Migrating and Upgrading to Windows Server 2025 and Azure – Hands-on-Lab Guide

Techmentor Orlando 2024 Edition

A diagram of a computer network

Description automatically generated

By:

Dave Kawula Cristal Kawula

Emile Cabot Cary Sun John O’Neill Sr

PUBLISHED BY

MVPDays Publishing  
http://www.mvpdays.com

Copyright © 2024 by MVPDays Publishing

All rights reserved. No part of this book may be reproduced or transmitted in any form or without the publisher's prior written permission.

ISBN: TBA

Warning and Disclaimer

Every effort has been made to make this manual as complete and accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity concerning any loss or damages arising from the information contained in this book.

Feedback Information

We’d like to hear from you! If you have any comments about how we could improve the quality of this book, please don’t hesitate to contact us by visiting www.checkyourlogs.net or sending an email to dave@mvpdays.com.

# Contents

[Contents v](#_Toc182301058)

[Getting Started 10](#_Toc182301059)

[Gaining Access to your Lab and initial configurations 10](#_Toc182301060)

[Lab 1 19](#_Toc182301061)

[Migrating Active Directory Domain Services (ADDS) 2016 to 2025 and Azure 19](#_Toc182301062)

[Exercise 1.1 Verify Healthy Replication of Active Directory Domain Services (ADDS) 22](#_Toc182301063)

[Exercise 1.2 Run ADPREP to Extend the Active Directory Schema 26](#_Toc182301064)

[Exercise 1.3 - Installing Active Directory Domain Services (ADDS) on a Windows Server 2025 Member Server (TMDC05) 37](#_Toc182301065)

[Exercise 1.4 - Transfer FSMO (Flexible Single Master Operations) Roles 44](#_Toc182301066)

[Exercise 1.5 - Installing Active Directory Domain Services (ADDS) on a Windows Server 2025 Member Server (TMDC06) 46](#_Toc182301067)

[Exercise 1.6 – Tune SRV Records for older Domain Controllers 53](#_Toc182301068)

[Exercise 1.7 - Demote TMDC02 55](#_Toc182301069)

[Exercise 1.8 - Demote TMDC01 56](#_Toc182301070)

[Exercise 1.9 – Steal the IP from TMDC01 57](#_Toc182301071)

[Exercise 1.10 – Steal the IP from TMDC02 61](#_Toc182301072)

[Exercise 1.11 – Configure NTP for an External Time Source on TMDC05 65](#_Toc182301073)

[Exercise 1.12 – Automate External NTP Configuration with Group Policy for PDC Emulators 68](#_Toc182301074)

[Exercise 1.13 – Recommended Settings for Virtual Domain Controllers Guest Time Settings 79](#_Toc182301075)

[Exercise 1.14 – Update the Domain and Forest Functional Levels to Server 2025 82](#_Toc182301076)

[Exercise 1.15 – Configure a Domain Controller in Azure (Instructor Demo) 86](#_Toc182301077)

[Lab 2 96](#_Toc182301078)

[Windows Admin Center and Azure Hybrid Services 96](#_Toc182301079)

[Exercise 2.1- Configure Windows Admin Center 98](#_Toc182301080)

[Exercise 2.2 - Connecting Windows Admin Center to Azure Hybrid Services 102](#_Toc182301081)

[Exercise 2.3 - Test Failover to Azure using Azure Site Recovery 113](#_Toc182301082)

[Exercise 2.4 – Onboard Machines to Azure Arc 134](#_Toc182301083)

[Exercise 2.4.1 – Manually Onboarding to Azure Arc via PowerShell 137](#_Toc182301084)

[Exercise 2.4.2 – Managing Updates on Servers using Azure Update via Azure Arc 137](#_Toc182301085)

[Exercise 2.5 – Azure Migrate Server Assessment 137](#_Toc182301086)

[Exercise 2.6 – Configure Azure Extended Network (Instructor Led Discussion) 142](#_Toc182301087)

[Exercise 2.7 – Connect to Azure using Azure Network Adapter (Instructor Led Discussion/Demo Only) 147](#_Toc182301088)

[Lab 3 152](#_Toc182301089)

[Migrating File Servers 152](#_Toc182301090)

[Exercise 3.1 - Migrate TMFile01 using Windows Admin Center and the Storage Migration Service 152](#_Toc182301091)

[Exercise 3.2 - Migrate Tmfile03 to Azure Files using Windows Admin Center (Instructor Led Demo) 169](#_Toc182301092)

[Lab 4 178](#_Toc182301093)

[Upgrading IIS Servers 178](#_Toc182301094)

[Exercise 4.0 - Backup the IIS Server 178](#_Toc182301095)

[Exercise 4.1 - Installing WordPress, PHP, and MySQL using PowerShell on Server 2012R2 using PowerShell (Instructor Guided) 179](#_Toc182301096)

[Exercise 4.2 – Azure Migrate Appliance Configuration (Instructor Led Demo) 186](#_Toc182301097)

[Exercise 4.3 –Using Azure App Service Migration Assistant to Migrate Sites | Web Apps (Instructor Led Demo) 195](#_Toc182301098)

[Exercise 4.4 - Backup the IIS Server 202](#_Toc182301099)

[Exercise 4.5 - Upgrading from 2012R2 to Windows Server 2022 Double Swing (Deprecated) – Review Only 203](#_Toc182301100)

[Exercise 4.6 – Migrating Web Server to Azure (Instructor Led) 221](#_Toc182301101)

[Lab 5 225](#_Toc182301102)

[Migrating Print Servers 225](#_Toc182301103)

[Exercise 5.0 – Configuring TMPrint01 226](#_Toc182301104)

[Exercise 5.1 – Exporting the Windows Server2016 Print Server’s Configurations 236](#_Toc182301105)

[Exercise 5.2 – Importing the Print Server’s Configurations into Windows Server 2022 242](#_Toc182301106)

[Exercise 5.3 – Step by Step walkthrough Microsoft Universal Print 249](#_Toc182301107)

[Lab 6 250](#_Toc182301108)

[Hardening Windows Server 250](#_Toc182301109)

[6.1 Locking Down Windows Server 2019/2022 and Windows 10/11 with Group Policy Security Baselines via Security Compliance Toolkit 1.0 250](#_Toc182301110)

[Lab 7 261](#_Toc182301111)

[Migrating DHCP 261](#_Toc182301112)

[Exercise 7.1 - Migrate DHCP by moving the DHCP Database 261](#_Toc182301113)

[Lab 8 269](#_Toc182301114)

[Migrating DNS 269](#_Toc182301115)

[Exercise 8.1 – Migrate Primary Forward Lookup Zone by copying the Zone Database File 269](#_Toc182301116)

[Exercise 8.2 – Migrate Primary Forward Lookup Zone by Converting a Secondary Zone to Primary Zone 280](#_Toc182301117)

[Lab 9 294](#_Toc182301118)

[Upgrading Storage Spaces Standalone from Server 2016 to Windows Server 2022 294](#_Toc182301119)

[Exercise 9.1 – In-Place Upgrading from Storage Spaces 2016 to 2022 – Review Only 294](#_Toc182301120)

[Lab 10 311](#_Toc182301121)

[Upgrading WSUS from Windows Server 2012R2 to Windows Server 2019 311](#_Toc182301122)

[Exercise 10.1 - Planning for WSUS Upgrade 312](#_Toc182301123)

[Exercise 10.2 - In-Place OS Upgrade from Windows Server 2016 to 2019 315](#_Toc182301124)

[Exercise 10.3 - Post Upgrade Tasks 320](#_Toc182301125)

[Lab 11 325](#_Toc182301126)

[Upgrading a Storage Spaces Direct Cluster to Windows Server 2022 325](#_Toc182301127)

[Exercise 11.1 - Prerequisites and limitations 325](#_Toc182301128)

[Exercise 11.2 - Performing an in-place upgrade while VMs are running 327](#_Toc182301129)

[Wrap-up 340](#_Toc182301130)

[Join us at MVPDays and meet great MVPs like this in person 340](#_Toc182301131)

[Live Presentations 340](#_Toc182301132)

[Video Training 340](#_Toc182301133)

[Live Instructor-led Classes 340](#_Toc182301134)

[Consulting Services 341](#_Toc182301135)

Getting Started

Gaining Access to your Lab and initial configurations

Follow these steps provided by your instruction to gain access to the lab and perform some initial configurations to help with your Hands-on-Labs for Techmentor 2024.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Your instructor will provide you with instructions on the day of the lab so that you can connect to the lab on the day of the event. |  |
| 1. The password for the RDP Host Connection to the lab is Lab$123456!!@@## |  |
| 1. Click on yes to connect to your LAB VM |  |
| 1. In the lab, we use Routing and Remote Access to give the Lab VM access to the internet. This is required later for Hybrid Azure Labs. 2. During the provision steps, the local network adapter changes, which breaks a setting. 3. Click on Start, Windows Administrative Tools, Routing and Remote Access |  |
| 1. Expand your server, IPv4, and NAT |  |
| 1. Right Click on NAT and click New Interface |  |
| 1. Select Ethernet 5 and click OK |  |
| 1. Select the radio button Public interface connected to the internet, check the Enable NAT on this interface checkbox, then click OK. |  |
| 1. Close Routing and Remote Access |  |
| 1. Open Edge and browse to [www.github.com/dkawula](http://www.github.com/dkawula) 2. Click on Techmentor\Operations\Techmentor\HOL-OrlandoNovember2024 Repository 3. Click on Hands-On-Labs-TechmentorOnlineMay2024-LabCommands.txt |  |
| 1. Click on RAW 2. Select all the code and copy it to the clipboard |  |
| 1. Open Notepad 2. Paste the commands into the Notepad and save as c:\users\lab-admin\desktop\labcommands.txt |  |
| 1. On the Desktop you will have a pre-created Remote Desktop Connection Manager file called LabVMs.RDG. Double click on this. |  |
| 1. You should be connected like this now. |  |

Lab 1

Migrating Active Directory Domain Services (ADDS) 2016 to 2025 and Azure

Welcome to this hands-on lab, where we will guide you through the steps required to perform a zero-downtime migration to Windows Server 2025 Active Directory Domain Services (ADDS). In our lab environment, we have two existing Domain Controllers, TMDC01 and TMDC02, running Windows Server 2016 ADDS. Additionally, two servers, TMDC05 and TMDC06, have been pre-installed with Windows Server 2025 and joined to the Techmentor.com domain as member servers.

Our goal is to ensure a seamless transition to Windows Server 2025 ADDS and extend our hybrid environment by deploying a Domain Controller to our Azure Tenant. By following the steps outlined in this lab, you will gain hands-on experience with the following tasks:

1. Extending the ADDS Schema to Windows Server 2025 (AD Prep)
2. Installing the ADDS Roles on DC05 and DC06
3. Joining DC05 and DC06 as replica domain controllers
4. Adjusting Service (SRV) records to manage connections and drain traffic from TMDC01 and TMDC02
5. Transferring FSMO (Flexible Single Master Operations) roles from TMDC01 and TMDC02 using PowerShell
6. Performing validation and replication tests
7. Migrating Primary DNS functionality from TMDC01 to DC05
8. Demoting TMDC01 and TMDC02
9. Configuring NTP Settings
10. Transferring FSMO Roles (as needed)
11. Configuring an IaaS VM in Azure as a Domain Controller

By the end of this lab, you will have a robust understanding of the zero-downtime migration process and how to effectively manage an Active Directory environment during a server upgrade. Let's get started!

***BIG Note: November 5,2024 – Microsoft is starting to push Upgrade Prompts on Windows Servers. The below prompt is via Windows Updates on a Server 2022 VM that is a domain controller. Please DO NOT Upgrade Domain Controllers using this method. Follow our instructions below for a seamless migration process! For 20 + years we don’t directly upgrade domain controllers. This is still true.***



### Exercise 1.1 Verify Healthy Replication of Active Directory Domain Services (ADDS)

Before undertaking any operational tasks in Active Directory Domain Services (ADDS), such as adding or removing domain controllers, it is essential to verify the health of the system. This can be achieved using command-line tools like **repadmin.exe** and **dcdiag.exe**. In a production environment, it is highly recommended to save the output of these tools to text files and include them in your project documentation. This practice ensures that you have a record of the system's health before making any changes.

Remember for these labs you should copy and paste the commands from the lab commands file copied earlier.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC01 as Administrator |  |
| 1. Open an Administrative Command Prompt 2. Type: repadmin /replsum /bysrc /bydest /sort:delta >c:\repltest.txt & start c:\repltest.txt 3. When reviewing the file, note any issues; they could be used for troubleshooting later. 4. If there are no issues, then we can move on to the next step.   NOTE: In a lab environment such as this, it is pretty common for Active Directory Domain Controllers to exceed replication thresholds and show error messages. | The above screenshot is an example of some errors that we might be looking for. |
| 1. Type dcdiag.exe /e /test:frssysvol >c:\frstest.txt & start c:\frstest.txt 2. Open c:\frstest.txt and verify that no errors exist. 3. When reviewing the file, note any issues; they could be used for troubleshooting later. |  |
| 1. Type dcdiag /test:fsmocheck >c:\fsmocheck.txt & start c:\fsmocheck.txt 2. Open c:\fsmocheck.txt 3. When reviewing the file, note any issues; they could be used for troubleshooting later. |  |
| 1. Type repadmin /SHOWREPS TMDC01 >c:\Showreps.txt & start c:\showreps.txt 2. Open c:\Showreps.txt 3. When reviewing the file, note any issues; they could be used for troubleshooting later. |  |
| 1. Did you find anything that looks out of place? |  |
| 1. What are the options available? |  |
| 1. Hint – If you see any errors try Replicating through AD Sites and Services. Then Re-Run the tests. |  |

### Exercise 1.2 Run ADPREP to Extend the Active Directory Schema

To extend the Active Directory Domain Services (ADDS) schema for Windows Server 2025, you will need the installation media for Windows Server 2022. The necessary files are located in the **.\support\adprep** directory on the installation media. The executable used for this process is **adprep.exe.**

**Note:** When you install the first Windows Server 2025 domain controller, ADPREP will automatically run and extend the schema. However, this method is not preferred, especially in larger environments, because different administrators typically have Enterprise Admins and Schema Admins rights. The steps outlined below allow for verification and control before integrating a new version of Windows Server into ADDS.

