**Worldskills Windows-Linux Integration Test**

**Test Paper**

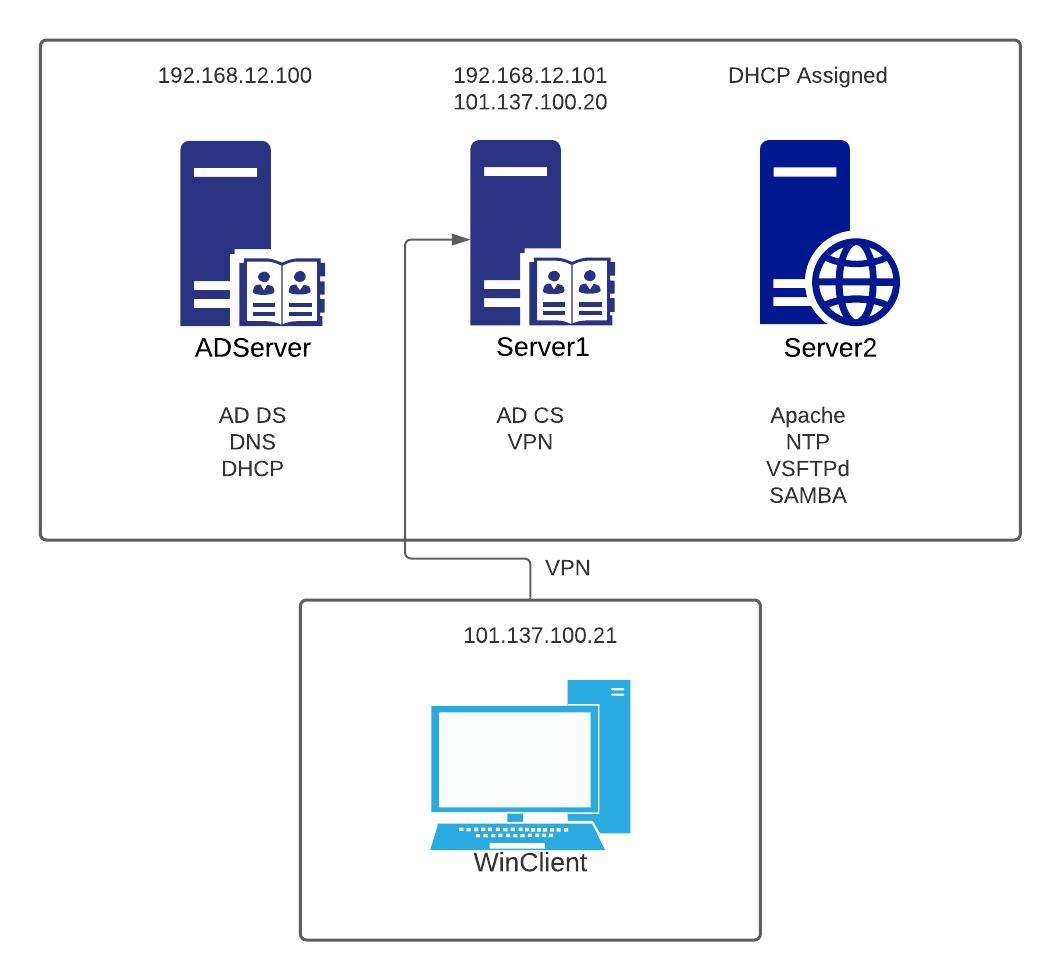
**Task**

Study the network topology and configuration carefully. You will require 4 VMs (2 Windows Server, 1 Windows 10 and 1 CentOS 7) to complete this paper. Read the requirements carefully before configuring your servers.

Internet access **IS** allowed for this test. You are **NOT** to discuss your methodologies or workings with any other students. Document your workings/steps in another document and submit it by the end of the day.

A reminder to take snapshots of your VMs once you’ve completed a certain task. No extra time will be given in the event your VM is corrupted and you find yourself in a situation where you have to re-install the VM

**Network Topology**

****

**Network Configurations**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **PC Name** | **Network Adapter &**  **VMNet Settings** | **VM**  **ID/Passwords** |
| 1 | **ADServer**  Domain name: **wss2021.com** | VMNet 14 | Winserver2019: **ADServer**  IP: 192.168.12.100  VM Gateway: 192.168.12.1  Administrator/P@ssw0rd |
| 2 | **Server1**  Domain name: **wss2021.com** | VMNet 14/15 | Winserver2019: **Server1**  IP: 192.168.12.101 (VMNet 14), 101.137.100.20 (VMNet 15)  VM Gateway: 192.168.12.101 (VMNet 14)  Administrator/P@ssw0rd |
| 3 | **Server2**  Domain name: **wss2021.com** | VMNet 14 | CentOS7: **Server2**  IP: DHCP-assigned IP    superadmin/P@ssw0rd  root/root@redhat |
| 4 | **WinClient** | VMNet 15 | Windows 20H2: **WinClient**  IP: 101.137.100.21  VM Gateway: 101.137.100.20    Administrator/P@ssw0rd |

**1. Inside Zone**

1.1 ADServer - Windows Server 2019 (VM)

Basic Installation

1. Provision hardware resources and install Windows Server 2019 from the given ISO file.
2. Setup basic configuration of **ADServer** as stated in Network Configurations.

