WSUS Config lab and Active Directory Backup and Authoritative Restore lab.

Yogaraj Govindarajalu Prabagaran

# Table of Contents

[Table of Contents 2](#_Toc151328679)

[Assignment- 3 WSUS Config lab and Active Directory Backup and Authoritative Restore lab. 3](#_Toc151328680)

[Parts 3](#_Toc151328681)

[Description 3](#_Toc151328682)

[Preparation 4](#_Toc151328683)

[Observations 6](#_Toc151328684)

[Screenshots 8](#_Toc151328685)

[Reflection 28](#_Toc151328686)

[References 30](#_Toc151328687)

# WSUS Config lab and Active Directory Backup and Authoritative Restore lab.

# Parts

## Description

Windows Update and Service Configuration.

I was undertaking the Windows Update Service Configuration lab to enhance my practical knowledge in installing and configuring the Windows Update Service (WSUS) for efficient system patch management. The lab involved setting up a three-VM environment, each with a specific role, personalized using my student ID.

In Part 1, I installed the WSUS role on the designated server (SUSMS VM), emphasizing key configuration details. Reflecting on the significance of IIS installation highlighted its impact on system security.

Part 2 extended the configuration to the workstation (SUSWS VM), involving the creation of Active Directory OUs and GPOs for streamlined update management. The reflection emphasized the advantages of using an in-house update server.

Part 3 focused on creating computer groups in WSUS, demonstrating an understanding of their role in controlled update deployment. Reflection in this section considered the strategic use of computer groups for tailored update management.

In Part 4, I deployed updates, approving the Cumulative Update for Windows Server 2019. The associated reflection discussed the optimization of system stability and security through WSUS.

Throughout the lab, meticulous documentation and clear, labeled screenshots were prioritized, providing a comprehensive hands-on experience and a deeper understanding of WSUS's strategic role in maintaining a secure and stable IT environment.

Active Directory Backup and Authoritative Restore

In this lab exercise, I engaged in practical activities related to Windows Infrastructure and Security. The focus was installing a feature in Server 2019, performing a system state backup of the Active Directory (AD) domain database, and executing an authoritative restore to recover a deliberately deleted Organizational Unit (OU). Initial preparations involved creating storage space for backup, and subsequent steps included configuring the system for DSRM, listing backups, and performing an authoritative restore using NT Domain Services utility commands. The exercise provided hands-on experience in Windows Infrastructure and Security, emphasizing AD backup and authoritative restore procedures, ultimately enhancing practical skills in navigating critical Windows functionalities.

## Preparation

Windows Update and Service Configuration.

Before delving into the Windows Update Service Configuration lab, I prepared the lab environment to ensure a seamless and practical learning experience. The following steps outline my preparation process:

Setting Up the Lab Environment:

I initiated the setup by creating a lab environment consisting of three Windows Server VMs, each assigned a specific role: SUSDC, SUSMS, and SUSWS.

Configuring Computer Names:

I aligned the computer names on all VMs with the designated VM names to ensure consistency and clarity throughout the lab.

Disk Configuration for WSUS Server:

To designate the SUSMS VM as the Windows Update Service server, I added a 40GB thin provisioned disk.

The disk was initialized, and an NTFS volume was created, consuming the entire new disk for optimal WSUS storage.

Promoting the DC VM to Domain Controller:

The DC VM was promoted to domain controller using the domain name 8869578-SUS.corp.

Ensured that the domain provided DNS services as required for a smoothly functioning AD environment.

Joining VMs to the AD Domain:

The other two VMs, SUSMS and SUSWS, were joined to the AD domain for seamless integration within the network.

Designating Workstation VM:

Identified the SUSWS VM as the designated "workstation" to serve as an update client in the lab environment.

By meticulously completing these preparation steps, I established a robust foundation for the lab's subsequent installation and configuration tasks. This approach aimed at ensuring a well-organized and personalized learning experience tailored to the objectives of the Windows Update Service Configuration lab.

Active Directory Backup and Authoritative Restore

I initiated the environment preparation for the upcoming Active Directory (AD) backup and authoritative restore exercises. Please note that the same domain controller- “8869578-SUSDC,” was also used in this exercise. The initial step involved creating storage space for the backup, mirroring real-world scenarios where backing up to the same disk as the source is discouraged.

Disk Addition:

A 60GB thin provisioned disk was added to the domain controller, setting the stage for a dedicated backup location.