**Upgrading ADDS Forest and Domain with ADPrep.exe**

The commands to upgrade the ADDS forest and domain using adprep.exe are derived from our standard production procedures. Although simply adding a Windows Server 2025 domain controller will trigger ADPREP automatically if it hasn't been run, we prefer a more controlled approach. This method ensures granular control and verification, which is essential for schema modifications in a production environment and aligns with change control processes. Automatic execution does not offer the same level of validation and oversight required.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC01 as Administrator |  |
| 1. Open Active Directory Users and Computers, click on the Users Container, right Click on the Administrator Account and click properties 2. Verify that the account is a member of Domain Admins, Enterprise Admins, and Schema Admins groups |  |
| 1. What are FSMO Roles and why are they important to Active Directory? | Flexible Single Master Operations (**FSMO**) roles, also known as operations master roles, are specialized domain controller (DC) tasks in Active Directory (AD). These roles are crucial for the smooth functioning of AD and to avoid conflicts during operations. There are five FSMO roles, divided into two categories: **forest-wide** and **domain-wide** roles.  **Forest-Wide Roles**  **Schema Master**  **Role:** Manages updates and modifications to the AD schema.  **Responsibility:** Ensures that any schema changes (such as adding new attributes or object types) are replicated throughout the forest.  **Location:** Only one schema master per AD forest.  **Domain Naming Master**  **Role:** Manages the addition and removal of domains in the AD forest.  **Responsibility:** Ensures that the creation and deletion of domains are handled without name conflicts.  **Location:** Only one domain naming master per AD forest.  **Domain-Wide Roles**  **PDC Emulator**  **Role:** Acts as a primary domain controller emulator for backward compatibility with older Windows NT systems.  **Responsibilities:**  Handles password changes and account lockouts.  Synchronizes time across the domain to ensure consistent timestamps.  Processes Group Policy updates and manages domain-wide replication.  **Location:** One PDC emulator per AD domain.  **RID Master**  **Role:** Allocates pools of relative identifiers (RIDs) to DCs within a domain.  **Responsibility:** Ensures unique security identifiers (SIDs) for objects created in the domain by managing the RID pool.  **Location:** One RID master per AD domain.  **Infrastructure Master**  **Role:** Maintains references to objects in other domains (cross-domain object references).  **Responsibility:** Updates object references whenever objects are moved, renamed, or deleted in other domains.  **Location:** One infrastructure master per AD domain. It should not be on a global catalog server unless all DCs in the domain are global catalog servers.  Importance of FSMO Roles  **Consistency and Integrity:** FSMO roles help maintain the integrity and consistency of AD operations by ensuring that specific critical tasks are handled by designated DCs.  **Conflict Prevention:** By assigning unique roles to specific DCs, FSMO roles prevent conflicts that could arise from simultaneous changes or operations being performed by multiple DCs.  **Centralized Management:** FSMO roles allow for centralized management of critical tasks, simplifying administration and troubleshooting.  **Transferring FSMO Roles**  FSMO roles can be transferred between DCs using tools like the Active Directory Users and Computers (ADUC) snap-in, the NTDSUtil command-line utility, or PowerShell commands. It is essential to transfer FSMO roles gracefully to ensure continuous availability and to avoid disruptions in AD services.  In summary, FSMO roles are vital components of Active Directory's infrastructure, ensuring efficient and conflict-free operation of critical domain and forest-wide functions. |
| 1. Determine the Flexible Single Master Operations (FSMO) role 2. From an Administrative Command Prompt type Netdom Query FSMO |  |
| 1. Who are the owners of the FSMO Roles? | All roles are currently being held by TMDC02, which means that the ADPREP operations should be run from TMDC02. Specifically, ADPREP needs to be run directly against the Domain Controller holding the Schema Master Role. |
| 1. Logon to TMDC02 |  |
| 1. What does the Active Directory Replication Process look like? | Active Directory (AD) replication ensures that changes made to the AD database (NTDS.DIT) are consistently propagated across all domain controllers (DCs) within an AD forest. This process is crucial for maintaining the integrity and consistency of the AD data, including user accounts, group memberships, and policies.  **Key Components of AD Replication**  **Multimaster Replication:**  All DCs within a domain can accept changes and replicate those changes to other DCs. This allows for redundancy and ensures that changes can be made even if some DCs are unavailable.  **Replication Topology:**  AD uses a replication topology that defines how DCs communicate and replicate changes with one another. This topology is automatically generated by the **Knowledge Consistency Checker (KCC)**.  **Change Tracking:**  AD uses update sequence numbers (USNs) to track changes. Each DC has a local USN that increments with each change. This ensures that only the latest changes are replicated.  **Replication Intervals:**  Replication occurs at defined intervals, which can be configured to optimize network usage and ensure timely propagation of changes. |
| 1. Open DSSite.msc and force Replication prior to starting |  |
| 1. Disable Outbound Replication from TCDC02 | In our production environment, we undertake this step as a precautionary measure to contain any potential issues that may arise during the Schema Modification process, preventing them from affecting the entire enterprise. Should a scenario occur where the Schema Extension becomes corrupted or fails, we have a contingency plan in place. By shutting down TMDC02 and manually removing it from Active Directory using NTDSUTIL, we can isolate any adverse effects. Subsequently, we can easily reintegrate TMDC02 back into the domain controller pool by re-adding it as a domain controller. This approach ensures minimal disruption and swift recovery in the event of any unforeseen complications during schema modifications. |
| 1. From the Administrative Command prompt type repadmin /options TMDC02 +DISABLE\_OUTBOUND\_REPL |  |
| 1. On the Host go to Hyper-V Manager, right click on TMDC02 and click settings 2. Click on SCSI Controller and click on DVD Drive and click Add 3. Click on Image File and type e:\iso\26100.1742.240906-0331.ge\_release\_svc\_refresh\_SERVER\_EVAL\_x64FRE\_en-us.iso   and click apply   1. **Return to TMDC02** |  |
| 1. From an Administrative Command Prompt type:  D: CD \support\adprep |  |
| 1. Type Adprep.exe /forestprep and press enter When prompted, press C and Enter |  |
| 1. You will see the current Schema version of 47 upgrading to 91 You should see a message at the bottom stating ADPrep successfully updated the forest-wide information |  |
| 1. Type Adprep.exe /domainprep and press enter |  |
| 1. Review c:\windows\debug\adprep\logs 2. Each run of Adprep is stored here 3. The logfile is called adprep.log 4. Does it look like it succeeded? |  |
| 1. Enable Outbound Replication by running repadmin /options TMDC02 -DISABLE\_OUTBOUND\_REPL |  |
| 1. Force replication of all Active Directory Domain Services (AD DS) domain controllers by typing repadmin /syncall /e /d /a /P and  repadmin /syncall /e /d /a 2. If you see any error messages wait 30 seconds and repeat step 21. |  |
| 1. Validate the Schema version number by typing dsquery \* "cn=schema,cn=configuration,dc=techmentor,dc=com" -scope base -attr objectVersion |  |
| 1. Of note, these are the valid SCHEMA Version Numbers | 13 -> Windows 2000 Server  30 -> Windows Server 2003 RTM, Windows 2003 With Service Pack 1, Windows 2003 With Service Pack 2  31 -> Windows Server 2003 R2  44 -> Windows Server 2008 RTM  87 -> Windows Server 2016  88 -> Windows Server 2019 and 2022  91 -> Windows Server 2025 |

### Exercise 1.3 - Installing Active Directory Domain Services (ADDS) on a Windows Server 2025 Member Server (TMDC05)

Transitioning to Active Directory Domain Services (ADDS) for Windows Server 2025 necessitates adding new domain controllers. Consequently, throughout this exercise, we will introduce four active domain controllers capable of handling client authentication for both Kerberos and NTLM logins.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC05 as Techmentor\Administrator |  |
| 1. Startup a PowerShell prompt and type in the command Install-WindowsFeature AD-Domain-Services |  |
| 1. Install the ADDSDeployment module by running Import-Module ADDSDeployment -verbose |  |
| 1. Once those additional tools have been installed, run Test-ADDSDomainControllerInstallation -DomainName Techmentor.com to test for any prerequisites.   Use Lab$123456!!@@## as the DsRestoremode Password |  |
| 1. Promote this member server into a domain controller by running Install-ADDSDomainController -CreateDnsDelegation:$false -InstallDns:$true -DatabasePath 'C:\Windows\NTDS' -DomainName 'Techmentor.com'  Type Lab$123456!!@@## for the Directory Services Restore Mode Password  Press [A] Yes to All |  |
| 1. TMDC05 will reboot |  |
| 1. Logon as Techmentor\Administrator  It is normal for a Domain Controller to take a few minutes before the login screen is ready |  |
| 1. Type ipconfig /registerdns |  |
| 1. Open an Administrative Command Prompt and type net stop netlogon & Net start netlogon and press enter | The netlogon service updates DNS by reading a file called netlogon.DNS to create Service Records (SRV) for Domain Controllers. Part of the production process is to stop and start the netlogon service to force these records propagation. |
| 1. Type Repadmin /kcc and press enter | Repadmin /kcc triggers the Knowledge Consistency Checker. The Knowledge Consistency checker is what helps create the automatically generated connection objects in Active Directory Sites and Services. |
| 1. Type Repadmin /syncall /e /d /a and press enter |  |
| 1. Type Repadmin /syncall /e /d /a /P |  |
| 1. Try opening Active Directory Users and Computers (ADUC)  Did that work?  How about Active Directory Sites and Services? | It did not work because it is not best practice to manage Active Directory from a Domain Controller itself. You should configure a Privileged Management Workstation for this in production.   For this lab, we will install the RSAT-ADDS-Tools. |
| 1. Open an Administrative PowerShell prompt and type Install-WindowsFeature RSAT-ADDS-Tools -verbose |  |

### Exercise 1.4 - Transfer FSMO (Flexible Single Master Operations) Roles

During the migration process, the Flexible Single Master Operations Roles (FSMO) must be transferred to TMDC05. It's typical for these roles to be distributed across the infrastructure. Understanding the functions of each of these five roles within a multi-master Active Directory Domain Services (ADDS) domain is crucial.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC05 as Techmentor\Administrator |  |
| 1. Open an Administrative PowerShell Prompt 2. run Get-ADForest Techmentor.com | Select SchemaMaster,DomainNamingMaster |  |
| 1. run Get-ADDomain Techmentor.com | Select RIDMaster,InfrastructureMaster,PDCEmulator |  |
| 1. Run Netdom Query FSMO |  |
| 1. run Move-ADDirectoryServerOperationMasterRole -identity TMDC05 -OperationMasterRole PDCEmulator,RIDMaster,InfrastructureMaster,SchemaMaster,DomainNamingMaster |  |
| 1. Run Netdom Query FSMO |  |

### Exercise 1.5 - Installing Active Directory Domain Services (ADDS) on a Windows Server 2025 Member Server (TMDC06)

Part of the migration process will be replacing TMDC02 with TMDC06. This process is nearly identical to TMDC05 except for the transfer of the FSMO Roles.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC06 as Techmentor\Administrator |  |
| 1. Startup a PowerShell prompt and type in the command Install-WindowsFeature AD-Domain-Services | Graphical user interface, text, application  Description automatically generated |
| 1. Install the ADDSDeployment module by running Import-Module ADDSDeployment -verbose | A picture containing text  Description automatically generated |
| 1. Once those additional tools have been installed, run Test-ADDSDomainControllerInstallation -DomainName Techmentor.com to test for any prerequisites. | A picture containing text  Description automatically generated  Graphical user interface  Description automatically generated with low confidence |
| 1. Promote this member server into a domain controller by running Install-ADDSDomainController -CreateDnsDelegation:$false -InstallDns:$true -DatabasePath 'C:\Windows\NTDS' -DomainName 'Techmentor.com'  Type Lab$123456!!@@## for the Directory Services Restore Mode Password  Press [A] Yes to All  Did you see any potential problems with the way the TMDC04 is configured? | Text  Description automatically generated  Text  Description automatically generated  It appears that TMDC04 did not have a static IP Address. Typically we always want Domain Controllers to be configured with Static IP Addresses. Because this is a lab where we will be decomissioning TMDC02 anyways and assuming its IP Address this change can happen at that time. |
| 1. TMDC06 will reboot | Graphical user interface  Description automatically generated |
| 1. Logon as Techmentor\Administrator  It is normal for a Domain Controller to take a few minutes before the login screen is ready | Graphical user interface, application  Description automatically generated |
| 1. Open an Administrative Command Prompt and type ipconfig /registerdns | Text  Description automatically generated |
| 1. Type net stop netlogon & Net start netlogon and press enter | Text  Description automatically generated  The netlogon service updates DNS by reading a file called netlogon.DNS to create Service Records (SRV) for Domain Controllers. Part of the production process is to stop and start the netlogon service to force these records propagation. |
| 1. Type Repadmin /kcc and press enter | Text  Description automatically generated  Repadmin /kcc triggers the Knowledge Consistency Checker. The Knowledge Consistency checker is what helps create the automatically generated connection objects in Active Directory Sites and Services. |
| 1. Type Repadmin syncall /e /d /a and press enter | Text  Description automatically generated |
| 1. Type Repadmin /syncall /e /d /a /P  Did this command run successfully? | This command didn’t run successfully; as you can see, we get the topology incomplete error message. We will need to invoke the knowledge consistency checker on each domain controller to fix this.   Run Repadmin /kcc from the other DCs and try again. |
| 1. Did Replication complete | Yes, replication is now working correctly after triggering the KCC on TMDC03. |

### Exercise 1.6 – Tune SRV Records for older Domain Controllers

Tuning Service Records (SRV) in Active Directory is crucial for controlling authentication traffic within an Active Directory site. By default, without proper tuning, all authentication traffic becomes round-robin, leading to inefficiencies and making it impossible to manage traffic redirection prior to decommissioning a domain controller.

To prevent old domain controllers from continuing to authenticate clients, it's essential to tune their Service Records by modifying their local registry. This process ensures that any live Active Directory Domain Services (ADDS) connections for these domain controllers are gradually drained off before decommissioning.

By adjusting the Service Records, administrators can strategically manage the flow of authentication traffic, redirecting it away from specific domain controllers slated for decommissioning. This proactive approach helps maintain the stability and performance of the Active Directory environment while facilitating the seamless transition and retirement of outdated infrastructure components.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC02 as Techmentor\Administrator |  |
| 1. Run Regedit 2. Create a new Registry key in HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters 3. New Reg DWORD 32Bit 4. LdapSrvPriority 5. Set the value to 10 |  |
| 1. Open an Administrative Command Prompt 2. Type: Net Stop Netlogon & Net Start Netlogon |  |
| 1. Open the DNSmgmt.msc (DNS Management Console) and review the \_MSDSC.techmentor.com zone 2. Validate that the change in the Service Records has taken place à You can see TMDC02 with a value of 16 now. |  |
|  |  |

### Exercise 1.7 - Demote TMDC02

In this exercise, we will demote the old Windows Server 2016 Domain Controller TMDC02 and return it to a status of a Member Server in the Techmentor.com domain.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC02 as Techmentor\Administrator |  |
| 1. Open an Administrative PowerShell Prompt 2. Type Uninstall-ADDSDomainController -Verbose and press enter 3. When prompted for a password type Lab$123456!!@@## |  |
| 1. Shut down TMDC02 VM |  |

### Exercise 1.8 - Demote TMDC01

In this exercise, we will demote the old Windows Server 2016 Domain Controller TMDC01 and return it to a status of a Member Server in the Techmentor.com domain.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC01 as Techmentor\Administrator |  |
| 1. Open an Administrative PowerShell Prompt 2. Type Uninstall-ADDSDomainController -Verbose and press enter 3. When prompted for a password type Lab$123456!!@@## |  |
| 1. Shutdown TMDC01 |  |

### Exercise 1.9 – Steal the IP from TMDC01

During the Active Directory Directory Service (ADDS) decommissioning process for old domain controllers, stealing the IP address of the primary DNS servers is a technique used to facilitate a seamless transition without necessitating changes to static IP entries pointing to the removed domain controllers. In this scenario, the objective is to take over the IP address currently assigned to TMDC01 and reassign it to TMDC05. This action ensures that any static and DHCP DNS entries are automatically ported over to TMDC05, minimizing disruptions and simplifying the migration process.

The process involves the following steps:

1. **Preparation:**

* Ensure that TMDC05 is properly configured and ready to assume the responsibilities of TMDC01.
* Verify that TMDC01 is slated for decommissioning and no longer required in the AD infrastructure.

1. **Stealing the IP Address:**

* Access the network settings of TMDC01 and release its current IP address.
* Assign the same IP address to TMDC05, effectively "stealing" the IP address from TMDC01.
* Update DNS settings on TMDC05 to reflect its new IP address assignment.

1. **Verification:**

* Confirm that TMDC05 has successfully assumed the IP address of TMDC01.
* Validate that all static and DHCP DNS entries have been automatically redirected to TMDC05.

1. **Testing:**

* Conduct thorough testing to ensure that TMDC03 is functioning correctly with its new IP address.
* Verify that all DNS queries are being handled appropriately by TMDC05.

By stealing the IP address of the primary DNS server during the AD decommissioning process, organizations can simplify the transition to new domain controllers while maintaining the integrity and continuity of DNS services. This approach minimizes the need for manual configuration changes and reduces the risk of service disruptions during the migration process.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC05 as Techmentor\Administrator |  |
| 1. Configure the IP Address with 192.168.11.3 |  |
| 1. Open an Administrative Command Prompt and type ipconfig /registerdns | Text  Description automatically generated |
| 1. Type net stop netlogon & Net start netlogon and press enter | Text  Description automatically generated  The netlogon service updates DNS by reading a file called netlogon.DNS to create Service Records (SRV) for Domain Controllers. Part of the production process is to stop and start the netlogon service to force these records propagation. |
| 1. Type Repadmin /kcc and press enter | Text  Description automatically generated  Repadmin /kcc triggers the Knowledge Consistency Checker. The Knowledge Consistency checker is what helps create the automatically generated connection objects in Active Directory Sites and Services. |
| 1. Type Repadmin /syncall /e /d /a and press enter | Text  Description automatically generated |
| 1. Type Repadmin /syncall /e /d /a /P  Did this command run successfully? | This command didn’t run successfully; as you can see, we get the topology incomplete error message. We will need to invoke the knowledge consistency checker on each domain controller to fix this.   Run Repadmin /kcc from the other DCs and try again. |

### Exercise 1.10 – Steal the IP from TMDC02

In this exercise, we will repeat the steps outlined in the previous exercise, but this time, we will take over the IP Address assigned to TMDC02 and assign it to TMDC06. This action will ensure that any static and DHCP DNS entries are seamlessly ported over to TMDC06, facilitating a smooth transition in the Active Directory (AD) decommissioning process.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC06 as Techmentor\Administrator |  |
| 1. Configure the IP Address for 192.168.11.4 |  |
| 1. Open an Administrative Command Prompt and type ipconfig /registerdns | Text  Description automatically generated |
| 1. Type net stop netlogon & Net start netlogon and press enter | Text  Description automatically generated  The netlogon service updates DNS by reading a file called netlogon.DNS to create Service Records (SRV) for Domain Controllers. Part of the production process is to stop and start the netlogon service to force the propagation of these records. |
| 1. Type Repadmin /kcc and press enter | Text  Description automatically generated  Repadmin /kcc triggers the Knowledge Consistency Checker. The Knowledge Consistency checker is what helps create the automatically generated connection objects in Active Directory Sites and Services. |
| 1. Type Repadmin /e /d /a and press enter | Text  Description automatically generated |
| 1. Type Repadmin /e /d /a /P  Did this command run successfully? | This command didn’t run successfully; as you can see, we get the topology incomplete error message. We will need to invoke the knowledge consistency checker on each domain controller to fix this.   Run Repadmin /kcc from the other DCs and try again. |

### Exercise 1.11 – Configure NTP for an External Time Source on TMDC05

The PDC Emulator (**FSMO**) role in Active Directory plays a critical role in maintaining time synchronization within the domain. As the primary domain controller emulator, the PDC Emulator serves as the authoritative time source for the entire domain. It ensures that all domain controllers and domain-joined computers maintain consistent and accurate time, which is essential for various AD operations, authentication processes, and security protocols.

Here's how the PDC Emulator handles time synchronization in Active Directory:

1. **Domain Time Synchronization:**

* All domain computers and member servers synchronize their time with the nearest domain controller within their Active Directory site. If AD sites are not configured, they synchronize with the domain controller holding the PDC Emulator role.
* Domain controllers synchronize their time with the domain controller holding the PDC Emulator role, ensuring that all DCs maintain consistent time.

1. **External Time Source Synchronization:**

* The PDC Emulator can be configured to synchronize its time with an external time source, typically an NTP (Network Time Protocol) server on the internet.
* Synchronizing with an external time source ensures that the domain maintains accurate time, even if the internal clock of the PDC Emulator drifts or if there are discrepancies between internal clocks and external time standards.