Installation and Configuration of Services

1. Install and configure Active Directory Domain Services (AD DS) and promote this server to be the Domain Controller.
   * Set domain name as “wss2021.com”
   * Use "P@ssw0rd" as Active Directory recovery password
2. Install and configure Domain Name Service (DNS) for the domain with the following configurations:
   * Setup both forward and reverse zone
   * Include all necessary records (**A** and **PTR**)for this domain
   * Include any other necessary records in order for services to function in the domain
3. Add users and groups in Active Directory as specified in Appendix A. For ease of checking by Judges – set to “User cannot change password” and “Password never expires”.
4. Configure Group Policy with the following outcomes, applicable to all machines connected to the domain. For ease of checking by Judges, create a Group Policy Object for each respective outcome.
5. Warning Banner in Message Text for users attempting to log on for all servers
   * Message “Unauthorized access prohibited!”
6. Disable Guest Account
7. Deny registry editing utilities for all users except “TechGrp”
8. Deny access to the command prompt and control panel to all users and machines. An exception shall be made for users under “TechGrp” and Domain Controller machines
9. Deny execute access on removable disks
10. Change the Kerberos maximum lifetime for user ticket to 4 hours
11. Configure DHCP service with the following settings:

* Set IP address range to lease from 192.168.12.50 to 192.168.12.65
* Set lease duration to 10 days
* Reserve an IP address for **Server2**

1.2 Server1 - Windows Server 2019 (VM)

Basic Installation

1. Provision hardware resources and install Windows Server 2019 from the given ISO file.
2. Setup basic configuration of **Server1** as stated in Network Configurations.

Installation and Configuration of Services

1. Install and configure Active Directory Certificate Server (AD CS) for root CA. Root certificate should use:
   * RSA SHA512 with key length 2048
   * Common name = WSS2021-CA
   * Validity Period = 8 years
2. Install any other required services to support the signing the web certificate for **Server2**.
3. Configure RRAS VPN service that supports PPTP protocol. Allows only users under “VPNGrp” can utilise the VPN service. Showcase that you can successfully establish a VPN connection from **WinClient**.

1.3 Server2 - Centos (VM)

Basic Installation

1. Provision hardware resources and install CentOS 7 from the given ISO file.
2. Setup basic configuration of **Server2** as stated in Network Configurations.

Installation and Configuration of Services

1. Install and configure VSFTPD service with the following settings:
   * Create user ftpuser
   * Bind the FTP service to port 221
   * Disable read/write access for anonymous
   * Allow ftpuser read access only
   * Allow superadmin both read and write access
   * Demonstrate that **WinClient** can access the service
2. Install Apache service and configure Apache web service with the following settings:

* Website named [www.wss2021.com](http://www.wss2021.com)
* Configure HTTPS using the signed web certificate from **Server1**
* Change HTTPS from default port 443 to 8443
* Redirect all HTTP port 80 traffic to port 8443 only
* Enable error logging on [www.wss2021.com](http://www.wss2021.com) and showcase the logs from the log file

1. Install and configure Samba with the following settings:

* Global configuration:
* workgroup = WORKGROUP
* netbios name = centos
* security = user
* map to guest = bad user
* dns proxy = no
* Allow anonymous read and write remote access
* Configure a second folder named **topsecret**, giving read and write access to user **smbuser1** with **smbgrp** group
* Showcase that you can access the Samba folders from **ADServer** and **Server1** as per the security requirements

1. Install and configure NTP service with the following settings
   * Synchronise with local time on **Server2**, with stratum level set to 1
   * Configure all machines to synchronise time with **Server2**

**2. Outside Zone**

1.1 WinClient - Windows 10 (VM)

Basic Installation

1. Provision hardware resources and install Windows Server 2019 from the given ISO file.
2. Setup basic configuration of **ADServer** as stated in Network Configurations.

Installation and Configuration of Services

1. Synchronise the computer time to **Server2**.
2. Ensure that you can connect to the RRAS VPN service successfully
3. Showcase that you can connect to the FTP service from **Server2**
4. Showcase that you can access the webpage from **Server2** (ignore the certificate error if it pops up on **WinClient**. However, there must be no errors when showcasing from **Server2**)

**Appendix**

**A.**

**Organization Unit Table**

|  |
| --- |
| **Organization Unit** |
| Tech |
| Sales |
| Engineer |

**Group Table**

|  |  |  |
| --- | --- | --- |
| **Group Name** | **Group Scope** | **Group Type** |
| TechGrp | Global | Security |
| SalesGrp | Global | Security |
| EngineerGrp | Global | Security |
| VPNGrp | Global | Security |

**User Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Organization Unit** | **Group** | **Logon Name** | **Password** |
| Tech | TechGrp | Tech1 | P@ssw0rd |
| Sales | SalesGrp | Sales1 | P@ssw0rd |
| - | EngineerGrp | Engineer1 | P@ssw0rd |
| - | EngineerGrp | Engineer1 | P@ssw0rd |
|  | VPNGrp | VPN1 | P@ssw0rd |
|  | VPNGrp | VPN2 | P@ssw0rd |