Initialization:

With the new disk in place, it was brought online and initialized, ensuring it was ready for the upcoming backup operations.

Volume Creation:

The next logical step was to create a new NTFS volume on the initialized disk. This volume, driven E, would be the designated space for the system state backup.

OU Creation:

To mimic real-world scenarios, a new Organizational Unit (OU) named "Test-Restore" was created without accidental deletion protection. This OU and its distinguished name (DN) and Update Sequence Number (USN) value were pivotal in the subsequent exercises.

Security Groups and Users:

A security group named "Test-Group" was crafted within the Test-Restore OU. Additionally, to simulate a more comprehensive restore scenario, two new users were created within the Test-Restore OU, making them members of the Test-Group security group.

These preparatory steps laid the groundwork for the subsequent tasks involving AD backup, OU deletion, and the crucial authoritative restore process. The intentional focus on realistic configurations and settings aimed to replicate the challenges and considerations one might encounter in a production environment.

## Observations

Windows Update and Service Configuration.

The execution of the Windows Update Service Configuration lab proceeded smoothly, and I observed the following outcomes during each phase:

Installation and Initial Configuration (Part 1):

Installing the WSUS role on the SUSMS VM was seamless, with all defaults accepted as per the instructions.

The WSUS management console opened without any issues after the installation, allowing for the completion of the configuration wizard.

Configuration settings were applied without unexpected challenges, including storage path and synchronization preferences.

The initiation of the initial synchronization with Microsoft Update occurred as expected, and the chosen product categories and classifications were successfully configured.

Workstation Update Configuration (Part 2):

Creating the AD OU and sub-OU for workstations proceeded without hitches, and the GPO named WSUS was successfully linked to the Workstation OU.

Editing the Windows Update policy within the GPO and configuring the update server address were straightforward tasks.

Moving the SUSWS VM to the designated OU, forcing a group policy update, and manually triggering a software update unfolded seamlessly.

The expected screenshots capturing the configuration of Windows Update on the workstation, registration with the WSUS server, and placement in the Unassigned computers container were successfully obtained.

Computer Containers Configuration (Part 3):

Computer groups were created in the WSUS console for different categories, such as workstations and servers, without complications.

Moving the SUSWS VM to the Workstations group was straightforward, and the subsequent patch status observation provided the anticipated results.

Screenshots captured all created groups, the VM's placement in the designated group, and the workstation's patch status as intended.

Update Deployment (Part 4):

Approving the Cumulative Update for Windows Server 2019 in the WSUS console was completed without any unexpected issues.

The subsequent manual run of Windows Update on the workstation VM resulted in the expected deployment of the approved updates.

Screenshots successfully documented the approval of updates and the 100% deployment status outlined in the lab instructions.

Overall, the lab's execution aligned with the anticipated outcomes, and the seamless progression through each phase underscored the effectiveness of the preparation and configuration steps.

Active Directory Backup and Authoritative Restore

As I progressed through the lab, the execution of Active Directory (AD) backup and authoritative restore unfolded seamlessly, meeting the anticipated outcomes. Here's a firsthand account of the observations during and after the process:

Backup Execution:

Installing the Windows Backup feature and the subsequent one-time backup of the system state proceeded without any issues. The backup operation targeted the designated E: drive, as planned during the preparation phase.

OU Deletion:

After the successful backup, I deleted the Test-Restore Organizational Unit (OU). The deletion went as expected, simulating an accidental deletion scenario.

Authoritative Restore:

Configuring the system to reboot into Directory Services Recovery Mode (DSRM) and authenticating using the local Administrator account facilitated the authoritative restore process. The command-line operations within the NT Domain Services utility executed smoothly, guiding me through the recovery steps.

Verification Steps:

After the system rebooted into normal mode, I logged in to verify the results. The Test-Restore OU and its subordinate objects were present as expected. A critical verification step included comparing the OU's Update Sequence Number (USN) value to the pre-deletion and restoration values. This comparison validated the successful authoritative restoration.

Final Checks:

To ensure completeness, I verified the presence of the Test-Group security group and the two users within the Test-Restore OU. All components were intact, confirming the accurate recovery of the deleted objects.

In summary, the execution of the AD backup, OU deletion, and authoritative restore processes unfolded smoothly, aligning with the lab objectives. This hands-on experience reinforced theoretical knowledge and provided practical insights into the nuances of Windows Infrastructure and Security, particularly in AD recovery procedures.