1. **Configuration Options:**

* Time synchronization on the PDC Emulator can be configured manually or through Group Policy Objects (GPOs).
  + Further to this configuration you can set up WMI Filters to detect which Domain Controller holds the PDC Emulator role. If this role transitions to a new domain controller the WMI Filter will link the group policy to the new domain controller thus having a floating master time server with no manual configuration necessary, post FSMO role transfers.
* The **w32tm.exe** utility is commonly used to configure time synchronization settings manually on the PDC Emulator.

In summary, the PDC Emulator role ensures that time synchronization is maintained within the Active Directory domain by serving as the authoritative time source. By synchronizing with external time sources, the PDC Emulator helps to ensure the accuracy and consistency of time across the entire domain, facilitating smooth operation of AD services and security mechanisms. In this exercise, we will focus on configuring a domain controller with the PDC Emulator role to synchronize time with an external NTP server, ensuring precise timekeeping within the AD environment.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC05 as Techmentor\Administrator |  |
| 1. Open an administrative Command Prompt 2. w32tm.exe /config /manualpeerlist:"0.pool.ntp.org,0x8 1.pool.ntp.org,0x8 2.pool.ntp.org,0x8" /syncfromflags:manual /update |  |
| 1. w32tm /config /reliable:yes |  |
| 1. net stop w32time && net start w32time |  |
| 1. w32tm /resync |  |
| 1. The list of current NTP sources is stored in the registry critical HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters in the NtpServer parameter. |  |

### Exercise 1.12 – Automate External NTP Configuration with Group Policy for PDC Emulators

Creating a Group Policy with a WMI Filter that detects the PDC Emulator FSMO Role holder and automatically configures NTP settings is a proactive approach to ensuring consistent time synchronization within an Active Directory (AD) environment. This automated solution simplifies the management of NTP settings, particularly when the PDC Emulator role is transferred between domain controllers. Here's how it works:

1. **WMI Filter Detection:**

* A WMI (Windows Management Instrumentation) filter is created to detect the domain controller holding the PDC Emulator FSMO role. WMI filters allow administrators to dynamically apply Group Policy based on specific conditions.
* The WMI filter queries the AD infrastructure to identify the domain controller currently serving as the PDC Emulator.

1. **Group Policy Configuration:**

* A Group Policy Object (GPO) is created or modified to include settings for configuring NTP (Network Time Protocol) settings.
* Within the GPO, settings for specifying the NTP server address(es) and other time-related configurations are configured.

1. **Linking the GPO:**

* The GPO, along with the associated WMI filter, is linked to the domain controllers Organizational Unit (OU) within Active Directory.
* This ensures that the GPO is applied only to domain controllers and specifically targets the PDC Emulator role holder based on the WMI filter condition.

1. **Automated NTP Configuration:**

* When the PDC Emulator FSMO role is transferred between domain controllers, the WMI filter detects the change.
* As a result, the associated Group Policy is automatically applied to the new PDC Emulator role holder.
* The NTP settings configured within the GPO are then applied to the new PDC Emulator, ensuring that time synchronization remains accurate and consistent.

By implementing this automated solution, administrators can ensure that NTP settings are consistently applied to the domain controller holding the PDC Emulator role, regardless of which domain controller currently serves in that capacity. This approach reduces manual intervention and helps maintain reliable time synchronization throughout the AD environment, promoting stability and consistency in timekeeping operations.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC05 as Techmentor\Administrator |  |
| 1. Open the Group Policy Management Console (GPMC.msc) and create a new policy PDC External Time and link it to the Domain Controllers OU |  |
|  |  |
| 1. Create a WMI filter with the following code and link it to your policy (this WMI filter allows you to find a domain controller with the role of PDC and apply the policy only to it): Select \* from Win32\_ComputerSystem where DomainRole = 5 2. Configure the PDC External Time Group Policy with the WMI Filter you just created |  |
| 1. Switch to the policy editing mode and go to the section Computer Configuration > Policies > Administrative Templates > System > Windows Time Service > Time Providers. Enable the policy Enable Windows NTP Client and edit the Configure Windows NTP Client policy |  |
| 1. Specify the following policy settings: 2. Enabled 3. NtpServer: 0.pool.ntp.org,0x8 1.pool.ntp.org,0x8 2.pool.ntp.org,0x8 4. Type: NTP 5. CrossSiteSyncFlags: 2 6. ResolvePeerBackoffMinutes: 15 7. ResolvePeerBackoffMaxTimes: 7 8. SpecialPollInterval: 1024 9. EventLogFlags: 0 |  |
| 1. On TMDC05 – Run the following: w32tm /config /syncfromflags:domhier /update 2. net stop w32time && net start w32time |  |
| 1. w32tm /query /peers |  |
| 1. net stop w32time 2. w32tm /unregister 3. w32tm /register 4. net start w32time |  |
| 1. gpupdate /force |  |
| 1. gpresult /z |  |
| 1. Verify NTP Settings via GPO |  |
| 1. Check the W32 Peers list that has been set via GPO  w32tm / query /peers |  |
| 1. Next, let’s move the FSMO Roles to TMDC06  Move-ADDirectoryServerOperationMasterRole -identity TMDC06 -OperationMasterRole PDCEmulator,RIDMaster,InfrastructureMaster,SchemaMaster,DomainNamingMaster |  |
| 1. Verify that the roles have moved by running netdom query fsmo |  |
| 1. Run gpupdate /force to remove the NTP Policy from TMDC05 2. Run gpresult /z to view the policies applied 3. You should see the policy removed |  |
| 1. Validate the NTP Peer Settings  w32tm /query /peers |  |
| 1. From an administrative PowerShell Enter-PSSession -ComputerName TMDC06 2. Cmd.exe 3. Gpupdate /force 4. Gpresult /z |  |
| 1. W32tm /query /peers |  |

### Exercise 1.13 – Recommended Settings for Virtual Domain Controllers Guest Time Settings

Disabling integrated services time sync on domain controllers is paramount, especially in environments where hypervisors operate outside the primary domain infrastructure. In many cases, hypervisors reside in separate Active Directory forests and domains, making it crucial to prevent time configurations from being pushed down from the hypervisors to the virtual machines (VMs). Here's why this practice is essential:

1. **Preventing Time Drift:**

* Enabling integrated services time sync on hypervisors can result in time configurations being pushed down to VMs. This can lead to time drift issues, where VMs' clocks become out of sync with the domain controllers and other systems.
* Time drift can cause synchronization issues, impacting critical operations such as AD replication and user logons.

1. **Impact on Production:**

* Time discrepancies in virtualized environments can have severe consequences on production systems. Applications and services that rely on accurate timekeeping may experience errors or failures.
* For example, authentication mechanisms in AD rely on precise time synchronization. Any discrepancies can lead to authentication failures, disrupting access to resources and services.

1. **Best Practice Recommendations:**

* It is considered a best practice to disable time sync settings in hypervisors altogether for environments where VMs are domain-joined.
* By disabling integrated services time sync, administrators retain control over time synchronization settings within the domain, ensuring consistency and accuracy across all systems.

Disabling integrated services time sync on domain controllers is critical for preventing time drift issues and ensuring accurate time synchronization within the Active Directory environment. By implementing an automated solution to configure NTP settings based on PDC Emulator role transfers, administrators can effectively manage time synchronization and minimize the risk of disruptions to critical operations.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMHVHost |  |
| 1. Open Hyper-V Management Console |  |
| 1. Right Click on TMDC03 and click Settings 2. Click |  |
| 1. Click on Integration Services, and Uncheck Time Synchronization |  |
| 1. Repeat on the rest of the DCs in the lab |  |

### Exercise 1.14 – Update the Domain and Forest Functional Levels to Server 2025

Forest and Domain Functional Levels in Active Directory determine the available features and capabilities within an AD forest or domain. These levels dictate the minimum operating system requirements for domain controllers and enable specific functionality unique to each level. However, it's crucial to understand that raising the functional levels is a one-way process, meaning there's no going back once the change is made.

1. **Forest Functional Level**:
   * The Forest Functional Level represents the capabilities and features available at the forest-wide level.
   * It determines the highest Windows Server operating system that can be used for domain controllers within the forest.
   * Features such as Active Directory Recycle Bin, Fine-Grained Password Policies, and Domain Controller Read-Only Domain Controller (RODC) compatibility are enabled based on the forest functional level.
   * Raising the forest functional level affects all domains within the forest.
2. **Domain Functional Level**:
   * The Domain Functional Level determines the capabilities and features available within a specific domain.
   * It dictates the minimum operating system requirements for domain controllers in the domain.
   * Features such as Authentication Mechanism Assurance, Protected Users group, and Kerberos AES encryption are enabled based on the domain functional level.
   * Raising the domain functional level affects only the specific domain in which the change is made.
3. **One-Way Process**:
   * It's important to emphasize that raising the functional levels is irreversible. Once the levels are raised, there's no option to revert to a lower level (except for an Authoritative Restore of Active Directory).
   * Administrators should carefully consider the implications and thoroughly test their environment before proceeding with the change.
   * Proper planning and documentation are essential to mitigate potential risks and ensure a smooth transition.
4. **Windows Server 2025 Functional Levels**:
   * With the introduction of Windows Server 2025, new Forest and Domain Functional Levels are available, specifically tailored for Server 2025.
   * These functional levels introduce enhanced features and security capabilities that can only be leveraged when all domain controllers within the forest or domain are running Windows Server 2025.
   * Organizations planning to upgrade to Windows Server 2025 should consider the benefits of these new functional levels and ensure that their environment is prepared for this change.

Understanding Forest and Domain Functional Levels is crucial for managing an Active Directory environment effectively. Administrators should carefully evaluate the impact of raising functional levels and ensure proper planning and testing before making any changes, considering that these changes are irreversible. Additionally, organizations using Windows Server 2022 should assess the benefits of upgrading to Server 2025 functional levels to take advantage of the latest Active Directory features and capabilities.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDC05 and Techmentor\Administrator |  |
| 1. Open an Administrative PowerShell prompt and run the following: 2. Get-ADDomain | select domain mode, DistinguishedName |  |
| 1. Get-ADForest | select forestMode |  |
| 1. Get-ADDomain –identity techmentor.com |  |
| #Run against the PDC Eumulator   1. c |  |
| 1. #Update the Forest Functional Level 2. $pdc = Get-ADDomainController -Discover -Service PrimaryDC 3. Set-ADForestMode -Identity $pdc.Domain -Server $pdc.HostName[0] -Forest Windows2025Forest |  |
| 1. Get-ADDomain | select domainMode, DistinguishedName 2. Get-ADForest | select forestMode |  |

### Exercise 1.15 – Configure a Domain Controller in Azure (Instructor Demo)

In this lab, we've already set up Azure Hybrid Connectivity by configuring a local Site-to-Site (S2S) VPN on the Host. This VPN allows connectivity to our Azure Tenant. Now, we're leveraging this connectivity to extend our Active Directory (AD) services to the cloud.

1. **Azure Hybrid Connectivity:**

* There is a Site-to-Site VPN connected to the instructor's lab. This will provide bi-directional connectivity between 192.168.11.0/24 and 172.16.0.0/24

1. **Extending AD to the Cloud:**

* We're taking a Virtual Machine (VM) configured on the 172.16.0.x/24 subnet in Azure.
* By extending our AD services to this Azure VM, we can have local logins for any cloud resources that will be moved.

1. **Authentication for Cloud Resources:**

* This extended AD service also serves as a source of authentication for migrating our Remote Desktop Session Host Infrastructure (RDSH) to Azure Virtual Desktop.
* It ensures seamless authentication for users accessing resources in the cloud while maintaining internal accounts for authentication.

By establishing Azure Hybrid Connectivity and extending our AD services to cloud, we're enabling seamless access to cloud resources while maintaining centralized authentication and security through our existing AD infrastructure. This setup streamlines the migration process and ensures consistent user experience across both on-premises and cloud environments.

***NOTE: Instructor you must update the NSG network Security Gateway in Azure with the IP Address of the instructor demo VM with the Virtual Network Gateway External IP. You must also change the Local Network Gateway to have the public IP Address of the Instructor demo VM. Once done on the host machine you should be able to connect using Routing and remote Access on the IKEV2 VPN. The Azure LAB VM must also be turned on and has a pre-configured Static IP of 172.16.0.4. All static routes and transit routes to the lab have been pre-configured in the Lab VM Image template.***

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMAZINSTDC01 and Techmentor\Administrator |  |
| 1. As this is a repeat of Lab Exercise 1.4 we are not going to include screen shots. Run the following commands in an Admin PowerShell Prompt | Install-WindowsFeature AD-Domain-Services  Import-Module ADDSDeployment -verbose  $Credential = Get-Credential  Test-ADDSDomainControllerInstallation -DomainName Techmentor.com  Install-ADDSDomainController -CreateDnsDelegation:$false -InstallDns:$true -DatabasePath 'C:\Windows\NTDS' -DomainName 'Techmentor.com' -Credential $Credential |
| 1. With the DNS Record cleared up it should look like this during the install. Although running in Azure it is pretty much the same as running on-prem |  |
| 1. One note for Domain Controllers in Azure is that all Virtual Networks are DHCP in Azure. If you get a STATIC IP it is basically the same as giving a reservation. 2. Never change an Azure VM from DHCP. 3. How you would change this is on the Network Interface connected to the Domain Controller Azure VM. We can change from Dynamic to Static in here. |  |
| 1. The last thing we would need to Change for our Azure Domain Controller enabled Virtual Network is the default DNS Settings on the Virtual network |  |
| 1. Changing this to Custom basically takes the DHCP setting from Azure DNS to your own. Because we want to have DNS Pointing to this domain controller for future objects we could change this to 172.16.0.4 2. Because this is a shared VNET for the lab we will leave this setting alone and manually modify any resources requiring connectivity. For production you would likely way to change this. 3. Please don’t change this setting in the lab. |  |
| 1. When the Domain Controller Reboots we will get AD Connection Objects Replicating | ipconfig /registerdns  net stop netlogon & Net start netlogon  Repadmin /kcc  Repadmin /syncall /e /d /a  Repadmin /syncall /e /d /a /P |
| 1. Return to TMDC03 2. Next we will create AD Sites and Associate the Subnets so clients know where to authenticate. 3. Open DSSite.msc |  |
| 1. In the Name field type Azure and then Select DefaultSiteLink and click OK |  |
| 1. Click on Sites, Inter-Site Transports, IP, right click on DefaultSiteLink and click Properties 2. Modify the Replicate Every Attribute to 15 minutes which is the lowest possible Value and click OK. |  |
| 1. On Subnets create a new subnet defined as in the Screenshot. |  |
| 1. Move your new Azure Server to the Azure Site. |  |
| 1. After Replication Converges it should look like this. Congratulations you know have a Domain Controller running up in your Azure Tenant. |  |

Lab 2

Windows Admin Center and Azure Hybrid Services

In this lab, we will explore the setup and configuration of Windows Admin Center, a powerful tool for managing Windows Server environments. Following the initial setup, we will extend our capabilities by integrating Azure Arc and Azure Hybrid Services. This integration is crucial for creating a seamless management experience between on-premises and cloud environments, providing numerous benefits such as enhanced security, scalability, and streamlined operations.

Lab Objectives

1. **Setting Up Windows Admin Center:**

* Begin with basic configurations of Windows Admin Center.
* Understand its interface and primary features.
* Learn how to manage Windows Servers and other Windows-based infrastructure from a centralized, browser-based platform.

1. **Enabling Azure Arc:**

* Extend the hybrid management capabilities by integrating Azure Arc.
* Learn how Azure Arc enables management of on-premises servers and services as if they were native Azure resources.
* Understand the benefits of Azure Arc for resource organization, policy enforcement, and governance.

1. **Integrating Azure Hybrid Services:**

* Integrate Windows Admin Center with Azure Hybrid Services.
* Enable and configure services such as Azure Backup, Azure Site Recovery, and Azure Monitor.
* Discover how these services enhance data protection, disaster recovery, and monitoring for on-premises environments.
* Importance of Using Azure Hybrid Services

1. **Unified Management:**

* Windows Admin Center, combined with Azure Hybrid Services, provides a unified management interface for both on-premises and cloud resources.
* This unification simplifies administrative tasks, reduces the learning curve, and improves operational efficiency.

1. **Enhanced Security and Compliance:**

* Azure Hybrid Services offer advanced security features, including Azure Security Center integration, which provides security recommendations and threat protection for hybrid environments.
* Compliance is easier to manage with consistent policies applied across on-premises and cloud resources using Azure Policy.

1. **Scalability and Flexibility:**

* Hybrid services allow organizations to scale their infrastructure seamlessly by leveraging cloud resources when needed.
* Workloads can be dynamically moved or extended to Azure, providing flexibility to handle varying demands.

1. **Cost Efficiency:**

* Utilizing Azure Hybrid Services can be more cost-effective by optimizing resource usage and taking advantage of Azure's pay-as-you-go model.
* Organizations can avoid over-provisioning on-premises resources by extending workloads to the cloud as necessary.

1. **Business Continuity:**

* Services like Azure Backup and Azure Site Recovery ensure data protection and disaster recovery, enabling quick recovery from outages or data loss incidents.
* This capability is critical for maintaining business continuity and minimizing downtime.

1. **Improved Monitoring and Insights:**

* Azure Monitor and other monitoring tools provide comprehensive insights into the health and performance of both on-premises and cloud resources.
* Proactive monitoring helps in identifying and resolving issues before they impact operations.

Lab Workflow

1. **Initial Setup:**

* Install Windows Admin Center
* Verify the installation of Windows Admin Center.
* Perform basic configuration tasks.

