, the user should have access to all resources of the DC.
- Create a volume of 100 MB at C:\workfiles and use bitlocker to encrypt the contents of this volume. Save the bitlocker recovery key to C:\bitkey\ on REMCLT. Use a password of “Skills39” for the bitlocker encryption.
- 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.wsc2021.cn".
  - ADFS web authentication should work.
  - Work Folders should be accessible and writable for the Managers group.
- This client should be able to receive a certificate from CES.
  - Create a local Enrolment Policy.
  - Get a certificate which contains CN=PUBCLIENT from CES.
- Create an IKEv2connection "WSC2021-VPN" for test purpose and make don't remember credential.

CORE - ISP

Verify configuration if required

- This machine is preconfigured for your use, if you wish to, you may re-install and configure this machine to these specifications.
- Host NCSI website.
  - Clients on the Internet should indicate network connection as the "Internet".
- Check and configure DNS server.
  - Create zones and records for NCSI.
  - Add an A record "cs.msftncsi.com" of 20.20.2.1.
  - Add an A record "ns.msftncsi.com" of 20.20.2.1.
  - Add an A record “wfh.itnsa.com” of 20.20.2.200.
  - 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.
- Check and configure DHCP service.
  - Range: 20.20.2.151 - 20.20.2.175
  - DNS: 20.20.2.1
  - Gateway: 20.20.2.1
- Check and configure the Certification Authority.
  - Common name: CORE-CA
  - Enable extensions for CDP and AIA URL through HTTP.
  - URL for CDP: http://cs.msftncsi.com/CertEnroll/CORE-CA.crl
  - URL for AIA: http://cs.msftncsi.com/CertEnroll/CORE-CA.crt
  - Issue certificate request for WSC2021-CA.

Configuration Table

Hostname	Operation System	Domain	IP Address(es)	Preinstalled
DC1	Windows Server 2019Desktop	WSC2021.CN	20.20.1.1/24	Yes – Configured as DC
INTCLT	Windows 10 Enterprise	WSC2021.CN	DHCP	Yes
FW1	Windows Server 2019Desktop	WORKGROUP	20.20.1.254/24 20.20.2.100/24	Yes
FW2	Windows Server 2019 Core	WORKGROUP	20.20.2.200/24 20.20.70.254/24	Yes
DC2	Windows Server 2019Core	WSC2021.CN	20.20.70.101/24	Yes
REMCLT	Windows 10 Enterprise	WSC2021.CN	DHCP	Yes
CORE	Windows Server 2019Desktop	WORKGROUP	20.20.2.1/24	Yes – Configured as CORE machine; root CA, ncsi, DNS, and DHCP for the Internet

Machines indicated as being preinstalled with "**Yes - Configured**" will have the operating system installed and pre-configured for Competitor use. Competitors may need to do further configuration to match the specifications laid out in this document.

Machines indicated as "**Yes**" are standard installs which have either had the IP preconfigured, hostnames set, or both to save installation time, services will still need to be installed and configured. These machines SHOULD have the correct names and IP addresses set to them, but you should verify this in all cases.

Instructions to the Competitor

- Do not bring any materials with you to the competition.
- Mobile phones are not to be used.
- Do not disclose any competition material / information to any person during each day's competition.
- Read the whole competition script prior to starting work.
- Be aware different tasks attract a percentage of the overall mark. Plan your time carefully.
- If your virtual machines spontaneously turn off, run slmgr /rearm command with the administrator credentials