## Screenshots

Windows Update and Service Configuration.

A screenshot of a computer

Description automatically generated

Figure 1.1: The above screenshot shows that the workstation's Windows Update is pointed to a private server.

A screenshot of a computer

Description automatically generated

Figure 1.2: The above screenshot showcases the same thing as Figure 1.1 but verifies it in the registry editor.

A screenshot of a computer

Description automatically generated

Figure 2: The above screenshot showcases the 8869578- SUSWS VM in the Workstation OU.

A screenshot of a computer

Description automatically generated

Figure 3: The above screenshot shows that the workstation is registered with the WSUS server and in the Unassigned computers container.

A screenshot of a computer

Description automatically generated

Figure 4: The above screenshot showcases all groups created correctly in the WSUS console, WSUSWS VM in the Workstation group, and workstation patch status.

A screenshot of a computer

Description automatically generated

Figure 5: The above screenshot showcases the approved updates with 100% deployment from the WSUS console.

Active Directory Backup and Authoritative Restore

A screenshot of a computer

Description automatically generated

Figure 1: The above screenshot showcases the Windows Server Backup feature installation in the 8869578- SUSDC.

A screenshot of a computer

Description automatically generated

Figure 2: The above screenshot showcases the one-time backed-up system back up to the E: drive.

A screenshot of a computer

Description automatically generated

Figure 3: The above screenshot showcases the deletion of the Test-Restore OU.

A screenshot of a computer

Description automatically generated

Figure 4: Configure into safe mode and Reboot

This screenshot illustrates the elevated command prompt with the entry "bcdedit /set safeboot dsrepair" to configure the system to reboot into safe mode. The subsequent command "shutdown -r -t 0" initiates the server reboot, a crucial step for the authoritative restore process.

A computer screen shot of a computer

Description automatically generated

Figure 5: This screenshot showcases the 8869578-SUSDC in Safe mode.

A screenshot of a computer

Description automatically generated

Figure 6: Backup Versions Listing

Displayed in Figure 6 is the command-line interface showing the available backups for restoration. The command "wbadmin get versions" is executed, and the version information is noted for reference in the subsequent steps.

A screenshot of a computer

Description automatically generated

Figure 7: System State Recovery

In this screenshot (Figure 7), the command "wbadmin start systemstaterecovery -version:mm/dd/yyyy-hh:mm" is executed to perform a system state recovery. The version information matches the identified backup version, and the process prompts for a restart, allowing for a controlled exit from the wbadmin utility.

A screenshot of a computer program

Description automatically generated

Figure 8: This screenshot showcases how to escape the restart sequence by pressing ^C to exit the wbadmin utility.

A screenshot of a computer

Description automatically generated

Figure 9: Launch NTDS Utility

This screenshot (Figure 9) captures the command prompt with the entry "ntdsutil" to launch the NT Domain Services utility. This marks the initiation of the utility, a crucial step in the authoritative restore process.

A screenshot of a computer program

Description automatically generated

Figure 10: Activate NTDS Instance

In Figure 10, the NTDS utility is active, and the command "activate instance ntds" is executed. This step ensures that the utility works within the context of the NTDS instance, preparing for authoritative restore operations.

A screenshot of a computer program

Description automatically generated

Figure 11: Authoritative Restore Mode

Displayed in Figure 11 is the command "authoritative restore" within the NTDS utility. This command switches the utility to authoritative restore mode, allowing for the precise recovery of the deleted Test-Restore OU and its subordinate objects.

A screenshot of a computer

Description automatically generated

Figure 12: Specify Restore Subtree

In this screenshot (Figure 12), the command "restore subtree ou=Test-Restore,dc= 8869578-SUS,dc= corp" is executed within the authoritative restore mode.

A screenshot of a computer program

Description automatically generated

Figure 13: Exit Authoritative Restore and NTDS Utility

This combined screenshot showcases the sequence of commands within the NT Domain Services utility. The command "q" is entered to exit the authoritative restore mode, concluding the specific restoration actions. The same command "q" is used to exit the NTDS utility entirely. These steps mark the completion of the authoritative restore process, with the utility closed and the system ready for the final configurations before a normal reboot.

A screenshot of a computer

Description automatically generated

Figure 14: System Configuration for Normal Boot

This screenshot (Figure 9) showcases the command "bcdedit /deletevalue safeboot" to configure the system for a normal boot. Subsequently, the system is rebooted using the command "shutdown -r -t 0," transitioning from Directory Services Recovery Mode to the standard operating mode.