1. **Azure Arc Integration:**

* Register on-premises servers with Azure Arc.
* Explore management capabilities provided by Azure Arc.

1. **Enabling Azure Hybrid Services:**

* Configure Azure Site Recovery
* Use Azure Site Recovery to Migrate VMs to Azure
* Optionally Configure Azure Backup, Azure Monitor, and Azure Extended Network through Windows Admin Center.
* Test and validate the integration.

By the end of this lab, you will have a solid understanding of how Windows Admin Center and Azure Hybrid Services work together to create a robust, scalable, and secure hybrid IT environment. This knowledge is essential for modern IT administration, where hybrid cloud strategies play a critical role in optimizing infrastructure and operations.

### Exercise 2.1- Configure Windows Admin Center

In this exercise, we will begin by installing Windows Admin Center, a crucial tool for managing Windows Servers and other Windows-based infrastructure from a single, centralized, browser-based platform. The installation process involves downloading the Windows Admin Center setup package, running the installer, and configuring the necessary settings such as network ports and user access permissions. Once installed, we will proceed with the base configurations, including connecting to our servers, setting up role-based access control, and integrating essential management extensions. This setup will lay the foundation for extending our capabilities with Azure Arc and Azure Hybrid Services, enabling a seamless hybrid management experience.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. On the Hyper-V Host Computer, open PowerShell ISE as administrator |  |
| 1. Download and install Windows Admin Center | ## Download the msi file  Invoke-WebRequest 'https://aka.ms/WACDownload' -OutFile "$pwd\WAC.msi"  ## install windows admin center  $msiArgs = @("/i", "$pwd\WAC.msi", "/qn", "/L\*v", "log.txt", "SME\_PORT=443", "SSL\_CERTIFICATE\_OPTION=generate")  Start-Process msiexec.exe -Wait -ArgumentList $msiArgs |
| 1. Open Edge and browse to [https://localhost](https://localhost:6516) 2. Click Advanced and accept the Security Warnings to continue. | Graphical user interface, text, application, email  Description automatically generated |
| 1. If any updates are available, ensure you are on the latest version   This process can take 10-15 minutes to complete. |  |
| 1. Click on Skip Tour | Graphical user interface, text, application  Description automatically generated |
| 1. Click on your Hyper-V Host Machine |  |
| 1. Verify that Windows Admin Center connects and is working |  |

### Exercise 2.2 - Connecting Windows Admin Center to Azure Hybrid Services

In this exercise, we will configure Windows Admin Center by registering your gateway with Azure. Following the installation, we will connect the Windows Admin Center gateway to your Azure account, enabling cloud-based features and integrations. This registration process involves signing in to Azure, granting necessary permissions, and configuring the gateway settings. Once registered, you can leverage Azure Hybrid Services, such as Azure Backup, Azure Monitor, and Azure Security Center, directly from the Windows Admin Center interface. This setup is a crucial step in extending the platform's capabilities for comprehensive hybrid management and integration with Azure.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
|  |  |
| 1. Open Edge and browse to <https://localhost> 2. Click Advanced and accept the Security Warnings to continue. | Graphical user interface, text, application, email  Description automatically generated |
| 1. Select your Lab VM it should be the only object in Windows Admin Center at this point. Click Manage As and use the credentials TMAdmin with the lab password |  |
| 1. On the Specify Credentials screen select Use these Credentials for All Connections and Click Connect. 2. Note: If you don’t type the credentials Windows Admin Center has issues with this localhost Machine. |  |
| 1. Next, Click on your Lab VM it looks like a hyperlink with [Gateway] |  |
| 1. Click on Azure Hybrid Center and click on Register your Windows Admin Center Gateway |  |
| 1. On the Get Started with Azure in Windows Admin Center, click on Copy on Copy this Code 2. Then click on Enter the code | Graphical user interface, application  Description automatically generated |
| 1. Edge Browser will open and paste the code in and click next | Graphical user interface, application  Description automatically generated |
| 1. On the Register, the gateway with Azure, click Copy Code and click Device Logon 2. When prompted, log in using tmazadmin@checkyourlogs.net  Your Instructor has provided the login at the beginning of class. |  |
| 1. Make sure to click the skip for NOW!!! Do not set up MFA on this account |  |
| 1. On the More information required page, click next |  |
| 1. IT IS SUPER IMPORTANT that you always click cancel on this screen. 2. We use a shared account to access the lab, and we don’t want an MFA setup. |  |
| 1. On the Are you were trying to sign in to Windows Admin Center page, click Continue |  |
| 1. On the Windows Admin Center Page, it should display this message | Graphical user interface, text, application  Description automatically generated |
| 1. Return to Windows Admin Center, and in the Get Started with Azure in Windows Admin Center prompt, choose the correct Azure Active Directory Tenant ID 2. In Azure Active Directory Application click Create New and click Connect |  |
| 1. Once connected, you will see a green checkbox beside Now Connected to Azure AD. 2. Click Sign In | Graphical user interface, text, application  Description automatically generated |
| 1. You will see a pop-up dialog box check Consent on Behalf of your Organization and click Accept. |  |
| 1. In Windows Admin Center Hybrid Center, click on Sign in Azure Hybrid Center | Graphical user interface, text, application, chat or text message  Description automatically generated |
| 1. You will see Loading Azure Service Information | A picture containing scatter chart  Description automatically generated |
| 1. Review all the options available | Graphical user interface, text, application, email  Description automatically generated |
|  |  |

### Exercise 2.3 - Test Failover to Azure using Azure Site Recovery

In this lab exercise, we will perform a test failover of the virtual machine TMFile01 or TMDC01 to Azure using Azure Site Recovery (ASR). This process will demonstrate how to protect and recover critical workloads in the event of an outage or disaster. Azure Site Recovery will be integrated into our Hyper-V Host Server through the deployment of Site Recovery Agents, all managed via Windows Admin Center.

We will begin by setting up the Site Recovery Vaults using Windows Admin Center, which simplifies the configuration and management of ASR. It is important to note that Microsoft offers Site Recovery Vaults free of charge for the first 31 days, allowing for comprehensive testing without incurring costs. This exercise will cover the steps to configure ASR, replicate the chosen virtual machine to Azure, and execute a test failover to ensure that the VM can be successfully restored and brought online in the Azure environment.

By completing this exercise, you will gain hands-on experience with Azure Site Recovery, understand its integration with Windows Admin Center, and learn how to effectively use this powerful tool to ensure business continuity and disaster recovery for your virtual machines.

Note: Your Instructor must assign your student number as it will be used to uniquely identify your Site Recovery Vault that will be created in the steps below. It follows the format Student00(x). Please make sure to read the instructions and adjust when required as documented.

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. There are 2 VM’s that we won’t use for this lab that need to be deleted. They have orphaned Virtual Disks and this will cause the setup of Site Recovery to fail. 2. Delete TMS2D01 and TMS2D02 prior to starting this lab via Hyper-V manager. |  |
| 1. From the Hyper-V Host Server, open Edge and browse to <https://localhost> 2. Click on the Host Server 3. Click on Azure Site Recovery Setup |  |
| 1. On the Setting up a host with Azure Site Recovery page, Select the Use Existing Resource Group radio button and select rgtmlab 2. On the Recovery Services Value, select the create new radio button and type TMLABStudentXXX  Where XXX is your assigned Student Number for the Lab 3. Ensure the region is set to Canada Central and click Setup |  |
| 1. You can view the progress in the bell notification area in Windows Admin Center |  |
| 1. During our testing in the lab, we noticed that sometimes the setup would fail with the following error message. 2. We find that Azure Hybrid Services can tend to be a bit buggy and can throw various errors. 3. If you didn’t see any errors proceed to step 23 |  |
| 1. To re-run the setup of Azure Site Recovery from Windows Admin Center again, we need to remove to installed binaries.   Microsoft Azure Recovery Services Agent and Microsoft Azure Site Recovery Provider  Once removed, you can simply reload the windows admin center and retry the setup again |  |
| 1. Click on Start and type Add remove Programs 2. In addremove program, browse to Microsoft Azure Recovery Services Agent and Click Uninstall |  |
| 1. Click on Microsoft Azure Site Recovery Provider and click Uninstall |  |
| 1. Close Edge Browser and reopen |  |
| 1. Re-open windows admin center by typing <http://localhost> on edge 2. Click on your Hyper-V Host System 3. Click on Azure Site Recovery Setup |  |
| 1. On the Setting up a host with Azure Site Recovery page, select use existing resource group rgtmlab 2. Select use existing recovery services vault TMLABStudentXXX  Where XXX is your student number 3. Click Setup |  |
| 1. This time we will see if it works |  |
| 1. Yes it did |  |
| 1. On the Virtual Machines Node, Select TMFile01 or TMDC01 |  |
| 1. Click on manage and select Replicate using Azure Site Recovery |  |
| 1. On the Protect TMFile01 with Azure Site Recovery, click use existing for storage account sttmlab and click protect VM |  |
| 1. You should see a green checkmark in a few minutes with Protecting VM with Azure Site Recovery 2. It will take about 15 minutes to replicate this VM completely 3. In the meantime, repeat the above steps to replicate TMDC01 as well. |  |
| 1. Logon to Portal.Azure.com using [TMAZADmin@Checkyourlogs.net](mailto:TMAZADmin@Checkyourlogs.net) 2. On the home page, search for recovery |  |
| 1. Only work in your pre-assigned Recovery Vault |  |
| 1. In the Recovery Vault, click on Replicated Items |  |
| 1. You will see your VM here 2. Once it changes to a state of protected, you may proceed |  |
| 1. Click on the VM 2. Click on the test failover button at the top  We are going to fail this over to Azure, which will spin up a new Azure VM for us to provide validation and testing. |  |
| 1. On the Test Failover, Validation warning, click the red text to click here to continue. |  |
| 1. Change the VM name to STUDENTVMXXX Where XXX is your student number 2. Select the Virtual Network TMVNET2 3. Select Network interfaces and target network interface type of primary 4. Select Azure Hybrid Benefits YES 5. Select I Confirm I have an eligible Windows Server license with Software Assurance or Windows Server Subscription to apply to this azure hybrid benefit. |  |
| 1. At the top, click Save |  |
| 1. You will see a notification bell icon with updating the failover configuration for your VM |  |
| 1. On your VM in Replicated Items, click Test Failover again |  |
| 1. On the Test Failover Wizard, select tmvnet2 for Azure virtual network |  |
| 1. You can view the progress via the bell Icon. If you click the Starting the test failover of TMDC01, it will take you further into the step-by-step notifications. |  |
| 1. Return to the Azure Homepage 2. Click on Virtual Machines |  |
| 1. In a few minutes, you will see temp VMs being created. These are your test failover VMs. The name will change as soon as it is complete with the test failover. |  |
| 1. If you check in the bell icon progress, you can drill into further details |  |
| 1. Now we see the job is complete 2. You can also view these under site recovery jobs in the recovery services vault. |  |
| 1. Return to Virtual Machines, and you will see your VM Created 2. Click on your VM |  |
| 1. Review how Azure Site Recovery configured your VM |  |
| 1. Scroll down to Boot Diagnostics 2. Notice that you will see your VM either at a login prompt or already logged in. 3. Note: We have an autologin setup for some of the VMs in this lab. That is why it automatically logged in. |  |
| 1. Now that we are satisfied that our VM was Replicated and turned on, we will clean up the job. 2. Return to Replicated Items for your VM 3. Click on Cleanup Test Failover |  |
| 1. Click ok |  |
| 1. You can check the status of the jobs in the bell notification area |  |
| 1. You can also check the status of the job in the site recovery jobs in your recovery services vault |  |
| 1. Once completed, you will see everything as successful. Congratulations, you just performed your first live DR test to Azure. |  |
| 1. Now return to Virtual Machines and see the VM, and all objects have been removed. |  |

### Exercise 2.4 – Onboard Machines to Azure Arc

In this lab exercise, we will focus on onboarding machines to Azure Arc, enabling enhanced management and governance capabilities for your on-premises and multi-cloud environments. Azure Arc allows you to manage servers, Kubernetes clusters, and applications across various infrastructures as if they were native Azure resources.

We will start by installing the Azure Arc agents on our machines using Windows Admin Center, which simplifies the onboarding process. Once the machines are onboarded, they will appear on the Azure portal, where you can manage and monitor them alongside your other Azure resources.

Additionally, students are encouraged to explore other features and capabilities of Azure Arc beyond the scope of this lab exercise. For example, you can configure Azure Updates to manage patching and updates, set up Change Tracking to monitor changes in your environment, and investigate other management areas. Taking the initiative to explore these features in your own time will provide a deeper understanding of Azure Arc’s full potential and how it can enhance your IT operations.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. From the Hyper-V Host Server, open Edge and browse to <https://localhost> 2. Select the host system by selecting the checkbox to the left and click Connect to Arc |  |
| 1. Leave the Defaults and click Review & Setup |  |
| 1. In the notification bell area, you will see connecting systems to Azure Arc. |  |
| 1. In the Notification bell area, you will see successfully connected system to Azure Arc. |  |
| 1. Open the Azure Portal by going to portal.azure.com and searching for Azure Arc. Open Azure Arc and you should see you host machine in here. 2. Please note this is a shared lab tenant so please only work with your host machine. |  |
| 1. After Clicking on your host explore the available options. |  |
| 1. When you onboarded this system what Agent was Deployed? | The agent deployed to manage systems via Azure Arc is the **Azure Connected Machine Agent**. This agent facilitates the connection between your on-premises or multi-cloud servers and the Azure management plane, enabling you to manage and monitor these servers as if they were native Azure resources. Once the agent is installed and the machine is onboarded to Azure Arc, you can leverage various Azure management services, such as Azure Policy, Azure Monitor, Azure Security Center, and others, to manage and secure your infrastructure effectively. |

### Exercise 2.4.1 – Manually Onboarding to Azure Arc via PowerShell

### Exercise 2.4.2 – Managing Updates on Servers using Azure Update via Azure Arc

### Exercise 2.5 – Azure Migrate Server Assessment

In this lab exercise, we will explore the Azure Migrate Server Assessments available through Windows Admin Center and the Azure Portal. Azure Migrate is a powerful tool that helps you assess your on-premises workloads for migration to Azure. It provides insights into the readiness, cost, and performance of your virtual machines when running in Azure.

We will begin by using Windows Admin Center to initiate the Azure Migrate assessment, which simplifies the process of discovering and assessing your on-premises servers. This tool integrates seamlessly with the Azure Portal, where you can view detailed reports and recommendations.

By the end of this exercise, you will understand how to leverage Azure Migrate to determine the feasibility and cost implications of moving your virtual machines to Azure. This assessment is crucial for planning and budgeting, as it provides a clear picture of the expected costs and potential performance benefits of running your workloads in the cloud.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. From the Hyper-V Host Server, open Edge and browse to <https://localhost> |  |
| 1. Click on Virtual Machines 2. Select TMFILE01 and click Manage 3. Select Assess for Azure Migration 4. If it gives a warning message about running VM’s Start the VM and try the assessment again. |  |
| 1. On the Azure Migrate Server Assessment configure as seen in the screenshot. 2. Change the Azure Migrate Project to your student #. 3. Click Create Assessment |  |
| 1. It will take a little while to complete. 2. Seems like a good time for a coffee. |  |
| 1. After a few minutes we can see that the results are up in the Azure Portal. |  |
| 1. Open Portal.Azure.Com 2. Open Azure Migrate |  |
| 1. Expand Migration Goals, Servers, Databases, and Web Apps and then click on Assess, Under Assessments, select AZURE VM (1) |  |
| 1. Select the assessment created by Windows Admin Center in our case Student Student00x-AZMIG01Assessment1 |  |
| 1. Review the results 2. Repeat and run on other VM’s to see the results as well. |  |

### Exercise 2.6 – Configure Azure Extended Network (Instructor Led Discussion)

In this discussion, we will explore the Azure Extended Network and the benefits of using VXLAN Software Defined Networking (SDN) to maintain the same IP subnet both on-premises and in the cloud. Azure Extended Network allows organizations to extend their on-premises IP address space into Azure, facilitating seamless hybrid connectivity and simplifying network management.

VXLAN (Virtual Extensible LAN) is a network virtualization technology that enables the creation of a Layer 2 overlay network on top of a Layer 3 infrastructure. By leveraging VXLAN, Azure Extended Network allows you to extend your on-premises subnets to Azure, ensuring that virtual machines (VMs) in the cloud can use the same IP addresses as those on-premises. This capability is particularly beneficial for scenarios requiring low-latency communication, simplified IP address management, and maintaining application consistency across hybrid environments.

While this lab environment does not support the additional configurations required to fully implement Azure Extended Network and VXLAN, understanding these technologies provides valuable insights into advanced hybrid connectivity options. These solutions enable seamless integration and migration strategies, allowing for a more flexible and cohesive network infrastructure between your on-premises environment and Azure.

By discussing these options, students will gain a better understanding of the potential benefits and considerations of extending their networks to Azure, preparing them for more complex hybrid cloud implementations in real-world scenarios.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. From the Hyper-V Host Server, open Edge and browse to <https://localhost> 2. Click Azure Hybrid Center, Click Azure Extended Network and then click Set up |  |
| 1. This opens the Windows Admin Center Extensions Page and ensure that you select Azure Extended Network and click Install. |  |
| 1. Open your Host Machine back up in Windows Admin Center and you will see Azure Extended Network |  |
| 1. Click on Set Up |  |
| 1. IMPORTANT Note: This configuration requires the pre-setup of an Azure VM and an on-prem VM or Physical Machine. Both of these will have 2 network adapters installed and multiple virtual networks. 2. Traffic will pass to and from these Network Virtual Appliances both on-prem and in Azure. The purpose of these appliances is to tag traffic so that it understands that on-prem 192.168.11.x needs to route to the cloud Virtual Network of 192.168.11.x. 3. It seems weird because normally we can’t have overlapping subnets. However, with Azure Virtual Network this is the whole point. |  |
| 1. What are some benefits that you can see of Azure Extended Network technology? | Azure Extended Network offers several advantages for organizations looking to seamlessly integrate their on-premises and cloud environments. Some key benefits include:  **Seamless Failover with Azure Site Recovery:** Azure Extended Network allows virtual machines (VMs) to retain their on-premises IP addresses when failed over to Azure. This ensures immediate failover capabilities without the need to reconfigure IP settings, making disaster recovery processes faster and more reliable.  **Simplified Migration with Azure Migrate:** When migrating VMs to Azure using Azure Migrate, maintaining the same IP subnet eliminates the need for reassigning IP addresses or reconfiguring network settings. This reduces downtime and simplifies the migration process, ensuring a smoother transition to the cloud.  **Consistent Network Configuration:** By extending the on-premises subnet to Azure, you can maintain a consistent network configuration across your hybrid environment. This simplifies network management, reduces the complexity of IP address planning, and ensures that applications and services can communicate seamlessly regardless of their location.  **Enhanced Application Availability:** With the ability to extend subnets, applications that require low-latency communication and depend on specific IP configurations can operate more efficiently. This is particularly beneficial for applications with stringent networking requirements or those that rely on hardcoded IP addresses.  **Improved Disaster Recovery Testing:** Extending the on-premises network to Azure enables more effective disaster recovery testing. You can simulate failovers and validate recovery plans without impacting the production environment, ensuring that your disaster recovery strategy is robust and reliable.  **Simplified Hybrid Cloud Management:** Azure Extended Network simplifies the management of hybrid cloud environments by providing a unified network infrastructure. This reduces the administrative overhead associated with managing separate IP address spaces and network configurations for on-premises and cloud resources.  By leveraging Azure Extended Network and VXLAN Software Defined Networking, organizations can achieve a more integrated and resilient hybrid cloud infrastructure, facilitating seamless failovers, efficient migrations, and consistent network configurations across on-premises and Azure environments. |

### Exercise 2.7 – Connect to Azure using Azure Network Adapter (Instructor Led Discussion/Demo Only)

In this lab exercise, we will explore the use of Azure Network Adapter to easily configure a Point-to-Site (P2S) VPN in Azure, allowing individual servers or machines to connect securely to Azure resources. Azure Network Adapter simplifies the process of setting up P2S VPNs by providing an intuitive interface within Windows Admin Center.

**Objectives:**

1. **Introduction to Azure Network Adapter:**

* Understand the purpose and functionality of Azure Network Adapter.
* Learn how it simplifies the configuration of P2S VPNs for connecting on-premises servers or machines to Azure.

1. **Configuring P2S VPN with Azure Network Adapter:**

* Access Windows Admin Center and navigate to the Azure Network Adapter section.
* Follow the guided steps to configure a P2S VPN connection.
* Specify the desired settings, including authentication method, address space, and DNS settings.

1. **Connecting On-Premises Servers to Azure:**

* Install and configure the Azure Network Adapter client on the on-premises servers or machines.
* Establish a secure VPN connection to Azure using the provided credentials and connection information.

1. **Testing Connectivity and Validating Configuration:**

* Verify the establishment of the P2S VPN connection from the on-premises servers to Azure.
* Test connectivity to Azure resources, such as virtual machines or Azure services, from the on-premises environment.

Key Takeaways:

* Azure Network Adapter simplifies the configuration of P2S VPNs, streamlining the process of connecting on-premises servers or machines to Azure resources.
* By leveraging Windows Admin Center, administrators can easily manage and monitor P2S VPN connections, ensuring secure and reliable connectivity between on-premises and Azure environments.
* This lab exercise provides hands-on experience with Azure Network Adapter, equipping participants with the knowledge and skills to implement secure VPN connections in their own environments efficiently.

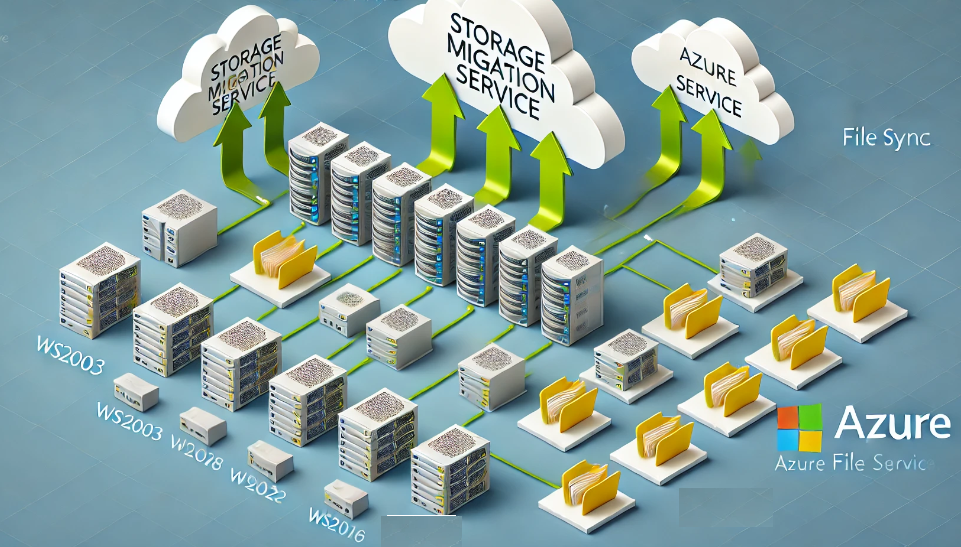
Through this lab exercise, participants will gain a deeper understanding of Azure Network Adapter and its role in enabling secure connectivity between on-premises infrastructure and Azure resources, ultimately enhancing their ability to manage hybrid cloud environments effectively.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. From the Hyper-V Host Server, open Edge and browse to <https://localhost> |  |
| 1. On the Add Azure Network Adapter page configure with the settings in the screen shot and then press create |  |
| 1. You should see the following message |  |
| 1. In the Virtual Network Gateway we can see that we now have a Point to Site Configuration Deployed. |  |
| 1. It can take 10-15 minutes for the new Azure Network Adapter to be displayed. |  |
|  |  |
| 1. View the Routing Table |  |
| 1. Try Ping to the running VM 172.16.2.5 2. Try to RDP to the running VM |  |
| 1. View the Deployment PowerShell Script that creates the P2S VPN with the Machine Cert |  |

Lab 3

Migrating File Servers

### Exercise 3.1 - Migrate TMFile01 using Windows Admin Center and the Storage Migration Service



In this lab exercise, we will explore the benefits and functionalities of the Storage Migration Service (SMS). The Storage Migration Service is a powerful tool designed to simplify the migration of servers to newer hardware or virtual machines. It facilitates the following key tasks:

1. **Inventory Management:**

* Inventory multiple servers and their data to get a comprehensive overview of the migration process.

1. **Rapid Data Transfer:**

* Quickly transfer files, file shares, and security configurations from source servers to destination servers.

1. **Identity Takeover:**

* Optionally take over the identity of the source servers (also known as "cutting over") so that users and applications can access existing data without any changes.

1. **Centralized Management:**

* Manage one or multiple migrations using the intuitive Windows Admin Center user interface.

**Objectives:**

In this lab, we will perform a migration from a Windows Server 2016 (TMFile01) to a Windows Server 2025 (Tmfile03) using Storage Migration Service via Windows Admin Center.

**High Level Steps:**

1. **Setup and Configuration:**

* Use Windows Admin Center on TMWAC01
* Install and configure Storage Migration Service on both the source (TMFile01) and destination (Tmfile03) servers.

1. **Inventory the Source Server:**

* Use SMS to inventory TMFile01, capturing all necessary data, file shares, and security configurations.

1. **Data Transfer:**

* Initiate and monitor the rapid transfer of files, file shares, and security configurations from TMFile01 to Tmfile03.

1. **Identity Cutover (Optional):**

* Configure the destination server (Tmfile03) to take over the identity of the source server (TMFile01), ensuring seamless access for users and applications.

1. **Validation:**

* Verify that all data has been successfully migrated and that Tmfile03 is functioning correctly with the transferred data and configurations.
* Ensure that users and applications can access the data on Tmfile03 without any issues.

**Key Takeaways:**

1. **Efficient Server Migrations:**

* Learn how Storage Migration Service streamlines the process of migrating data and configurations from old servers to new hardware or virtual machines.

1. **Minimized Downtime:**

* Understand how the identity takeover feature minimizes downtime and disruption for users and applications during the migration process.

1. **Centralized Management:**

* Gain experience in managing server migrations using the Windows Admin Center, enhancing your ability to handle multiple migrations efficiently.

By completing this lab exercise, participants will gain practical knowledge of the Storage Migration Service and its capabilities, enabling them to perform server migrations with minimal disruption and maximum efficiency in their own environments.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. From the Hyper-V Host System, open Edge Browser, and type https://TMWAC01.Techmentor.com   When prompted login as Techmentor\administrator |  |
| 1. Connect to tmwac01 and open the storage Migration Service tool | Graphical user interface, application  Description automatically generated |
| 1. Click on Install |  |
| 1. The installation will take a few minutes to complete. |  |
| 1. Note the three-step process for the Migration | Graphical user interface  Description automatically generated |
| 1. Click on New Job | Graphical user interface, application  Description automatically generated |
| 1. On the New Job window, type, MigrateTMFile01 and ensure Windows Servers and Clusters and click OK. | Graphical user interface, text, application, email  Description automatically generated |
| 1. Review the Check prerequisites window.  Does this scenario meet the requirements?   2016 to 2022 |  |
| 1. Under Enter Credentials for the devices you want to migrate. Use Techmentor\Administrator 2. Uncheck Migrate from Failover Clusters and click next |  |
| 1. Storage Migration Service will automatically deploy the prerequisites.  When done, click Next |  |
| 1. Click on Add a Device | Graphical user interface, text, application  Description automatically generated |
| 1. On Add source device, click on Active Directory search, choose Windows Server, type tmfile01, and select tmfile01.techmentor. Command click add. |  |
|  |  |
| 1. Did you notice the Inventory not Available message? |  |
| 1. Click on Start Scan | Graphical user interface, text, application, email  Description automatically generated |
| 1. Review the scan results and then click next |  |
| 1. On entering Credentials, use Techmentor\Administrator |  |
| 1. Return to Windows Admin Center select use an existing Server or VM 2. Type Tmfile03 and click scan |  |
| 1. If you see a similar error message while trying to scan the source or destination what could be the issue? 2. Start with step #1 physical layer one connectivity can you ping the server. 3. Does DNS resolve properly. 4. If DNS doesn’t resolve logon to TMDC05 and fix the issue. 5. Then try the scan again. 6. If the issue persists try logging into TMFILE03 and disable the firewall temporarily for the migration. |  |
| 1. Review the settings for Map each source volume and shares to transfer and click next. |  |
| 1. On Adjust transfer settings click next |  |
| 1. When prompted to specify credentials for this connection type techmentor\administrator |  |
| 1. The required features SMS-Proxy will be installed on Tmfile03 when complete click next. 2. This can take a few minutes to complete. 3. A little trick here if it looks like this is hung just hit the back button once and then next. |  |
| 1. Click on Validate |  |
| 1. Verify that it passes and click next | Graphical user interface, text, application  Description automatically generated |
| 1. Click on Start Transfer |  |
| 1. Validate that it completes successfully and click Next  If this hangs up, press F5 to refresh Windows Admin Center |  |
| 1. On the Cutover Enter Credentials prompt, click next | Graphical user interface, text, application, email  Description automatically generated |
| 1. On the Configure cutover from tmfile01.techmentor.com to tmfile03.techmentor.com 2. Configure the required network settings and click next | Graphical user interface, text, application, email  Description automatically generated |
| 1. On the Adjust Cutover Settings, enter new credentials of techmentor\administrator | Graphical user interface, text, application, email  Description automatically generated |
| 1. On the Validate source and destination, devices click validate | Graphical user interface, text, application, email  Description automatically generated |
| 1. Verify that everything looks ok | Graphical user interface, application  Description automatically generated |
| 1. Click next to proceed | Graphical user interface  Description automatically generated |
| 1. On start, the cutover click Start cutover | Graphical user interface, text, application  Description automatically generated |
| 1. Verify that everything looks good. Click Finish | Graphical user interface, text, application, email  Description automatically generated |
| 1. Check the corporate shares and ensure there is still access | Graphical user interface  Description automatically generated |
| 1. Turn off the old File Server |  |

### Exercise 3.2 - Migrate Tmfile03 to Azure Files using Windows Admin Center (Instructor Led Demo)

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. From the Hyper-V Host Server, open Edge and browse to <https://tmwac01.techmentor.com> 2. Add a connection to TMFILE01 |  |
| 1. Click on Azure File Sync 2. Click on Setup |  |
| 1. On the Getting Started with Windows Admin Center click on Copy Code and Enter Code 2. When prompted to login use the [TMAZAdmin@Checkyourlogs.net](mailto:TMAZAdmin@Checkyourlogs.net) account. 3. Same password as the previous lab. 4. Remember to not enroll with MFA for the lab. |  |
| 1. Create a new Entra ID Application by selecting Create New and clicking Connect 2. Finally click Sign in |  |
| 1. On the Setup Azure File Sync page choose Canada Central as the region and click the Set up button at the bottom. |  |
| 1. You will see progress like prepping the resource group, Creating the Storage Sync Service, Installing Agent and Registering with Azure 2. Note: To view this in the Azure portal search for the Storage Sync Service |  |
| 1. We can see that it is successfully setup. |  |
| 1. In Azure File Sync select Sync a Folder |  |
| 1. In Sync a Folder type c:\shares\accounting for the local share name 2. Use your Student # and type Student00(x)syncgroup 3. In Azure File Share to sync with type your student number with Student00xazfs01 |  |
| 1. In the Storage account use your student number and type student00(x)st01 2. Click on Set up Sync |  |
| 1. You can view the progress in the notification Bell Area |  |
| 1. Your instructor will give you a walkthrough of the following | Review of the Storage Sync Services in the Azure Portal  Review of the Storage Account and File Share Settings in the Azure Portal  Mapping a Drive to the Cloud File Share  Checking the Scheduled Tasks Assoicated with the Storage Sync Service |

Lab 4

Upgrading IIS Servers

An upgrade of IIS Servers can be very subjective as Websites are rarely built using flat architectures. Typically, we see multi-tier web farms connecting as applications to a SQL Database tier and then reaching into various data warehouses for historical reporting. Also, there are a lot of organizations that build their web applications which means that extensive testing is required with their development teams. For example, we will migrate a MySQL instance driving a WordPress site in this lab. Therefore, IIS could be a lab guide, and migrations should be treated with great care.

### Exercise 4.0 - Backup the IIS Server

Before performing any upgrade, you must backup the server. We will use a Hyper-V Checkpoint, but this might be Azure Backup or Azure Site Recovery in production.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Logon to your Hyper-V host server |  |
| 1. Open Hyper-V Manager Right-Click on TMWEB02 Checkpoint |  |

### Exercise 4.1 - Installing WordPress, PHP, and MySQL using PowerShell on Server 2012R2 using PowerShell (Instructor Guided)

To migrate something in the lab, we have first to set up a test site. I figured it would be great to use WordPress as a distributed application using IIS as the front end. This will also be an excellent test to check extensions to IIS, such as PHP and Web cache. These are very commonly installed, making this a great real-world example.