A screenshot of a computer

Description automatically generated

Figure 15: Post-Restore Verification

Figure 15 presents the presence of the Test-Restore OU and its subordinate objects verified, ensuring the successful authoritative restore. Additionally, the USN value of the OU is compared to pre-deletion and restoration values for confirmation. The Current Sequence number USN is greater than the original one.

## Reflection

Windows Update and Service Configuration.

What is the significance and role of IIS being installed, and how could that affect security?

The lab exercises explore the installation of Internet Information Services (IIS), highlighting its significance and potential impact on security. IIS exposes the system to external threats, necessitating secure configuration to mitigate risks like unauthorized access and injection attacks. The role of IIS in hosting Windows updates adds complexity, requiring robust security measures such as authentication and encryption. Timely application of security patches is emphasized to address evolving cyber threats. Balancing IIS's enhanced functionality with proactive security measures is crucial for maintaining a secure computing environment.

Write a reflection. At a minimum, discuss the advantages of using an in-house update server.?

Implementing an in-house update server, such as WSUS, offers several advantages. These include enhanced network control for strategic update scheduling, bandwidth optimization through centralized downloads, improved security with scrutiny over updates, customization and testing flexibility, and compliance with internal policies and regulatory requirements. This centralized approach streamlines the update process, ensuring a resilient and secure computing infrastructure.

Write a reflection. At a minimum, discuss how computer groups can control which updates are deployed to which computers.?

Computer groups within WSUS provide administrators with a powerful toolset for controlling the deployment of updates. This strategic approach enables targeted update deployment to specific sets of computers based on criteria such as function or department. The customization afforded by computer groups accommodates diverse environments, allowing for varied update schedules and prioritization. Additionally, computer groups support phased rollouts and testing, minimizing the risk of network-wide issues. Their role extends to compliance monitoring, ensuring systems adhere to established updated policies, and facilitating reporting for audits and regulatory requirements. Computer groups contribute to an organized, efficient, and secure update process within the Windows environment.

Write a reflection. At a minimum, discuss how system stability and security can be optimized regarding updates by using WSUS.

WSUS optimizes system stability and security by providing a centralized and controlled update approach. Through WSUS, administrators can regulate the timing and deployment of updates, ensuring stability by preventing widespread disruptions. The system's security is enhanced through the timely application of security patches, allowing for a proactive response to evolving threats. WSUS also enables customized security policies, aligning update practices with organizational requirements. The centralized monitoring and reporting features of WSUS streamline the identification of issues, contributing to a resilient and well-protected computing infrastructure. WSUS is a cornerstone for achieving a harmonious balance between system stability and security in the Windows environment.

Active Directory Backup and Authoritative Restore

Embarking on this lab proved instrumental in bridging theoretical concepts with practical applications. I seamlessly executed Windows Backup, system state recovery, and an authoritative restore to recover a deleted Organizational Unit (OU). The emphasis on realistic preparation, verification steps, and the intricate process of configuring Directory Services Recovery Mode provided valuable insights into Active Directory recovery procedures. The lab heightened my technical proficiency and underscored the critical thinking and troubleshooting skills essential in IT administration. This hands-on experience has fortified my confidence in navigating the complexities of Windows Infrastructure and Security, offering a holistic understanding of AD backup and authoritative restore intricacies.

# References

1. J. (2023, March 13). *Get started with Windows Server Update Services (WSUS)*. Microsoft Learn. <https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus>
2. J. D. (2019, March 4). *Installing and Initializing WSUS*. YouTube. <https://www.youtube.com/watch?v=DQ9lKE7dCcY>
3. J. D. (2019, March 4). *Configuring the WSUS Client*. YouTube. <https://www.youtube.com/watch?v=VfN-s9QYJUY>
4. J. D. (2019, March 4). *Configuring WSUS Computer Groups*. YouTube. <https://www.youtube.com/watch?v=qJjggNPScUo>
5. J. D. (2019, March 4). *Approving Patches for Deployment in WSUS*. YouTube. <https://www.youtube.com/watch?v=tuM6CAqv7-U>
6. J. D. (2020, April 2). *Active Directory Authoritative Restore*. YouTube. <https://www.youtube.com/watch?v=tJBT-n_cgos>