***LAB NOTE: It should only take about 10 minutes to complete the installation of WordPress and MySQL. During the downtime take a minute to make a few notes about your application and web servers in your environment. Start thinking about what it will take to get these upgraded and updated. Write down some of your questions and feel free to ask your instruction about options for your scenarios as time permits.***

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Logon to TMWEB02 as techmentor\administrator |  |
| 1. Open an administrative PowerShell ISE and type: | New-Item -Itemtype Directory -Path C:\ -Name Post-Install  [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12  Invoke-WebRequest -Uri " https://raw.githubusercontent.com/dkawula/Operations/master/Techmentor/HOL-OnlineMay2024/Install-Wordpress.ps1" -OutFile "C:\Post-Install\Install-WordPress.ps1" |
| 1. Open c:\post-install\Install-WordPress with PowerShell ISE Administrator and execute the script 2. Copy the WordPress Password into the clipboard |  |
| 1. On the Nuget Provider popup, click yes |  |
| 1. On the untrusted repository, click yes to all |  |
| 1. It will take a few minutes to install |  |
| 1. Don’t close the PowerShell ISE window. 2. Copy the Randomly Generated Passwords to a notepad file. |  |
| 1. Open <http://localhost> in Chrome 2. On the WordPress Startup page, click English and click Continue |  |
| 1. On the WordPress Configuration Screen, click Let’s Go |  |
| 1. On the Database connection details page, type WordPress for the username and paste the password from the script above 2. Click Submit |  |
| 1. Click Run the Installation |  |
| 1. On the Information Needed page, type an admin username and password and enter an email address 2. Click Install WordPress |  |
| 1. After the Install, click Login |  |
| 1. On the login page, type the user name and password from above |  |
| 1. View and customize the page as much as you like. |  |
|  |  |

### Exercise 4.2 – Azure Migrate Appliance Configuration (Instructor Led Demo)

In this lab exercise, we will focus on the installation and configuration of the Azure Migrate appliance, a crucial tool for assessing and migrating on-premises servers, applications, and databases to Azure. The Azure Migrate appliance is essential for discovering and analyzing your on-premises environment, providing detailed insights into workloads, performance metrics, and dependency mappings. These insights are vital for planning and executing a seamless migration to Azure. During this lab, you will learn how to deploy the Azure Migrate appliance in your environment, connect it to your Azure subscription, and initiate the discovery process. This will involve setting up the necessary prerequisites, such as ensuring network connectivity and proper permissions, configuring the appliance using the Azure Migrate portal, and running initial assessments to gather data about your infrastructure. By the end of this exercise, you will be proficient in using the Azure Migrate appliance to facilitate informed and efficient migration strategies, ensuring a smooth transition to the cloud.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Open Portal.Azure.Com and click on Azure Migrate |  |
| 1. We should have an existing Azure Migrate Project that was created from the Windows Admin Center VM Assessment done earlier. 2. Click on Servers, Databases, and Web Apps 3. Click on Discover and select using Appliance |  |
| 1. On the Discover page review the settings |  |
| 1. Click on Generate Key 2. This key will be used to register the appliance with the Azure Migrate Project in the Azure Tenant |  |
| 1. Click on Download .VHD – NOTE: For the lab prior to downloading make sure to change the download path to the temp drive running d: in the Azure Labs VM |  |
| 1. Copy the Azure Migrate Key |  |
| 1. Extract the .ZIP file |  |
| 1. Open Hyper-V Manager and Import the VM Appliance. |  |
| 1. Set the Path to D:\Temp and the path to the extracted ZIP containing the appliance |  |
| 1. Select the Virtual Machine AzureMigrateAppliance |  |
| 1. On the Choose Import Type Page leave the default of Register the Virtual Machine in-place (use the existing unique ID) |  |
| 1. On the Connect Network page change the Virtual Network to VSW02. |  |
| 1. Complete the Import |  |
| 1. Boot up the Azure Migrate Appliance and set a default Administrator Password. 2. This Appliance is a Sysprepped Virtual Machine with all of the components pre-installed |  |
| 1. Run the Azure Migrate Appliance Configuration shortcut on the Desktop |  |
| 1. On the Appliance Configuration manager Cloud:Public Page enter the Key Copied Earlier and complete the configuration by entering the details and credentials of the machines to scan. |  |
| 1. You can review more information on the process here | [Azure App Service assessments in Azure Migrate Discovery and assessment tool - Azure Migrate | Microsoft Learn](https://learn.microsoft.com/en-us/azure/migrate/concepts-azure-webapps-assessment-calculation) |
| 1. Your can review more information on the process here | [Tutorial to assess web apps for migration to Azure App Service - Azure Migrate | Microsoft Learn](https://learn.microsoft.com/en-us/azure/migrate/tutorial-assess-webapps?pivots=asp-net) |
| 1. You will need to login to your Azure Tenant |  |
| 1. Set the Credentials of the Hyper-V Host Lab Machine |  |
| 1. Add the Discovery Source this will change on a per student basis. 2. Run an Ipconfig /all on your student machine to verify. |  |
| 1. Make sure Validation is successful |  |
| 1. It will take about 10 minutes to complete the discovery |  |
| 1. Return to the Azure Migraton blade in the Azure Portal. 2. We can now click on Manage and see our discovered items in here. |  |

### Exercise 4.3 –Using Azure App Service Migration Assistant to Migrate Sites | Web Apps (Instructor Led Demo)

In this lab exercise, we will use the Azure App Service Migration Assistant to migrate existing websites to Azure App Service. The Azure App Service Migration Assistant is a free tool that simplifies the migration process by assessing your on-premises websites for compatibility with Azure App Service and then seamlessly migrating them. During this lab, you will learn how to download and install the Migration Assistant, run a compatibility assessment on your websites, and follow the guided steps to migrate them to Azure. This includes configuring the necessary Azure App Service resources, such as App Service Plans and Web Apps, and verifying the successful migration of your site. By the end of this exercise, you will have hands-on experience in using the Azure App Service Migration Assistant, making it easier to transition your web applications to the cloud with minimal downtime and effort.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. One of the items that is missing is a detailed process to help us migrate web apps and web applications to Azure. 2. Microsoft has developed the Azure App Service Migration Assistant to help us with this process 3. In this exercise, we will migrate the wordpress deployment to Azure using the Azure App Service migration Assistant. |  |
| 1. Download App Service Migration Assistant and install on TMWEB02 | <https://go.microsoft.com/fwlink/?linkid=2091900> |
| 1. There is also an option to download the App Service Migration Scripts.zip file |  |
| 1. Run the installer |  |
| 1. Open the AppServiceMigration Assistant |  |
| 1. On the Azure App Service Migration Assistant page ensure that choose site shows WordPress. |  |
| 1. On the Azure App Service Migration Assistant Page Assessment Report page ensure there are no errors. |  |
| 1. Review the settings |  |
| 1. We can see that there is an error in here that the database string is using a value of local host. 2. The App Migration Assistant will migrate the IIS Settings to Azure but not the DataBase this needs to be done manually. |  |
| 1. Review all the Successfully review settings |  |
| 1. Login to Azure |  |
|  |  |
| 1. Choose the Azure Migrate Project to associate this with. |  |
| 1. Select the options as directed in the screen shot |  |
| 1. Wait until the migration is complete |  |
| 1. Review the results |  |
| 1. Try Connecting to the Website 2. It is normal at this point to have the database error as we haven’t migrate the MYSQL portions required for Wordpress |  |
| 1. This does showcase that the App Migration tool will migrate website content to Azure Web Apps with ease. |  |

### Exercise 4.4 - Backup the IIS Server

Before performing any upgrade, you must backup the server. We will use a Hyper-V Checkpoint, but this might be Azure Backup or Azure Site Recovery in production.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Logon to your Hyper-V host server |  |
| 1. Open Hyper-V Manager Right-Click on TMWEB02 Checkpoint |  |

### Exercise 4.5 - Upgrading from 2012R2 to Windows Server 2022 Double Swing (Deprecated) – Review Only

Now we perform an in-place of Windows Server 2012 R2 to Windows Server. This mirrors what you will see in production, as many upgrades never directly go as planned. Therefore, it is essential to build up an upgrade LAB environment for your organization that mirrors production as closely as possible.

Often, we will do a direct restore of production to create a live test environment to test production upgrades. This particular upgrade will test the upgrade of the operating system and supportability for in-place upgrades of MySQL, PHP, and WordPress as an application stack. It is imperative to test all upgrades once applications get involved thoroughly, and it can get complicated swiftly. We hope you enjoy this lab exercise.

We call this a double swing migration because it is not possible to directly upgrade from Server 2012R2 to Server 2022. First, we need to upgrade to Server 2019 and then to Server 2022.

**NOTE: Once Server 2025 releases you will be able to upgrade directly to Server 2025!**

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Logon to TMWeb02 |  |
| 1. Open an Administrative PowerShell ISE and run the following to see which version of IIS we are currently on.  We case we are on IIS **8.5.9600.16384** | $w3wpPath = $Env:WinDir + "\System32\inetsrv\w3wp.exe"  If(Test-Path $w3wpPath) {  $productProperty = Get-ItemProperty -Path $w3wpPath  Write-Host $productProperty.VersionInfo.ProductVersion  }  Else {  Write-Host "Not find IIS."  } |
| 1. As it turns out for us, someone left behind an unattend.xml file in the root of the c: 2. The problem is future upgrades will look there. This one is designed for Server 2012r2, and we are trying to install Server 2019. If an unattend.xml file exists you must delete it prior to the upgrade. |  |
| 1. Go ahead and delete the unattend.xml file. |  |
| 1. In the Hyper-V Console click on File, Settings, Click on SCSI Controller and add a DVD Drive and click ok. |  |
| 1. On TMWEB02 Hyper-V Console, click on Media, Click on DVD Drive and click Insert Disk |  |
| 1. We have pre-downloaded this for the lab in the E:\ISO Folder. 2. Click Open to Mount the Server 2019 ISO |  |
| 1. Open Windows Explorer in TMWEB02 and double click D: |  |
| 1. On the Get updates, drivers, and optional features page, select not right now and click next |  |
| 1. On the select image page, select windows server 2019 standard (Desktop Experience) and click next |  |
| 1. On the Applicable notices and license terms page, click accept |  |
| 1. This is a widespread problem. This issue is that Server 2012 R2 is in Evaluation Mode. It can only be upgraded using Evaluation Media. There is a bug with the Download site at Microsoft, so we had to use full media. As you can see, we have an issue. 2. This problem can be solved by converting the version from Evaluation to Licensed Media; we will do that now. 3. First, go ahead and close the Setup |  |
| 1. Click start run and type winver 2. You can verify the version of windows here is indeed an evaluation edition. |  |
| 1. Open an Administrative Command Prompt 2. Type dism /online /get-currentedition  We can see that we are on Server Standard Eval |  |
| 1. Type dism /online /get-targeteditions  We can see that target editions for the upgrade are only non-evaluation versions |  |
| 1. Type Dism /online /set-edition:ServerStandard /productkey: D2N9P-3P6X9-2R39C-7RTCD-MDVJX /accepteula and press enter 2. When prompted, press Y to reboot. |  |
| 1. Log in as Techmentor\Administrator |  |
| 1. Click Start, click Run and type winver  Now notice we have changed the edition to non-evaluation media. |  |
| 1. Open Windows Explorer in TMWEB02 and double click D: |  |
| 1. On the Get Updates, Drivers and options features page, select the not right now radio button and click next |  |
| 1. On the Select Image page, click Windows Server 2019 Standard (Desktop Experience) and click next |  |
| 1. On the Applicable notices and license terms, click Accept |  |
| 1. On the choose what to keep, select the Keep personal files and apps radio button and click next |  |
| 1. On the Rady to install page, click Install |  |
| 1. While waiting for the installation, it is a great time to grab a refreshment |  |
| 1. Go ahead and log in as Techmentor\Administrator |  |
| 1. Verify the version upgrade by clicking start and typing winver 2. We can see that we are indeed on Server 2019 now |  |
| 1. Validate that the WordPress Site is still working by opening chrome and typing <http://localhost> |  |
| 1. Now it is time to try the upgrade to Server 2022 2. On the Hyper-V Console for TMWeb02, click on Media and DVD Drive |  |
| 1. On the Hyper-V console for TMWEB02, click on media and click DVD Drive |  |
| 1. Browse to e:\ISO and select the en-us\_Windows\_Server\_2022 iso and click open |  |
| 1. On the Install, Windows Server Page, click Next |  |
| 1. On the product key type VDYBN-27WPP-V4HQT-9VMD4-VMK7H and click next  This is the KMS Server 2022 key |  |
| 1. On the select image page, click Windows Server 2022 Standard (Desktop Experience) |  |
| 1. On the Applicable notices and license terms page, click accept |  |
| 1. On the choose what to keep page, click keep files, settings, and apps and click next |  |
| 1. On the Getting updates page, click next |  |
| 1. On the ready to install page, click install |  |
| 1. Wait about 15-20 minutes |  |
| 1. Once completed, log in as Techmentor\Administrator 2. Click Start and type winver 3. You can now see we are on Server 2022 |  |
| 1. Verify WordPress by opening Chrome and typing http://localhost |  |

### Exercise 4.6 – Migrating Web Server to Azure (Instructor Led)

In this lab exercise, we will focus on migrating an entire web server to Azure using Azure Site Recovery (ASR). Azure Site Recovery is a robust disaster recovery and migration solution that enables you to replicate on-premises servers to Azure, ensuring business continuity and simplifying migration processes. During this lab, you will learn how to configure Azure Site Recovery to replicate a web server, prepare your Azure environment, and initiate the failover process to migrate your web server to the cloud. This includes setting up the Recovery Services vault, installing the ASR agent on the web server, and configuring replication settings. You will also test the failover process to ensure a smooth transition with minimal downtime. By the end of this exercise, you will be adept at using Azure Site Recovery to migrate web servers to Azure, leveraging the cloud for greater scalability, reliability, and ease of management.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Open the Site Recovery Vault 2. Click on Replicated Items 3. Select TMWEB02 |  |
| 1. Click on Test Failover |  |
| 1. Configure the Azure Virtual Network |  |
| 1. It will take 5-10 minutes to complete |  |
| 1. Wait until complete |  |
| 1. Once successful move to the Virtual Machines Blade |  |
| 1. Click on the TMWEB02-Test |  |
| 1. Connect using Azure Bastion Host and ensure the Techmentor Test Site comes up 2. We have successfully ported the webserver VM to Azure. 3. Review the settings in IIS Manager as well. |  |

Lab 5

Migrating Print Servers

The new thought process for managing print servers is asking this question. Is IT in the business of managing print servers anymore? New Azure Universal Print options can organizations seriously consider moving to pure cloud-based printing. We will cover two scenarios in this lab: a traditional migration and an evaluation of Azure Universal Print and its viability.

### Exercise 5.0 – Configuring TMPrint01

In this exercise, we will configure TMPrint01 as a print server. This was not preconfigured in this lab, so you will need to take a few minutes to complete these steps, so we have something to migrate off to Server 2022.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Logon to TMPrint01 as Techmentor\Administrator 2. In Server Manager, click on Add Roles | A screenshot of a computer  Description automatically generated |
| 1. On the Before you begin page, click Next | A screenshot of a computer error  Description automatically generated |
| 1. On the Select Server Roles page, click Print and Document Services and click next | A computer screen shot of a server rules  Description automatically generated |
| 1. On the Print and Document Services information page, click Next | A screenshot of a computer screen  Description automatically generated |
| 1. On the Select Role, Services click Next | A screenshot of a computer  Description automatically generated |
| 1. On the Confirm Installation Selections, click Install | A screenshot of a computer  Description automatically generated |
| 1. On the Install Result Page, Click Close | A screenshot of a computer  Description automatically generated |
| 1. In Server Manager, expand Roles, Print and Document Services 2. Right Click on Printers and click add printer | A computer screen shot of a computer  Description automatically generated |
| 1. On the Printer Installation Page, select the add a TCP/IP or Web Services Printer by IP Address or Hostname and click next | A screenshot of a computer  Description automatically generated |
| 1. On the Printer, Address page, select TCP/IP Device 2. On Host Name or IP Address, type 192.168.11.222 3. On the Port Name, type 192.168.11.222 and click Next | A screenshot of a computer  Description automatically generated |
| 1. On the Additional Port, information required page, click Next | A screenshot of a computer error message  Description automatically generated |
| 1. On the Printer Driver Page, select the install a new driver radio button and click next | A screenshot of a computer  Description automatically generated |
| 1. On the Printer Installation page, select Fuji Xeron and FX AP-II 3000 PCL and click next | A screenshot of a computer  Description automatically generated |
| 1. On the Printer Name and Sharing Settings page, type Accounting\_Printer in Printer Name 2. Type Accounting\_printer on Share Name and click next | A screenshot of a computer  Description automatically generated |
| 1. On the Printer Found page, click next | A screenshot of a computer  Description automatically generated |
| 1. Repeat the steps above to create two more printers 2. IT\_Printer and Sales\_Printer 3. It doesn't matter what drivers or port IPs you use. 4. We just want three printers for the next steps. | A screenshot of a computer  Description automatically generated |
| 1. Verify the printers exist in the Printer Management Console | A computer screen shot of a printer  Description automatically generated |

### Exercise 5.1 – Exporting the Windows Server2016 Print Server’s Configurations

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Logon to TMPrint01 as Techmentor\Administrator 2. Open the Print Management Console and review the settings 3. In our example, we have three printers deployed via group policy: Accounting\_Printer, IT\_Printer, and Sales\_Printer 4. These are mapped via UNC path [\\TMPrint01](file:///\\TMPrint01) |  |
| 1. In the Print Management Console, we will first export the configuration by clicking Migrate Printers |  |
| 1. We will try and open up Paint on the server for this test. |  |
| 1. On the Printer, Migration window, select this print server ([\\TMPrint01](file:///\\TMPrint01)) and click next |  |
| 1. On the Printer, Migration summary click next |  |
| 1. On the Select, the file location, click next |  |
| 1. On the exporting screen, click finish |  |
|  |  |
| 1. Rename TMPRINT01 to TMPRINT01-OlD 2. Reboot TMPrint01 |  |
|  |  |

### Exercise 5.2 – Importing the Print Server’s Configurations into Windows Server 2022

When configuring the new print server, we will want to add a couple of final steps to impersonate the old Print Server. This is done because users can always manually map printers on the network and these will be configured using the old printer name. These printers will have already been configured to use a print server alias like CorpPrintServer or something like this in a perfect world. Usually, this is not the case, and we have to perform the following steps below to get this working.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Logon to TMPrint02 as Techmentor\Administrator 2. Install the Print Management Role using PowerShell ISE  add-windowsfeature print-server -verbose   add-windowsfeature RSAT-Print-Services -Verbose |  |
| 1. Open the Print Management Console, Right Click on TMPrint02 and click import printers from a file |  |
| 1. On the Select the file location page, type [\\tmprint01-old\c$\post-install\tmprint01.printerexport](file:///\\tmprint01-old\c$\post-install\tmprint01.printerexport) and click next |  |
| 1. On the Printer Migration Review page, click next |  |
| 1. On the Select import options page, click next |  |
| 1. The Import wizard will take about 1 minute to complete; once done, click finish |  |
| 1. Verify that the printers are available by opening windows explorer and typing [\\tmprint02](file:///\\tmprint02) |  |
| 1. Next, we will work to steal the name of TMPrint01 by disabling strict name-checking. 2. Download the Script for this by executing the code on the right in PowerShell ISE on TMPrint02 | New-Item -Itemtype Directory -Path C:\ -Name Post-Install  Invoke-WebRequest -Uri " https://raw.githubusercontent.com/dkawula/Operations/master/Active%20Directory/DisableStrictNameChecking.ps1" -OutFile "C:\Post-Install\DisableStrictNameChecking.ps1" |
| 1. There will be one error, but the script did work. 2. Restart TMPrint02 |  |
| 1. Log on to TMDC03 and open the DNS Management Console. 2. RightClick on Techmentor.com and select New Host (A or AAAA) |  |
| 1. On the New Host Page, type TMPRINT01 and put the IP Address of 192.168.11.101 and click add the host |  |
| 1. Remain on TMDC03 and open windows explorer 2. Browse to [\\tmprint01](file:///\\tmprint01) 3. Browse to tmprint02 4. Remember we renamed TMPRINT01 to TMPRINT01-old, so TMPRINT01 is TMPRINT02. 5. Why do we want to steal the Name of TMPRINT01?   Think about mapped Drives or Shared Printers as shortcuts or manually created throughout the enterprise.  By stealing the name, all of those old mappings will still work and create a transparent feel to the migration and cut down on the service desk tickets. |  |

### Exercise 5.3 – Step by Step walkthrough Microsoft Universal Print

In this lab exercise, we will explore the configuration of Universal Print, a Microsoft 365 service that modernizes and replaces traditional print servers. Universal Print provides a scalable, cloud-based print management solution that is especially beneficial for organizations managing hybrid environments with Intune. During this lab, you will follow a virtual walkthrough of the configuration steps required to set up Universal Print. This includes connecting printers to Universal Print, configuring printer settings, and managing print jobs from the cloud. You will also learn how to integrate Universal Print with Intune for seamless endpoint management, enabling you to deploy printers to users and devices efficiently. By the end of this exercise, you will understand how to leverage Universal Print to simplify your print infrastructure, reduce on-premises hardware dependencies, and enhance print management across hybrid environments.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. From a browser launch this URL for the Guided Walkthrough | [Universal Print Guided Simulation (regale.cloud)](https://regale.cloud/Microsoft/viewer/1265/universal-print/index.html#/0/0) |

Lab 6

Hardening Windows Server

### 6.1 Locking Down Windows Server 2019/2022 and Windows 10/11 with Group Policy Security Baselines via Security Compliance Toolkit 1.0

As you can see above, we are still quite vulnerable with this installation of Windows 10. The administrator is a next, next finish into production type of administrator. There are a lot of Security Lockdown recommendations that Microsoft, Mitre, and the Center for Internet Security Recommend. The lesson above is that if you give elevated rights, not much out there can protect you. You need to complete the lockdown.

Microsoft's free security baselines for Modern Operating Systems are available via the Security Compliance Toolkit 1.0. In the light exercise, we will look at the templates for hardening Windows Server 2022. The current Operating System of our Virtual Machine TMFILE03 is Windows Server 2022.

You must find the right security baseline and harden, import the group policy object and apply it to this server. Then validate the functionality of Windows Admin Center as the core application running on this server.

You will then find the appropriate Security Baselines to harden TMDC03, a Windows Server 2022 Active Directory Domain Services Domain Controller. Next, you will also need to set the Windows Server 2019, Windows 10 and Windows 11 systems in the lab. Once completed, we will review the Security recommendations via Microsoft Defender Advanced Threat Protection and close any remaining Security holes.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Log on to TMDC03, download the Microsoft Security Compliance Toolkit 1.0 and Extract it. | <https://www.microsoft.com/en-us/download/details.aspx?id=55319>  A screenshot of a computer  Description automatically generated |
| 1. Review all of the baselines. By default, these have been downloaded to the Downloads folder. 2. With this, we now have coverage for the older out of support operating systems as well as the in support versions from 2012R to Server 2022 3. Extract the Windows 10 Version 2004 4. Extract the Windows 10 version 1809 and Server 2019 Security Baseline 5. Extract the Server 2022 Security Baseline 6. Extract Windows 11 Security Baseline 7. Copy the extract folders to c:\post-install | Graphical user interface, text, application  Description automatically generated |
| 1. Open the c:\post-install\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\Documentation folder | This is an excellent location for your documentation listing the differences in GPOs between versions and what is configured.  As mentioned earlier, what is missing is the descriptive Windows Server Role Base Security Hardening Guidance.  We recommend looking at the Center for Internet Security (CIS) Benchmarks. They do an excellent job documenting all of this. Therefore, for the lab, we will proceed with these templates without making any changes.  As time permits, you are welcome to review all of these settings and determine if there will be issues in your environment.  **WE DO NOT Recommend importing these into a production environment without first going through extensive testing.**  The Policy Analyzer tool that comes with the toolkit can be used to compare what you have in production to what the changes will look like. Unfortunately, it is out of scope for this book, but we highly recommend looking at this tool. |
| 1. Next, open PowerShell as Administrator 2. Change Directory to c:\post-install\Windows 11 Security Baseline\Windows11-Security-Baseline-Final\Scripts | Text  Description automatically generated |
| 1. Run Baseline-Adimport.ps1 | Text  Description automatically generated |
| 1. Open the Group Policy Management Console and verify that the Group Policy Object (GPO) was imported successfully | Graphical user interface, text, application, email  Description automatically generated |
| 1. Repeat the steps above to import the Server 2022 Security Baselines | Text  Description automatically generated |
| 1. Repeat the steps for the Windows Server 2019 Security Baselines | Text  Description automatically generated |
| 1. Repeat the steps from the Windows 10 Security baselines | Text  Description automatically generated |
| 1. Verify that the baseline GPOs have been imported into the Group Policy Management Console |  |
| 1. Yup, it looks good | Graphical user interface, table  Description automatically generated with medium confidence |
| 1. Next, we will need to organize our Active Directory before putting these policies in. 2. Open Active Directory Users and Computers 3. For the lab, create the highlighted Organization Units 4. We will link the Baselines to these OU’s for testing purposes in our Lab | Graphical user interface, text, application  Description automatically generated |
| 1. Move TMDC03 to the Server 2022 DCs OU 2. Move TMMGMT01 to the Windows 10 Desktops OU 3. Move TMMGMT01 to the Windows 11 Desktops OU 4. Move TMWAC01 to the Windows Server 2019 Member Servers OU | Graphical user interface, text, application  Description automatically generated |
| 1. Create two new user objects for testing on Windows 10 and 11 called Windows10 Users and Windows11 Users; place each user in their Desktops OU | Graphical user interface, text, application, email  Description automatically generated |
| 1. On the Windows 10 Desktops OU link MSFT Windows 10 2004 Bitlocker, Computer, Defender Antivirus, User, and Domain Security | A screenshot of a computer  Description automatically generated with medium confidence |
| 1. On the Windows, 11 Desktops Link MSFT Windows 11 – Bitlocker, Computer, Credential Guard, Defender Antivirus, Domain Security, User | Text  Description automatically generated |
| 1. On the Windows Server 2019 Member Servers OU Link MSFT Windows 10 1809 and Server 2019 – Defender Antivirus, Domain Security, Member Server Credential Guard, Member Server | Text  Description automatically generated |
| 1. On the Windows Server 2022 Member Servers OU Link MSFT Windows Server 2022 – Defender Antivirus, Domain Security, Member Server, and Member Server Credential Guard | Text  Description automatically generated |
| 1. On Server 2022 DCs OU link MSFT Windows Server 2022 – Domain Controller, and Domain Security GPOs | Graphical user interface, text, application  Description automatically generated |
| 1. Reboot TMMGMT01, TMMGMT02, TMDC03, TMFILE03 |  |
| 1. Logon to TMWAC01 notes the popup message about User Account Control being enabled now. 2. Go ahead and reboot again. 3. We can see that user account control is now enabled on this system for administrative actions. | Text  Description automatically generated Graphical user interface, application  Description automatically generated |
| 1. Logon to TMDC03, open an administrative command prompt and run gpresult /z 2. Try replicating with the other 2008R2 Domain Controllers. Does it still work? Repadmin /syncall still works 3. We can see the UAC is now enabled on this Server | A picture containing application  Description automatically generated  Text  Description automatically generated |

Lab 7

Migrating DHCP

The process of migrating DHCP can be done in a few different ways. Our preferred method is a one-time complete migration of all Scopes and settings. Other methods include moving scope by scope using PowerShell. However, for this lab, we will focus on the method we have been using with our consulting services teams.

### Exercise 7.1 - Migrate DHCP by moving the DHCP Database

This lab exercise will show you the fastest way to migrate a DHCP Database by taking the DHCP.mdb file from one DHCP server to another. This method is not a slow cutover but a 100% over during a maintenance window. This method has proved successful for our team over the past ten years. Also included is the PowerShell method for DHCP Import and Export.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
|  |  |
| 1. Logon to TMDHCP02 as Techmentor\Administrator |  |
| 1. Open an Administrative PowerShell Prompt 2. Install the DHCP Role Add-WindowsFeature DHCP -IncludeMangementTools |  |
| 1. Click Start run type dhcpmgmt.msc and press enter 2. In the DHCP Management Console right, click on TMDHCP02 and click Authorize 3. Ensure that it is authorized with Active Directory Domain Services (ADDS) |  |
| 1. Right Click on TMDHCP02, click all tasks and click Stop |  |
| 1. In Windows, Explorer browse to c:\windows\system32\dhcp 2. Delete all of the existing files from c:\windows\system32\dhcp |  |
| 1. Return to TMDHCP01 and open the DHCP Management Console. 2. Review the Active Leases on TMDHCP01 |  |
| 1. In the DHCP Management Console, Right Click on TMDHCP01, click all tasks and click Stop |  |
| 1. Return to TMDCHP02 and open windows explorer. 2. Copy the DHCP Database from TMDHCP01 to TMDHCP02   [\\tmdhcp01\c$\windows\system32\dhcp](file:///\\tmdhcp01\c$\windows\system32\dhcp)  You ONLY need to copy the DHCP.MDB file. |  |
| 1. Note the IP Address configuration of TMDHCP01 192.168.11.6 2. To complete the migration, we will steal the IP Address. 3. Why is this step the essential part of a DHCP Migration?   A. DHCP Lease information on a click includes the source DHCP Server. If you don’t steal the IP, the clients will attempt to get a new IP Address, and the Lease migration will not work properly. Stealing the IP ensures they communicate with the now 12-year newer version of DHCP. |  |
| 1. On the Hyper-V Host Lab Server, Open the Hyper-V Management Console, Right Click on TMDHCP01 and click Turn Off |  |
| 1. Return to TMDHCP02 2. Configure the IP Address on TMDHCP02 with DHCP 1’s old IP Address |  |
| 1. Open the DHCP Management Console, right-click on THDHCP02, click all tasks and click Start |  |
| 1. Review the Lease information on TMDHCP02 |  |
| 1. Review the files in c:\windows\system32\DHCP 2. Notice how the Jet Engine Database Log Files regenerated themselves. |  |
| 1. Optional - Turn on TMPrint02 and validate that DHCP is working from the log files on TMDHCP02  The log file to check will depend on which day of the week you are running this lab. In my case, it was Saturday that I was testing. So I opened the DHCPSrvLog-Sat.log in c:\windows\system32\dhcp   Did TMDHCP02 successfully assign an IP Address from the Pool?  ITPRO Note: If you are using Microsoft DHCP like this and you are ever trying to figure out the DHCP Address of a BMC, IPMI, ILO, or DRAC interface on one of your servers checking the DHCP Logfiles is a super-fast way to find their default IP's when provisioning new Servers. |  |

Lab 8

Migrating DNS

You are migrating DNS when Active Directory Integrated is relatively easy because the DNS Zone information is stored in Active Directory partitions. Therefore, replication of DNS information can be either Forest or Domain-wide. However, you can still have standalone non-Active Directory-integrated zones that need to be migrated as part of your migration journey to Windows Server 2022. The exercises below will show you how to migrate Forward and Reverse lookup Zones using PowerShell.

### Exercise 8.1 – Migrate Primary Forward Lookup Zone by copying the Zone Database File

This exercise will migrate a forward lookup zone by copying the existing zone database file “.dns” from c:\windows\system32\dns on the source server to the target. Then once copied, we will recreate the forward lookup zone using the existing file.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Logon to TMDC03 |  |
| 1. Open dnsmgmt.msc |  |
| 1. Right Click on Forward Lookup Zones and click New Zone |  |
| 1. On the New Zone, Wizard Page, click Next |  |
| 1. On the Zone Type page, select the Primary Zone radio button and click next |  |
| 1. On the Zone, Name Page, type Techmentorlab.local in the Zone Name and click Next |  |
| 1. On the Zone File Page, select Create a new file with this file name and click next |  |
| 1. On the Dynamic Update, leave the defaults and click next |  |
| 1. On the Completing the New Zone Wizard page, Click Finish |  |
| 1. Right, Click on the Techmnetorlab. local zone and click New Host (A or AAAA) record |  |
| 1. On the New Host page, type Testserver and in the IP Address field, type 1.1.1.1. 2. Repeat the steps for TestServer2 – 1.1.1.2 and WebServer – 1.1.1.3 |  |
| 1. We just wanted a few records in there that we can use to validate the successful migrations |  |
| 1. Browse to c:\windows\system32\DNS and verify that there is a file called techmentor.local.DNS  This is known as the zone database file. 2. Why do you not see the other zones for techmentor.com?  The Techmentor.com zone database is stored as an Active Directory Integrated Zone. Therefore, you will not see a physical file on the file system when this is selected. |  |
| 1. Next, we will Add TMDC04 to the DNS Management Console. 2. Right Click on DNS and click Connect to DNS Server |  |
| 1. On the Connect to DNS Server page, select the following computer radio button and type TMDC04 |  |
| 1. Expand TMDC04 and review the zones. 2. Note that the Techmentorlab.local zone has not been migrated |  |
| 1. Next we will copy the techmentorlab.local.dns zone database file from c:\windows\system32\dns to [\\tmdc04\c$\windows\system32\dns](file:///\\tmdc04\c$\windows\system32\dns) |  |
| 1. Return to the DNS Management Console 2. Right Click on TMDC04 Forward Lookup Zones and click new zone |  |
| 1. On the New Zone, Wizard Page, click Next |  |
| 1. On the Zone, type Page, select the Primary Zone radio button and click Next |  |
| 1. On the Zone Name Page, type Techmentorlab.local and click Next |  |
| 1. On the Zone, File, select this existing file radio button. 2. Note how the name of the Zone Database File was automatically filled in, then click next |  |
| 1. On the Dynamic Updates Page, leave the defaults and click next |  |
| 1. On the Completing the New Zone Wizard page, click Finish |  |
| 1. Verify that the new zone has been created and that the three records exist |  |
| 1. Next, we will delete the Forward Lookup Zone Techmentorlab.local by right-clicking it and selecting delete. 2. We are doing this because we will be trying a different migration method next. |  |

### Exercise 8.2 – Migrate Primary Forward Lookup Zone by Converting a Secondary Zone to Primary Zone

In this exercise, we take the techmentorlab.local zone created on TMDC03 in the earlier exercise and Migrate it to TMDC04. This time, the method will have to use setup TMDC04 to host a secondary copy of the zone database file and then convert it to a primary zone to complete the migration.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Logon to TMDC03 |  |
| 1. Open dnsmgmt.msc 2. Verify that Techmentorlab.local does not exist on TMDC04 |  |
| 1. In the DNS Management Console, expand TMDC04, Right Click on Forward Lookup Zones and click New Zone |  |
| 1. On the New Zone Wizard, Click Next |  |
| 1. On the Zone, Type Page. Select the Secondary Zone radio button and click Next |  |
| 1. On the Zone Name page, in the Zone Name Field, type Techemntorlab.local and click next |  |
| 1. On the Master, DNS Servers Page, type 192.168.11.3 and click Next |  |
| 1. On the Completing the New Zone Wizard, Click Finish |  |
| 1. Refresh Techmentorlab. local, and you will notice an error message 2. Why is this not working? |  |
| 1. Try Right-clicking on the techmentorlab. local zone and click transfer new copy of the zone from master 2. Did that work? |  |
| 1. Why are Zone Transfers not working? |  |
| 1. Maybe we should check the settings on TMDC03 to see if Zone Transfers are allowed to TMDC04 |  |
| 1. Click on the Zone Transfers tab. 2. Does this look right? |  |
| 1. Select the Only to the following Servers radio button and type 192.168.11.4 and click ok |  |
| 1. On the Zone, properties click OK |  |
| 1. Refresh the Techmentorlab.local Zone again |  |
| 1. That seems to have done the trick |  |
| 1. Now that we can see the records, we can complete the migration. Currently, this is a Secondary Zone that is read-only. 2. Right Click on Techmentorlab.local and click properties |  |
| 1. On the General Tab, Click on the Change Button on the type field. |  |
| 1. On the Change Zone Type Page, select the Primary Zone radio button and click ok |  |
| 1. On the General Tab, not the type is now primary and click ok |  |
| 1. Refresh the Techmentorlab.local zone and note that the SOA “Start of Authority” record has changed from TMDC03 to TMDC04 |  |
| 1. Lastly, delete the Techmentorlab.local zone from TMDC04 again. We will try another method in the next exercise. |  |

Lab 9

Upgrading Storage Spaces Standalone from Server 2016 to Windows Server 2022

Microsoft supports the process of upgrading Storage Spaces and Storage Spaces Direct. We often use this process to upgrade production servers and backup targets. However, we still highly recommend that any data be verified with good backups before proceeding.

### Exercise 9.1 – In-Place Upgrading from Storage Spaces 2016 to 2022 – Review Only

This exercise will perform a double swing migration from Server 2016 Storage Spaces to Server 2022 Storage Spaces.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. On the Hyper-V Host, Right Click TMS2D01 and click Settings |  |
| 1. Click SCSI Controller and click DVD drive, then click Add |  |
| 1. Browse to e:\ISO 2. Select the ISO starting with 20348.169 |  |
| 1. If not running, Start TMS2D01 and logon as Techmentor\Administrator |  |
| 1. Review the Storage Spaces Configuration in Server Manager |  |
| 1. Open an Administrative Powershell Prompt and run the following commands.   Get-PhysicalDisk   Get-VirtualDisk  Get-StoragePool |  |
| 1. Review the File structure in windows explorer for the D. This is the virtual disk that is part of the Storage Pool. |  |
| 1. Don’t forget about that pesky unattend.xml file. 2. Go ahead and delete it. |  |
| 1. Double click on the E: |  |
| 1. Double click on Setup.exe |  |
| 1. On the Install Windows Server Page, Click Next |  |
| 1. On the Select, Image Page, Select Windows Server 2022 Datacenter Evaluation (Desktop Experience) and click next |  |
| 1. On the Applicable notices and license terms page, click accept |  |
| 1. Choose what to keep on the screen. Then, click the X at the top right to close the setup program. 2. It looks like that didn’t work. |  |
| 1. Why Did the Upgrade not work?   Is Server 2016 a valid Upgrade Path to 2022? |  |
| 1. From an administrative command prompt, run the command on the right. 2. When prompted, click y to reboot | You must run DISM /Online /Set-Edition:ServerStandard /ProductKey: CB7KF-BWN84-R7R2Y-793K2-8XDDG /AcceptEula |
| 1. On the Hyper-V Console for TMS2D01, click on media and DVD Drive and click insert |  |
| 1. Launch Setup |  |
| 1. On the Select Image Page, click Windows Server 2019 Datacenter (Desktop Experience) and click next |  |
| 1. On the Applicable notices and license terms, click accept |  |
| 1. On the choose what to keep page, click next |  |
| 1. On the ready to install page, click install |  |
| 1. It will take about 20 minutes to complete the install |  |
| 1. Logon as Techmentor\adminsitrator |  |
| 1. Review the Storage Spaces Configuration |  |
| 1. Open an administrative PowerShell prompt and run the following   Get-PhysicalDisk  Get-VirtualDisk  Get-StoragePool |  |
| 1. Now check the version of ReFS 2. Type fsutil fsinfo refsinfo d: and press enter 3. We can see the Version is 3.4, which indicates that it is Server 2019. |  |
| 1. From the Hyper-V Console for TMS2D01, click on Media and click DVD Drive and click insert disk 2. Insert the Server 2022 full media, not evaluation |  |
| 1. Launch the setup and on the Install, Windows Server Page, click next |  |
| 1. On the Product Key Page, type WX4NM-KYWYW-QJJR4-XV3QB-6VM33   This is the KMS Key   1. Click Next |  |
| 1. On the Select, Image Page, select Windows Server 2022 Datacenter (Desktop Experience) and click Next |  |
| 1. On the Applicable Notices and license terms, click accept |  |
| 1. On the Choose what to keep, select the keep files, settings, and apps and click next |  |
| 1. On the Ready to install page, click install |  |
| 1. The installation will take about 20 minutes |  |
| 1. When Completed, login as Techmentor\Administrator 2. Click Start and type winver 3. We can see we have been upgraded to Server 2022 |  |
| 1. From an Administrative PowerShell Prompt type   Get-PhysicalDisk  Get-VirtualDisk  Get-StoragePool |  |
| 1. Type fsutil fsinfo refsinfo d: 2. We can now see the refs version has been upgraded to Server 2022 (3.7) |  |
|  |  |

Lab 10

Upgrading WSUS from Windows Server 2012R2 to Windows Server 2019

There have been many different versions of WSUS since Server 2012 R2. Below are some of the versions listed:

Graphical user interface, application

Description automatically generated

Server 2012 R2 is Version 6.3.9600.18694

Graphical user interface, text, application

Description automatically generated

Server 2016 is Version 10.0.14393.2007

Graphical user interface, text, application

Description automatically generatedWindows Server 2022 is Version 10.0.17763,1

Essentially the Versions are very close between Windows Server 2016 and Windows Server 2022.

### Exercise 10.1 - Planning for WSUS Upgrade

The first step in the Upgrade of your Windows Server Update Services (WSUS) to Windows Server 2022 is to understand the supported and unsupported scenarios and the supported operating systems for this migration.

The following operating systems support the upgrade:

* **Windows Server 2012 R2 Standard Edition (Core)**
* **Windows Server 2012 R2 Standard Edition (Desktop Experience)**
* **Windows Server 2012 R2 DataCenter Edition (Core)**
* **Windows Server 2012 R2 DataCenter Edition (Desktop Experience)**
* **Windows Server 2016 Standard Edition (Core)**
* **Windows Server 2016 Standard Edition (Desktop Experience)**
* **Windows Server 2016 Datacenter Edition (Core)**
* **Windows Server 2016 Datacenter Edition (Desktop Experience)**

#### Supported Upgrade Scenarios

The following WSUS upgrade scenarios are supported:

Windows Server 2016 Standard and Datacenter editions can be used as source or destination servers.

With the previous in-place OS upgrade from Windows Server 2008 R2 to Windows Server 2012/R2, it was required to removed WSUS. This was due to a WSUS version change. This is no longer required, as Windows Server 2012/R2 and Windows Server 2016 use the same WSUS version

Per - <https://www.systemcenterdudes.com/inplace-os-upgrade-sccm-server/>

The version of WSUS will be acceptable from Windows Server 2016 to 2019, so we will just do an in-place upgrade in our case.

### Exercise 10.2 - In-Place OS Upgrade from Windows Server 2016 to 2019

Now we will upgrade to Windows Server 2019 by performing an in-place upgrade.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Logon to TMWSUS01 |  |
| 1. Open an Administrative PowerShell ISE and run the following to see which version of IIS we are currently on.  We can see that we are on IIS **10.0.14393.0** | $w3wpPath = $Env:WinDir + "\System32\inetsrv\w3wp.exe"  If(Test-Path $w3wpPath) {  $productProperty = Get-ItemProperty -Path $w3wpPath  Write-Host $productProperty.VersionInfo.ProductVersion  }  Else {  Write-Host "Not find IIS."  }  Graphical user interface, text  Description automatically generated |
| 1. Insert the Windows Server 2022 Media ISO and run setup.exe | Graphical user interface, application, Word  Description automatically generated |
| 1. On the Get Updates, Drivers, and optional Features, select Download updates, Drivers and optional features (Recommended) and click Next | Graphical user interface, text, application, website  Description automatically generated |
| 1. On the Product, Key Screen type your product key | Graphical user interface, application  Description automatically generated |
| 1. On the Version, make sure you match your version. If you don’t know, you can run msinfo32.exe to find out. | Graphical user interface, application, Teams  Description automatically generated |
| 1. On the licensing screen, click accept | Graphical user interface, text, application  Description automatically generated |
| 1. On the Choose what to keep the screen, select **Keep personal files and apps** and **click Next** | Graphical user interface, text, application  Description automatically generated |
| 1. Depending on the hardware, the upgrades typically take about 20-25 minutes in the field. | Graphical user interface, text, application  Description automatically generated |

### Exercise 10.3 - Post Upgrade Tasks

You will have a bit of cleanup to do when upgrading from Server 2016 to Windows Server 2022.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Logon to Management 01 |  |
| 1. Open Server Manager and run the Post-Deployment Configuration for WSUS | Graphical user interface, text, application  Description automatically generated |
| 1. Check Store Updates Locally | Graphical user interface, text, application  Description automatically generated |
| 1. Click Run | Graphical user interface, text, application, email  Description automatically generated |
| 1. Check the log in C:\Users\Administrator.MVPDAYS\appdata\local\temp\WSUS\_Postinstall….txt | Text  Description automatically generated |
| 1. Check the WSUS Services | Graphical user interface, text, application, email  Description automatically generated |
| 1. Change the Startup Type of the WSUS Service to Automatic and Start it | Graphical user interface  Description automatically generated with medium confidence |
| 1. The WSUS Console should now be back operational | Graphical user interface, text, application, email  Description automatically generated |
| 1. The WSUS server is synchronizing fine now. | Graphical user interface, text, application, email  Description automatically generated |

Lab 11

Upgrading a Storage Spaces Direct Cluster to Windows Server 2022

This topic describes how to upgrade a Storage Spaces Direct cluster to Windows Server 2022. There are four approaches to upgrading a Storage Spaces Direct cluster from Windows Server 2016 to Windows Server 2022, using the cluster OS rolling upgrade process—two that involve keeping the VMs running, and two that involve stopping all VMs. Each approach has different strengths and weaknesses, so select the one that best suits the needs of your organization:

* In-place upgrade while VMs are running on each server in the cluster—this option incurs no VM downtime, but you’ll need to wait for storage jobs (mirror repair) to complete after each server is upgraded.  **NOTE: A double swing migration is required to upgrade from Server 2016 to Server 2022.**
* Clean-OS installation while VMs are running on each server in the cluster—this option incurs no VM downtime. Still, you’ll need to wait for storage jobs (mirror repair) to complete after each server is upgraded, and you’ll have to set up each server and all its apps and roles again.
* In-place upgrade while VMs are stopped on each server in the cluster—this option incurs VM downtime, but you don’t need to wait for storage jobs (mirror repair), so it’s faster.
* Clean-OS install while VMs are stopped on each server in the cluster—This option incurs VM downtime, but you don’t need to wait for storage jobs (mirror repair), so it’s faster.

### Exercise 11.1 - Prerequisites and limitations

Before proceeding with an upgrade:

* Check that you have usable backups if there are any issues during the upgrade process.
* Check that your hardware vendor has a BIOS, firmware, and drivers for your servers that they will support on Windows Server 2022.

When upgrading a cluster with ReFS volumes, there are a few limitations:

* Upgrading is fully supported on ReFS volumes. However, upgraded volumes won’t benefit from ReFS enhancements in Windows Server 2022. These benefits, such as increased performance for mirror-accelerated parity, require a new Windows Server 2022 ReFS volume. In other words, you’d have to create new volumes using the New-Volume cmdlet or Server Manager. Here are some of the ReFS enhancements new volumes would get:
  + MAP log-bypass: a performance improvement in ReFS that only applies to clustered (Storage Spaces Direct) systems and doesn’t apply to stand-alone storage pools.
  + Compaction efficiency improvements in Windows Server 2022 that are specific to multi-resilient volumes
  + We recommend putting the server into storage maintenance mode before upgrading a Windows Server 2016 Storage Spaces Direct cluster server. See the Event 5120 section of Troubleshoot Storage Spaces Direct for more info. Although this issue has been fixed in Windows Server 2016, we recommend putting each Storage Spaces Direct server into storage maintenance mode during the upgrade as a best practice.
* There is a known issue with software-defined networking environments that use SET switches. This issue involves Hyper-V VM live migrations from Windows Server 2022 to Windows Server 2016 (live migration to an earlier operating system). To ensure successful live migrations, we recommend changing a VM network setting on VMs that are live-migrated from Windows Server 2022 to Windows Server 2016. This issue is fixed for Windows Server 2022 in the 2019-01D hotfix rollup package, AKA builds 17763.292. For more info, see Microsoft Knowledge Base article 4476976.

Because of the known issues above, some customers may consider building a new Windows Server 2022 cluster and copying data from the old cluster instead of upgrading their Windows Server 2016 clusters using one of the four processes described below.

### Exercise 11.2 - Performing an in-place upgrade while VMs are running

This option incurs no VM downtime, but you’ll need to wait for storage jobs (mirror repair) to complete after each server is upgraded. Although individual servers will be restarted sequentially during the upgrade process, the remaining servers in the cluster and all VMs will remain running.

|  |  |
| --- | --- |
| Instructions | Screenshot (if applicable) |
| 1. Logon to S2D01 |  |
| 1. Check that all the servers in the cluster have installed the latest Windows Updates |  |
| 1. If you are running Software Defined Networking with SET Switches, Open an Elevated PowerShell Prompt and run the following to disable VM live migration verification checks on all VMs on the cluster. | Get-ClusterResourceType -Cluster {clusterName} -Name "Virtual Machine" |  Set-ClusterParameter -Create SkipMigrationDestinationCheck -Value 1 |
| 1. Perform the following on one cluster server at a time: 2. Use Hyper-V VM live migration to move running VMs off the server you’re about to upgrade. |  |
| 1. Drain the Cluster Node by running | Suspend-ClusterNode -Drain |
| 1. Place the Server in Storage maintenance Mode by running | Get-StorageFaultDomain -type StorageScaleUnit |  Where FriendlyName -Eq <ServerName> |  Enable-StorageMaintenanceMode |
| 1. Get the operational status of the disks | Get-PhysicalDisk |
| 1. Insert the Windows Server 2022 Media ISO and run setup.exe | Graphical user interface, application, Word  Description automatically generated |
| 1. On the Get Updates, Drivers, and optional Features, select Download updates, Drivers and optional features (Recommended) and click Next | Graphical user interface, text, application, website  Description automatically generated |
| 1. On the Product, Key Screen type your product key | Graphical user interface, application  Description automatically generated |
| 1. On the Version, make sure you match your version. If you don’t know, you can run msinfo32.exe to find out. | Graphical user interface, application, Teams  Description automatically generated |
| 1. On the licensing screen, click accept | Graphical user interface, text, application  Description automatically generated |
| 1. On the Choose what to keep the screen, select **Keep personal files and apps** and **click Next** | Graphical user interface, text, application  Description automatically generated |
| 1. Depending on the hardware, the upgrades typically take about 20-25 minutes in the field. | Graphical user interface, text, application  Description automatically generated |
| 1. Fully Update the Node with Windows Updates |  |
| 1. Disable Storage Maintenance Mode | Get-StorageFaultDomain -type StorageScaleUnit |  Where FriendlyName -Eq <ServerName> |  Disable-StorageMaintenanceMode |
| 1. Resume the Cluster Node | Resume-ClusterNode |
| 1. Wait for the Storage Jobs to complete and for the Virtual disks to be healthy | Get-StorageJob  Get-VirtualDisk |
| 1. Logon to S2D2 |  |
| 1. Check that all the servers in the cluster have installed the latest Windows Updates |  |
| 1. Perform the following on one cluster server at the time:   Use Hyper-V VM live migration to move running VMs off the server you’re about to upgrade. |  |
| 1. Drain the Cluster Node by running | Suspend-ClusterNode -Drain |
| 1. Place the Server in Storage maintenance Mode by running | Get-StorageFaultDomain -type StorageScaleUnit |  Where FriendlyName -Eq <ServerName> |  Enable-StorageMaintenanceMode |
| 1. Get the operational status of the disks | Get-PhysicalDisk |
| 1. Insert the Windows Server 2022 Media ISO and run setup.exe | Graphical user interface, application, Word  Description automatically generated |
| 1. On the Get Updates, Drivers, and optional Features, select Download updates, Drivers and optional features (Recommended) and click Next | Graphical user interface, text, application, website  Description automatically generated |
| 1. On the Product, Key Screen type your product key | Graphical user interface, application  Description automatically generated |
| 1. On the Version, make sure you match your version. If you don’t know, you can run msinfo32.exe to find out. | Graphical user interface, application, Teams  Description automatically generated |
| 1. On the licensing screen, click accept | Graphical user interface, text, application  Description automatically generated |
| 1. On the Choose what to keep the screen, select **Keep personal files and apps** and **click Next** | Graphical user interface, text, application  Description automatically generated |
| 1. The upgrades typically take about 20-25 minutes in the field, depending on the hardware. | Graphical user interface, text, application  Description automatically generated |
| 1. Fully Update the Node with Windows Updates |  |
| 1. Disable Storage Maintenance Mode | Get-StorageFaultDomain -type StorageScaleUnit |  Where FriendlyName -Eq <ServerName> |  Disable-StorageMaintenanceMode |
| 1. Resume the Cluster Node | Resume-ClusterNode |
| 1. Wait for the Storage Jobs to complete and for the Virtual disks to be healthy | Get-StorageJob  Get-VirtualDisk |
| 1. Update the Functional Cluster Level | Update-ClusterFunctionalLevel |
| 1. Update the Storage Pool | Update-StoragePool |
| 1. Reset the VM Live Migration Checks | Get-ClusterResourceType -Cluster {clusterName} -Name "Virtual Machine" |  Set-ClusterParameter SkipMigrationDestinationCheck -Value 0 |
| 1. Upgrading to Server 2022 S2D | Upgrades from Server 2016 to Server 2022 are not directly supported. Thus, a double swing is required to get fully up to Server 2022. Repeat the steps above again this time with the Server 2022 media to complete the upgrade. The individual steps do not change as part of this process. |

Wrap-up

Join us at MVPDays and meet great MVPs like this in person

If you liked their book, you would love to hear them.

## Live Presentations

Dave frequently speaks at Microsoft conferences around North America, such as TechEd, VeeamOn, TechDays, and MVPDays Community Roadshow.

Cristal runs the MVPDays Community Roadshow.

You can find additional information on the following blog:

[www.checkyourlogs.net](http://www.checkyourlogs.net)

[www.techmentor.com](http://www.mvpdays.com)

## Video Training

For video-based training, see the following site:

www.techmentor.com

## Live Instructor-led Classes

Dave has been a Microsoft Certified Trainer (MCT) for more than 15 years and presents scheduled instructor-led classes in the US and Canada. For current dates and locations, see the following sites:

* www.truesec.com
* www.checkyourlogs.net

## Consulting Services

Dave and Cristal have worked with some of the largest companies in the world and had a wealth of experience and expertise. Customer engagements are typically between two weeks and six months.